Privacy Impact Assessment
for the

Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program

DHS/NPPD/PIA-018

May 4, 2011

Contact Point
Todd Klessman
NPPD / IP / ISCD
(703) 603-4614

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) / National Protection & Programs Directorate (NPPD) / Office of Infrastructure Protection (IP) / Infrastructure Security Compliance Division (ISCD) is conducting this Privacy Impact Assessment (PIA) to detail the privacy impact associated with the Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program and the required security assessments performed by high-risk chemical facilities in fulfillment of Risk-Based Performance Standard # 12 (6 CFR 27.230(a)(12)). This PIA describes the procedures for submitting personally identifiable information (PII) on individuals impacted by this program to NPPD, and also describes NPPD's uses of that PII.

Overview

On October 4, 2006, the President signed the Department of Homeland Security Appropriations Act of 2007 (the Act), Public Law 109-295. Section 550 of the Act (Section 550) provides DHS with the authority to regulate the security of high-risk chemical facilities. DHS has promulgated regulations implementing Section 550, the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27.

Section 550 requires that DHS establish Risk Based Performance Standards (RBPS) as part of CFATS. RBPS-12 (6 CFR 27.230(a)(12)(iv)) requires that regulated chemical facilities implement "measures designed to identify people with terrorist ties." The ability to identify individuals with terrorist ties is an inherently governmental function and requires the use of information held in government-maintained databases, which are unavailable to high-risk chemical facilities. Therefore, DHS is implementing the CFATS Personnel Surety Program, which will allow chemical facilities to comply with RBPS-12 by implementing "measures designed to identify people with terrorist ties."

High-risk chemical facilities must address how they will comply with RBPS-12 in their Site Security Plans (SSPs),[1] including how they will participate in the CFATS Personnel Surety Program. High-risk chemical facilities that fail to address how they will participate in the CFATS Personnel Surety Program may have their SSPs disapproved by NPPD. In addition, those high-risk chemical facilities that fail to submit the required PII to NPPD, in violation of their SSPs, may be subject to the issuance of administrative compliance orders or other consequences under CFATS.[2]

[1] See 6 CFR 27.225 (describing SSPs).
[2] See 6 CFR 27.300.

Affected Individuals

Certain individuals (known as "affected individuals") are subject to terrorist ties screening under CFATS. Specifically, affected individuals at high-risk chemical facilities are: 1) facility personnel who have or are seeking access, either unescorted or otherwise, to restricted areas or critical assets; and 2) unescorted visitors who have or are seeking access to restricted areas or critical assets. Individual high-risk facilities may classify particular contractors or categories of contractors either as "facility personnel" or as "visitors." This determination is a facility-specific determination, and is based on facility security, operational requirements, and business practices.

NPPD screens affected individuals for terrorist ties by comparing their PII against information pertaining to known and suspected terrorists maintained by the federal government in the Terrorist Screening Database (TSDB). For more information on the TSDB, see DOJ/FBI – 019 Terrorist Screening Records System, 72 FR 47073 (August 22, 2007).

Vetting Process

High-risk chemical facilities (or third-party individuals designated by facilities, hereinafter referred to as designees) will submit PII pertaining to affected individuals to NPPD through the Chemical Security Assessment Tool (CSAT), the online data collection portal for CFATS.[3] At a minimum, the high-risk chemical facilities or their designees are required to submit the following:

a. U.S. Citizens and Lawful Permanent Residents (LPRs)
    i. Full name;
    ii. Date of birth; and
    iii. Citizenship or Gender.
b. Non-U.S. persons
    i. Full name;
    ii. Date of birth;
    iii. Citizenship; and
    iv. Passport information and/or alien registration number.

[3] ISCD has issued another PIA that discuses information collected related to CSAT user accounts, information collected as part of SSPs, as well as other types of information collections. This PIA and subsequent PIA updates may be found at www.dhs.gov/privacy, or at www.dhs.gov/chemicalsecurity.

To reduce the likelihood of false positives in matching against the TSDB, high-risk chemical facilities may also submit the following information (optionally) for affected individuals:

a. Aliases;

b. Gender (for Non-U.S. persons);

c. Place of birth; and

d. Redress Number.

Facilities or their designees are required to use CSAT to: 1) submit information about an affected individual for the first time; 2) submit additional, updated, or corrected information about an affected individual; and/or 3) notify DHS that an affected individual no longer has or is seeking access to that facility's restricted areas or critical assets. High-risk chemical facilities and their designees will have access to the data they submit in order to update and/or correct affected individuals' PII, should the need arise.

High-risk chemical facilities will establish their own internal procedures for collecting and submitting the required PII from affected individuals. The high-risk chemical facility or its designees will submit the information of affected individuals to DHS through CSAT. The Submitter(s) of each high-risk chemical facility will affirm that, in accordance with their Site Security Plans, notice required by the Privacy Act of 1974, 5 U.S.C. § 552a has been given to affected individuals before their information is submitted to DHS. NPPD will make available to high-risk chemical facilities a sample notice, which complies with section (e)(3) of the Privacy Act of 1974. The notice will provide information to affected individuals about access, correction, and redress.[4] Each Submitter will also affirm, to the best of his/her knowledge, that the information submitted is: 1) true, correct, and complete; and 2) collected and submitted in compliance with his/her facility's SSP.

PII pertaining to affected individuals will be electronically transmitted by NPPD to DHS's Transportation Security Administration (TSA). TSA's Office of Transportation Threat Assessment and Credentialing (TTAC), which conducts vetting of information against the TSDB for several DHS programs, will conduct the vetting on behalf of NPPD.

TTAC will compare the information pertaining to affected individuals to information listed in the TSDB. TTAC will determine whether each individual's PII: 1) does not match a TSDB record; or 2) is a potential match to a TSDB record. Each potential match to the TSDB will then be manually vetted to determine whether a match has occurred.

[4] See Attachment 2.

TTAC will forward results of all positive matches to the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC), which will make final match determinations and coordinate any necessary response. TTAC will also notify NPPD of any positive match.

As part of this process, TTAC or the TSC may request that NPPD obtain additional information (e.g., visa information) about affected individuals from high-risk chemical facilities in order to clarify data errors or to resolve potential matches (e.g., in situations where an affected individual has a common name). Such requests will not imply, and should not be construed to indicate, that an individual has been confirmed as a match to the TSDB.

NPPD may also conduct data accuracy reviews and audits as part of the CFATS Personnel Surety Program. Such reviews may be conducted on random samples of affected individuals. To assist with this activity, NPPD may request information pertaining to affected individuals previously provided to NPPD by high-risk chemical facilities, to confirm the accuracy of that information.

Comparability with Other DHS Vetting Programs

In lieu of conducting new TSDB vetting of an affected individual, NPPD may collect information to verify that an individual is currently enrolled in a DHS program that also requires a TSDB check equivalent to the TSDB vetting performed as part of the CFATS Personnel Surety Program. Those programs are:

a. Transportation Worker Identification Credential[5] (TWIC);

b. Hazardous Material Endorsement (HME);

c. Trusted Traveler Programs,[6] including:

   i. NEXUS;

   ii. Free and Secure Trade (FAST); and

   iii. Secure Electronic Network for Travelers Rapid Inspection (SENTRI).

To verify an affected individual's enrollment, NPPD may collect the following PII on the affected individual:

a. Full Name;

b. Date of Birth; and

[5] The TWIC and HME Programs are covered under the Transportation Security Threat Assessment System of Records Notice. See DHS/TSA-002–Transportation Security Threat Assessment System, 75 FR 28046 (May 19, 2010).

[6] The Trusted Traveler Programs are covered under the Global Enrollment System of Records Notice. See DHS/CBP-002 – Global Enrollment System (GES), 71 FR 20708 (April 21, 2006).

c. Program-specific information or credential information, such as unique number, or issuing entity (e.g., State for Commercial Driver's License with an HME).

The table below outlines the information required to verify enrollment.

TABLE 1: Required Data Necessary To Verify Enrollment

	TWIC	HME	NEXUS	SENTRI	FAST
Name	Required	Required	Required	Required	Required
Date of Birth	Required	Required	Required	Required	Required
Unique Credential Information	- TWIC Serial Number: Required - Expiration Date: Required	- Commercial Drivers License (CDL) Issuing State(s): Required - CDL Number: Required - Expiration Date: Required	- PASS Number: Required - Expiration Date: Required	- PASS Number: Required - Expiration Date: Required	- PASS Number: Required - Expiration Date: Required

High-risk chemical facilities may also submit the following information (optionally) on affected individuals when verifying enrollment:

a. Aliases;

b. Place of birth;

c. Gender;

d. Citizenship; and

e. Redress Number.

Leveraging a previous equivalent TSDB background check will limit the number of instances in which different DHS programs may vet the same affected individual against the TSDB.

If high-risk chemical facilities find it administratively easier to submit the routine vetting information described in the Vetting Process section of this PIA for all individuals to DHS, even if they have been previously vetted, facilities may do so. In that case, DHS will vet affected individuals against the TSDB, and will not seek to verify an affected individual's enrollment in TWIC, HME, NEXUS, SENTRI or FAST.

Match Verification Process for Other DHS Vetting Programs

If DHS cannot confirm an affected individual's current enrollment in one of the previously mentioned programs, or if previous vetting results cannot be verified, DHS will either: 1) notify the high-risk chemical facility that the Department could not verify that the affected individual is currently enrolled in a DHS program; and/or 2) vet the affected individual against the TSDB. When a high-risk chemical facility is notified that the Department could not verify that the affected individual is currently enrolled in a DHS program, the high-risk chemical facility must either: 1) submit additional information, which corrects or updates the previous information to verify enrollment; or 2) provide sufficient information for the Department to conduct vetting of the affected individual against the TSDB. Such notifications from DHS will not imply, and should not be construed to indicate, that an individual has been confirmed as a match to the TSDB.

Federal Response to a Positive Match

Upon final determination by TSC that an individual is a positive match, TTAC, NPPD, and federal law enforcement agencies will be notified as appropriate. NPPD will not routinely provide vetting results to high-risk chemical facilities, nor will it provide results to an affected individual whose information has been submitted by a high-risk chemical facility. As warranted, high-risk chemical facilities may be contacted by DHS or federal law enforcement agencies as part of law enforcement investigation activity.

Bulk Submission of Data

The Department will allow high-risk chemical facilities and their designees to upload information about affected individuals in bulk to reduce the burden on high-risk chemical facilities. To assist in bulk upload, the Department may also collect information that will allow high-risk chemical facilities to manage their data submission (e.g., a unique designation for an electronic record that is associated with an affected individual). This information will be used by the high-risk chemical facility or its designees to manage the exchange of electronic records between a high-risk chemical facility's information systems (or its designees' information systems) and the records maintained for the high-risk chemical facility within CSAT.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

During an initial submission, NPPD will collect the following information pertaining to affected individuals who are U.S. citizens and LPRs: 1) full name; 2) date of birth; and 3) citizenship or gender for purposes of matching against the TSDB.

If an affected individual is a non-U.S. person, NPPD will collect the individual's: 1) full name; 2) date of birth; 3) citizenship; and 4) passport information and/or alien registration number for purposes of matching against the TSDB.

To reduce the likelihood of false positives in matching against the TSDB, high-risk chemical facilities may also (optionally) submit the following information on facility personnel and unescorted visitors who have or are seeking access to restricted areas or critical assets: 1) aliases; 2) gender (for non-U.S. persons), 3) place of birth; and 4) DHS redress number.

NPPD will also collect information that identifies the high-risk chemical facilities at which each affected individual has access, or is seeking access, to restricted areas or critical assets.

NPPD may collect information to verify that an individual is currently enrolled in a DHS program which includes a TSDB check equivalent to the TSDB vetting performed as part of the CFATS Personnel Surety Program. Such information will include: 1) full name; 2) date of birth; 3) name of the DHS program which conducts equivalent vetting against TSDB, such as the TWIC program or the HME program; 4) unique number or other program specific verifying information associated with a DHS screening program, necessary to verify an individual's enrollment, such as a TWIC serial number, or a CDL number and CDL issuing state(s) for the HME program; and 5) expiration date of the credential endorsed or issued by the DHS program. NPPD may also (optionally) collect information on affected individuals when verifying enrollment. Such information may include: 1) aliases; 2) place of birth; 3) gender; 4) citizenship; and 5) Redress Number.

NPPD may contact a high-risk chemical facility if additional information (e.g., visa information) is needed about an affected individual in order to resolve a data error or a potential match (e.g., in situations where an affected individual has a common name). Such requests will not imply, and should not be construed to indicate, that an individual has been confirmed as a

match to the TSDB. Information collected by high-risk chemical facilities and submitted to DHS for this purpose could include: 1) information listed above; 2) passport information; 3) visa information; 4) driver's license information: or 5) other available identifying particulars used to compare the identity of an individual being screened with information listed in the TSDB.

NPPD may also conduct data accuracy reviews and audits as a part of the CFATS Personnel Surety Program. Such reviews may be conducted on random samples of affected individuals. To assist with this activity, NPPD may request information previously submitted to NPPD about affected individuals from the high-risk chemical facilities to confirm its accuracy.

In addition, NPPD will also collect information necessary to assist in tracking submissions and transmission of records, including electronic verification that DHS has received a particular record.

Further, NPPD may also collect information on affected individuals as necessary to enable it to provide redress for individuals who believe they have been improperly impacted by the CFATS Personnel Surety Program. The information collected may include information necessary to conduct adjudications under Subpart C of CFATS.[7]

NPPD will also collect information about who to contact at a high-risk chemical facility if DHS or a federal law enforcement agency has any follow-up questions about an affected individual.

Information will be collected from other sources (including, but not limited to, law enforcement sources, and the TSDB) in the event that a match to the TSDB is identified as part of the Personnel Surety Program.

1.2 What are the sources of the information in the system?

High-risk chemical facilities will collect information about affected individuals and submit the individuals' information to NPPD through CSAT, the secure web-based application maintained by NPPD. A high-risk chemical facility may, at its discretion, leverage third party designees to submit information about affected individuals on behalf of the high-risk chemical facility. This capability seeks to ensure that the CFATS Personnel Surety Program allows high-risk chemical facilities flexibility in how they are able to comply with RBPS-12.

Submitters, whether they are facility employees, corporate employees, or third party designees, will be able to submit vetting information directly to NPPD on behalf of a facility. Each high-risk chemical facility will be responsible for ensuring that its Submitter(s) appropriately submit proper information pertaining to affected individuals to NPPD for vetting.

[7] See 6 CFR 27.300 – 6 CFR 27.345.

The Department will also obtain information about affected individuals from other DHS programs that perform TSDB vetting equivalent to CFATS Personnel Surety Program TSDB vetting.

1.3 Why is the information being collected, used, disseminated, or maintained?

The PII will be collected to vet and determine whether any ties to terrorism exist for high-risk chemical facilities personnel and unescorted visitors who have access, or are seeking access, to restricted areas or critical assets at those facilities. Identification of individuals with terrorist ties will allow the federal government to mitigate the risks of: 1) successful terrorist attacks against high-risk chemical facilities; and 2) individuals using chemicals from high-risk chemical facilities for the commission of terrorist attacks.

1.4 How is the information collected?

NPPD will routinely receive PII from high-risk chemical facilities or their designees through CSAT. In rare instances, if necessary and following coordination with DHS, facilities or their designees may also submit additional PII via email, facsimile, or telephone.

High-risk chemical facilities responsible for collecting PII from affected individuals under CFATS will establish their own internal procedures or processes for collecting the required PII. DHS will send a verification of receipt to a high-risk chemical facility when a high-risk chemical facility or designee: 1) submits information about an affected individual for the first time; 2) submits additional, updated, or corrected information about an affected individual; and/or 3) notifies DHS that an affected individual no longer has or is seeking access to that facility's restricted areas or critical assets.

NPPD may also collect enrollment and current status information to verify enrollment in other DHS programs from both: 1) the U.S. Customs and Border Protection (CBP) Trusted Traveler Programs; and 2) TSA's TWIC and HME programs.

1.5 How will the information be checked for accuracy?

High-risk chemical facilities will be responsible for the accuracy of PII submitted to NPPD. High-risk chemical facilities and their designees will be required to affirm that, to the best of their knowledge, the PII submitted is true, accurate, and complete.[8] NPPD may also conduct audits and data accuracy reviews as a part of the CFATS Personnel Surety Program. Such audits and reviews may be conducted on random samples of affected individuals.

[8] See Attachment 1.

Further, TTAC will forward the results from potential TSDB matches to the TSC, which will then determine whether an individual's information is a match to a TSDB record. In certain instances, NPPD may contact a high-risk chemical facility if additional information is needed on an affected individual in order to resolve a potential match (e.g., in situations where an affected individual has a common name, or to clarify a data error). Such requests will not imply, and should not be construed to indicate, that an individual has been confirmed as a match to the TSDB.

High-risk chemical facilities or their designees will be required to update and correct PII in CSAT as necessary (e.g., when an error or change in submitted information has been identified). A high-risk chemical facility and its designees will have access to the PII of a given individual in CSAT only for the duration of that affected individual's access to the facility's restricted areas or critical assets.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Section 550 of Public Law 109-295 provides DHS the authority to regulate high-risk chemical facilities. The implementing regulations for Section 550 require that high-risk chemical facilities implement "measures designed to identify people with terrorist ties."[9] The CFATS Personnel Surety Program will provide the capability for high-risk chemical facilities to meet this requirement by submitting PII to NPPD for vetting against the TSDB.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: Incorrect identification of an affected individual as a match to the TSDB may occur due to submission of inaccurate or limited PII to NPPD as part of the CFATS Personnel Surety Program.

Mitigation: NPPD will seek to reduce the potential for misidentification by: (1) requiring the minimum data elements which should be sufficient to distinguish each affected individual from individuals whose information is included in the TSDB; and (2) collecting, as optional data, information that can reduce even further the potential for misidentification (e.g., both citizenship and gender may be provided rather than just one data point or the other). NPPD will further mitigate the risk of misidentification by requiring Submitters to certify the accuracy, to the best of their knowledge, of the PII submitted to NPPD.

[9] See 6 CFR § 27.230(a)(12)(iv).

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

DHS will use the PII collected to identify individuals with terrorist ties by comparing affected individuals against information maintained in the TSDB. The PII collected by DHS may be used to facilitate operational, law enforcement, or intelligence responses, if appropriate, when affected individuals' identities match identities contained in the TSDB.

DHS may use information collected to verify that an individual is currently enrolled in a DHS program which relies on a TSDB check equivalent to the TSDB vetting performed as part of the CFATS Personnel Surety Program.

NPPD may conduct audits and data accuracy reviews as a part of the CFATS Personnel Surety Program. To assist with this activity, DHS may randomly request information previously provided to NPPD from high-risk chemical facilities on a small percentage of affected individuals to confirm its accuracy.

NPPD may collect information on affected individuals as necessary to enable it to provide redress for individuals who believe that they have been improperly impacted by the CFATS Personnel Surety Program. The information collected may include information necessary to conduct adjudications under Subpart C of CFATS.[10]

NPPD may also use the PII collected to ensure that high-risk chemical facilities are in compliance with the CFATS regulations. Compliance assurance activities may involve the use of PII to conduct inspections or audits under 6 CFR 27.245 and 6 CFR 27.250 to ensure that high-risk chemical facilities are in compliance with their SSPs.

2.2 What types of tools are used to analyze data and what type of data may be produced?

DHS will use standard tools to compare collected PII with information contained in the TSDB. Collected PII will be used to determine whether an individual is a match or a potential match to a TSDB record.

[10] See 6 CFR § 27.300 – 6 CFR § 27.345.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The CFATS Personnel Surety Program will not rely on commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above-described uses.

Privacy Risk: There is a potential privacy risk that PII may be improperly used.

Mitigation: PII collected by NPPD will be used only in accordance with the described uses by integrating administrative, technical, and physical security controls that place limitations on the collection of PII and protect PII against unauthorized disclosure, use, modification, or destruction. Specifically, administrative safeguards will restrict the permissible uses of PII and ensure adherence to those permissible uses. As part of its technical safeguards, CSAT will employ role-based access controls and audit logging, as described in Section 8.0 of this PIA, to control and monitor the use of PII. Further, all DHS personnel who are authorized to handle PII will be required to complete annual privacy training. These safeguards will minimize the potential privacy risk that PII may be improperly used.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

NPPD will retain the biographic information noted in Section 1.1, as well as the results of TSDB vetting. NPPD may also retain records or information collected from other sources in the event that an individual is determined to be a positive match to a TSDB record.

3.2 How long is information retained?

The length of time NPPD will retain information on individuals will be dependent on individual TSDB vetting results. Specifically, individuals' information will be retained as described below, based on individuals' placements into three categories:

a. Information pertaining to an individual who is not a potential match to a TSDB record will be retained for one year after a high-risk chemical facility has notified NPPD that the individual no longer has or is seeking access to the restricted areas or critical assets of the facility.

b. Information pertaining to an individual who may originally have appeared to be a match to a TSDB record, but who was subsequently determined not to be a match, will be retained for seven years after completion of TSDB matching, or one year after the high-risk chemical facility that submitted that individual's information has notified NPPD that the individual no longer has or is seeking access to the restricted areas or critical assets of the facility, whichever is later.

c. Information pertaining to an individual who is determined to be a positive match to a TSDB record will be retained for ninety-nine years after completion of matching activity, or seven years after NPPD learns that the individual is deceased, whichever is earlier.

TTAC will maintain records within its possession in accordance with the DHS/TSA-002 Transportation Security Threat Assessment System of Records, 75 FR 28046 (May 19, 2010). CBP will maintain records in its possession in accordance with the DHS/CBP-002 Global Enrollment System of Records, 71 FR 20708 (April 21, 2006).

NPPD will also retain records to conduct inspections or audits under 6 CFR 27.245 and 6 CFR 27.250 to ensure that high-risk chemical facilities are in compliance with CFATS. These records could include: 1) names of individuals with access to high-risk chemical facilities' restricted areas and critical assets; 2) periods of time during which high-risk chemical facilities indicate that such individuals have/had access; and 3) any other information listed elsewhere in this notice, as appropriate.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

A proposed schedule for the retention and disposal of records collected under the CFATS Personnel Surety Program is being developed by the DHS and NPPD Offices of Records Management for approval by National Archives and Records Administration (NARA).

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: There is a privacy risk that records containing PII collected under this program will not qualify as matches to the TSDB after further investigation and analysis but will be retained in the system longer than needed.

Mitigation: PII will be retained for only the minimum amount of time necessary and in accordance with the retention schedule listed above. Audits and ongoing vigilance will be applied to verify adherence to applicable record retention schedules.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

PII will be shared with authorized individuals within DHS who have a need to know the information to perform their official duties.

PII submitted by high-risk chemical facilities or their designees will be shared with TSA for the purpose of vetting against the TSDB. In addition, information may be shared with TSA and CBP for purposes of verifying enrollment in other DHS Programs. Information may also be shared within DHS to support responses by federal law enforcement and intelligence agencies, and/or to address threats to critical infrastructure and national security.

Affected individuals' PII may also be shared within DHS to facilitate records corrections, adjudications, and/or redress, as appropriate.

4.2 How is the information transmitted or disclosed?

PII will, when possible, be transmitted internally via an encrypted data network. However, depending on the urgency, PII may occasionally be transmitted by secure e-mail, in person, in paper format, by facsimile, by telephone, or otherwise as required by the circumstances necessitating such sharing.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: The primary privacy risks associated with internal information sharing and disclosure are unauthorized disclosure or loss of PII.

Mitigation: To mitigate the potential privacy risk of unauthorized disclosure of PII, NPPD will implement the necessary security controls to ensure that all personnel granted access to the information have a confirmed need to know the information to perform their duties and are authorized to handle information collected by NPPD under the CFATS Personnel Surety

Program. These individuals will be required to complete DHS privacy training on at least an annual basis.

Additionally, DHS has well-established and comprehensive information handling processes to enhance information security and eliminate possibilities for inappropriate sharing, misuse and/or loss, including the information handling processes described in the Department's *Handbook for Safeguarding Sensitive Personally Identifiable Information.*[11] CFATS Personnel Surety Program personnel will adhere to established internal information security policies, as well as those outlined in DHS information technology security documents. Periodic audits and evaluations will ensure continued compliance with DHS security and privacy requirements, including those that cover the internal sharing of PII.

Finally, any internal organization to which information will routinely be transmitted must have a documented interagency security agreement on file with DHS, approved by both parties, that outlines security and privacy controls in place to protect the confidentiality, integrity, and availability of PII being shared or processed. Internal components with whom PII is shared must agree to maintain reasonable physical, electronic, and procedural safeguards to appropriately protect the shared information. DHS is also required to handle PII in accordance with the requirements of the Privacy Act,[12] E-Government Act of 2002,[13] and Federal Information Security Management Act (FISMA),[14] as appropriate.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS, which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

PII collected by DHS will be shared externally in accordance with the routine uses listed in the CFATS Personnel Surety Program System of Records Notice (SORN).

DHS may externally share PII, matching analyses, and vetting results for appropriate action by federal law enforcement and intelligence agencies. DHS will also share information with the TSC, which maintains the federal government's consolidated and integrated terrorist watchlist (the TSDB).[15]

---

[11] Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf
[12] See 5 USC § 552a.
[13] See 44 USC Ch. 36.
[14] See 44 USC § 3541 et seq.
[15] The TSC shares information in accordance with the routine uses in the Terrorist Screening Records System,

DHS will share limited information about an affected individual with the high-risk chemical facility and the Submitter that submitted that individual's PII to DHS. Specifically, DHS will share information by: 1) allowing access to CSAT to update or correct PII; and 2) sending "verification of receipt" when a Submitter submits information about an affected individual to DHS. DHS will not routinely notify high-risk chemical facilities of vetting results.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Sharing of PII outside DHS is compatible with the CFATS Personnel Surety Program's SORN. The CFATS Personnel Surety Program's SORN covers sharing of PII by DHS with external entities (e.g., sharing information with the TSC to determine if an affected individual's PII matches PII contained in the TSDB). DHS will share PII with external parties as authorized by those routine uses cited in the CFATS Personnel Surety Program SORN.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

PII will, when possible, be transmitted outside DHS via an encrypted data network or made available through a protected web-based portal. Depending on urgency, PII may also be shared via e-mail using file encryption, in person, in paper format, via facsimile or telephone, or as otherwise required by the circumstance necessitating such sharing.

Information shared with high-risk chemical facilities may be accessed by those facilities via CSAT.

Further, the "verification of receipt" qualifies as Chemical-terrorism Vulnerability Information (CVI) as defined by 6 CFR 27.400, and must be safeguarded in compliance with 6 CFR 27.400 and the CVI Procedural Manual.[16]

Justice/FBI–019 SORN. See the amendment to the Federal Bureau of Investigation's Terrorist Screening Records System, published in the Federal Register on August 22, 2007, at 72 FR 47073.

[16] Available at http://www.dhs.gov/xlibrary/assets/chemsec_cvi_proceduresmanual.pdf

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy Risk: There is a privacy risk of unauthorized access to the PII collected, risk of unauthorized use/disclosure of the PII collected, and risk of loss of PII.

Mitigation: Each external organization that will maintain a direct connection with CSAT to transmit information will be required to have a documented interconnectivity security agreement on file with DHS, approved by both parties, that outlines security and privacy controls in place to protect the confidentiality, integrity, and availability of PII being shared or processed. External organizations with whom DHS shares PII must agree to maintain physical, electronic, and procedural safeguards to protect the shared information. Federal agencies receiving CFATS-related PII will also be required to handle it in accordance with federal data protection requirements, including the Privacy Act, E-Government Act, and FISMA, as appropriate.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. High-risk chemical facilities and their designees will be required to provide notice to affected individuals prior to any PII being submitted to NPPD. The notice will also advise the affected individual that additional information may be collected in order to clarify a data error, or to resolve a potential match (e.g., in situations where an affected individual has a common name). In these cases, NPPD may ask a high-risk chemical facility to provide additional PII. Such requests will not imply, and should not be construed to indicate, that an individual has been confirmed as a match to the TSDB. DHS may review notices or notice procedures as part of inspections or audits under 6 CFR 27.245 and 6 CFR 27.250. A sample notice is provided in Attachment 2.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes, however, if an individual declines to provide information, he or she may impact a high-risk chemical facility's compliance with CFATS. NPPD will not collect the information of affected individuals from the individuals themselves, but rather from high-risk chemical facilities or their designees. As such, affected individuals have no obligation to provide information to NPPD directly.

NPPD will not regulate the relationships between high-risk chemical facilities and affected individuals. NPPD, therefore, is not in a position to ascertain or comment on how high-risk chemical facilities will manage affected individuals who refuse to provide information for submission to NPPD under the CFATS Personnel Surety Program.

NPPD may disapprove the SSPs of high-risk chemical facilities that fail to include provisions for participation in the CFATS Personnel Surety Program. Further, NPPD may also take enforcement action under CFATS against high-risk chemical facilities that do not obtain and submit information of affected individuals in accordance with their SSPs.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. Affected individuals will not have the right to consent to particular uses of PII.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: There is a privacy risk that the high-risk chemical facility will fail to provide notice to the affected individual.

Mitigation: Prior to submitting the PII of affected individuals to NPPD, high-risk chemical facilities or their designees are required to affirm in CSAT that affected individuals are given notice indicating: 1) that their PII is submitted to DHS for the purposes of vetting against the TSDB; 2) steps for correcting inaccurate PII; and 3) that additional PII may be requested and will be submitted to DHS for the completion of the vetting process.

NPPD has made available to high-risk chemical facilities a sample notice that complies with subsection (e)(3) of the Privacy Act, 5 USC 552a(e)(3). This notice provides information about access, correction, and redress to affected individuals.[17]

By providing a sample notice to high-risk chemical facilities, NPPD will mitigate privacy risks including, but not limited to, lack of understanding on the part of the individual regarding a facility's collection and use of PII, and lack of ability to correct inaccurate information provided by a high-risk chemical facility.

Failure by high-risk chemical facilities to provide adequate notice may be identified during DHS inspections or audits under 6 CFR 27.245 and 6 CFR 27.250.

[17] See Attachment 2.

The Department has also provided notice through publication of a SORN for the CFATS Personnel Surety Program.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Affected individuals with questions about the accuracy of the PII submitted by a high-risk chemical facility should contact that facility. An affected individual may also request a copy of his/her PII from DHS by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to the NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380. Affected individuals may obtain directions on how to submit a FOIA/PA request at http://www.dhs.gov/xfoia/editorial_0316.shtm.

7.2 What are the procedures for correcting inaccurate or erroneous information?

To correct inaccurate or erroneous PII submitted by a high-risk chemical facility, affected individuals should contact the high-risk chemical facility responsible for the CFATS submission in question and request that the submission be updated with correct information. If the high-risk chemical facility is unable to, or refuses to, correct the inaccurate or erroneous information, the affected individual may write to the NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380, to have inaccurate or erroneous PII corrected.

7.3 How are individuals notified of the procedures for correcting their information?

As part of the CFATS Personnel Surety Program's notice requirements,[18] high-risk chemical facilities or their designees will notify affected individuals of the procedures for correcting inaccurate or erroneous PII. A sample notice is provided in Attachment 2. Additionally, procedures for correcting information are described in this PIA and its corresponding SORN.

[18] See section 6.0, above.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Formal redress will be provided as described above in sections 7.1-7.3. As appropriate, affected individuals may also request administrative adjudications under CFATS.[19]

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: There is a risk that high-risk chemical facilities or their designees will fail to provide notice to affected individuals of redress options or of the right to correct inaccurate or erroneous PII.

Mitigation: These risks will be mitigated by requiring Submitters to affirm that notification, including information about access, correction, and redress (similar to the sample notice provided in Attachment 2), is provided to each affected individual prior to submission of PII to DHS. DHS may evaluate a facility's notification procedures, as appropriate, under CFATS.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

Established security controls will be in place to limit access based on user roles and responsibilities, need to know, least privilege, and separation of duties. Rules governing a user's access to the system will be applied by the system automatically, based on the user's assigned role. Categories of users will be approved by the CSAT Information Systems Security Officer (ISSO) and any changes in roles will need approval prior to access.

8.2 Will Department contractors have access to the system?

Yes, designated DHS contractors will have access to the system as part of their contractual obligations.

[19] See 6 CFR 27.310(a)(1).

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Individuals with access to CSAT, working for or on behalf of, high-risk chemical facilities will not receive privacy training from DHS.

However, all government personnel and government contractors with access to CSAT will undergo DHS privacy training, which includes a discussion of Fair Information Practice Principles (FIPPs) and instructions on handling PII in accordance with FIPPs and DHS privacy policy. Additionally, all DHS personnel and government contractors will be required to complete annual privacy refresher training to retain system access. In addition, security training will be provided on an annual basis, which will help to maintain the level of awareness for protecting PII. DHS will report on employees, including contractors, who receive IT security and privacy training, as required by FISMA.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

CSAT is certified and accredited at the sensitive but unclassified (SBU) and Secret levels per National Institute Standards & Technology (NIST) 800-53 specifications and DHS policy and guidance, including DHS Sensitive System Policy Directive 4300A and DHS National Security System Policy Directive 4300B.

The NPPD Chief Information Security Officer (CISO) completed an initial Certification & Accreditation in July 2010, and subsequently issued a two-year Authority to Operate.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

DHS Management Directives 4300A and 4300B require that systems implement auditing at the user level and regularly analyze audit logs to determine misuse or abuse. The likelihood of unauthorized access will be mitigated through technical controls, including firewalls, intrusion detection, encryption, access control lists, system hardening techniques, and other security methods. All implemented controls will meet federal and DHS requirements governing information assurance.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: Privacy risks identified include system breach through unauthorized access to the PII collected, and risks of unauthorized use/disclosure of the PII collected.

Mitigation: To mitigate these risks, a variety of security controls will be implemented. DHS has well-established and comprehensive processes to enhance information security and minimize possibilities for unauthorized access. DHS personnel will adhere to internal information security policies. In addition, robust auditing measures and technical safeguards will monitor for unauthorized access or attempted access. To reduce the risk of a successful breach, proactive monitoring of logs will identify potential incidents as early as possible, and audit trails will be maintained to facilitate investigation of incidents in accordance with DHS Privacy Incident Handling Guidance.[20] Regularly scheduled risk assessments will be performed on the security controls for security vulnerabilities, including technical, managerial, and physical security access.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics, and other technology.

9.1 What type of project is the program or system?

The CFATS Personnel Surety Program is a specific element of the Infrastructure Security Compliance Project (ISCP), which is a Level 3 IT Program as defined by the DHS Acquisition Instruction/Guidebook #102-01-001 v1.9, issued in November 2008.

9.2 What stage of development is the system in and what project development lifecycle was used?

While ISCP is entering the operations and maintenance stage, the CFATS Personnel Surety Program is in the planning stage of its lifecycle development.

[20] Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The CFATS Personnel Surety Program will not employ technology that raises privacy concerns; rather, it will utilize existing technology for accepting and processing PII and leverages existing processes to conduct checks against the TSDB.

Responsible Official

Todd Klessman
Project Manager, Chemical Facility Anti-Terrorism Standards
Infrastructure Security Compliance Division
Office of Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

(Original signed copy on file with the DHS Privacy Office)

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

ATTACHMENT 1

Affirmations Required by a High-Risk Chemical Facility's Submitter Prior To Submitting Information

Prior to submitting information within CSAT about affected individuals, the Submitter(s) for a high-risk chemical facility must affirm the following statements:

Affirmation of Information Veracity

I affirm that, to the best of my knowledge, the information I am about to submit is true, complete, and correct. I understand that making knowing or willful false statements to the federal government as a part of this information submission is prohibited by federal law.

Affirmation of SSP Compliance

I affirm that, to the best of my knowledge, the collection and submission to the Department of Homeland Security of this information is in compliance with a high-risk chemical facility's Site Security Plan, as authorized or approved under 6 CFR Part 27.

Affirmation of Privacy Act Notice

I affirm that notice has been provided to the affected individuals whose information is being submitted which: (1) notifies those individuals that their information is being submitted to DHS for vetting against the Terrorist Screening Database, and that 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 of Homeland Security to information contained in the Terrorist Screening Database.

ATTACHMENT 2

Sample Notice to Individuals Regarding the Collection of Information

This is a sample notice, which high-risk chemical facilities may choose to use to provide notice to affected individuals. DHS may review notices for adequacy, as appropriate, under CFATS.

(To Be Provided by a High-Risk Chemical Facility's Submitter to Affected Individuals Prior to the Submission of PII to DHS)

The Department of Homeland Security (DHS) requires [INSERT NAME OF CFATS COVERED FACILITY] to collect and submit the personally identifiable information (PII) of: (1) facility personnel (e.g., employees and contractors) with access, or seeking access, (unescorted or otherwise) to restricted areas or critical assets; and (2) unescorted visitors with access, or seeking access, to restricted areas or critical assets, for the purpose of comparing that PII against information pertaining to known and suspected terrorists maintained by the federal government in the Terrorist Screening Database (TSDB).

In certain cases, DHS may require [INSERT NAME OF CFATS COVERED FACILITY] to collect and submit additional information (e.g., visa information) about affected individuals in order to clarify data errors or to resolve potential matches (e.g., in situations where an affected individual has a common name). Such requests will not imply, and should not be construed to indicate, that an individual has been confirmed as a match to the TSDB.

DHS conducts these activities pursuant to section 550 of the Homeland Security Appropriations Act of 2007, and section 27.230(a)(12)(iv) of the Chemical Facility Anti-Terrorism Standards (CFATS).

DHS may share information provided by [INSERT NAME OF CFATS COVERED FACILITY, AND OF THIRD PARTY SUBMITTER (IF APPLICABLE)] about you with law enforcement or intelligence agencies or others under its System of Records Notice published in the Federal Register. To view this System of Records Notice and for more information on DHS privacy policies, please see the DHS Privacy Office website at http://www.dhs.gov/privacy.

DHS may also share your information and information about you with [INSERT NAME OF CFATS COVERED FACILITY, AND OF THIRD PARTY SUBMITTER (IF APPLICABLE)].

ACCESS & CORRECTIONS:

If you would like access to the information provided by [INSERT NAME OF CFATS COVERED FACILITY, AND OF THIRD PARTY SUBMITTER (IF APPLICABLE)], you may contact [INSERT CONTACT NAME & NUMBER OR EXPLAIN INTERNAL PROCEDURE].

If your information contains errors, you should inform [INSERT NAME OF CFATS COVERED FACILITY], which is obligated to correct your information and resubmit it to DHS.

You may also write to the NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380, to obtain access to your information, and if necessary to correct inaccurate or erroneous information. The requirements for filing such a request may be found at 6 CFR §5.21(d) or accessed from the DHS Privacy Office website at http://www.dhs.gov/foia.

Please note that DHS will not make available information about you that was not supplied by [INSERT NAME OF CFATS COVERED FACILITY, AND OF THIRD PARTY SUBMITTER (IF APPLICABLE)], such as TSDB matching results or analyses.

REDRESS:

If you believe that the information submitted by [INSERT NAME OF CFATS COVERED FACILITY AND OF THIRD PARTY SUBMITTER (IF APPLICABLE)] has been improperly matched by DHS to the identity of a known or suspected terrorist, you may write to the NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380. You may also request an administrative adjudication under CFATS.[21]

[21] See 6 CFR 27.310(a)(1).