Privacy Impact Assessment Update
for the

Chemical Facility Anti-Terrorism Standards Personnel Surety Program

DHS/CISA/PIA-018(d)

March 10, 2020

Contact Point
David Wulf
CISA/Infrastructure Security Division/Infrastructure Security Compliance Division
(703) 235-8221

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) / Cybersecurity and Infrastructure Security Agency (CISA) / Infrastructure Security Division (ISD) / 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. This PIA: (1) consolidates the original PIA published in May 2011 along with multiple updates since published, and (2) provides notice that CISA is commencing full implementation of the CFATS Personnel Surety Program at all high-risk chemical facilities, to now include Tier 3 and Tier 4 chemical facilities.

Overview

Section 550 of the Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295 (2006) ("Section 550"), provided the Department with the authority to identify and regulate the security of high-risk chemical facilities using a risk-based approach. On April 9, 2007, the Department issued the CFATS Interim Final Rule (IFR) implementing this statutory mandate.[1]

Section 550 required that the Department establish risk-based performance standards for high-risk chemical facilities, and through the CFATS regulations the Department promulgated 18 Risk-Based Performance Standards (RBPS), including RBPS 12 -- Personnel Surety. Under RBPS 12, high-risk chemical facilities regulated under CFATS are required to account for the conduct of certain types of background checks in their Site Security Plans. Specifically, RBPS 12 requires high-risk chemical facilities to:

> Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including, (i) Measures designed to verify and validate identity; (ii) Measures designed to check criminal history; (iii) Measures designed to verify and validate legal authorization to work; and (iv) Measures designed to identify people with terrorist ties.[2]

The first three aspects of RBPS 12 (checks for identity, criminal history, and legal authorization to work) have already been implemented, and high-risk chemical facilities have addressed these aspects of RBPS 12 in their Site Security Plans. This PIA announces to the public and chemical facilities that CISA is commencing full implementation of the CFATS Personnel

[1] *See* 72 FR 17688.
[2] *See* 6 CFR 27.230(a)(12).

Surety Program at all high-risk chemical facilities, which requires high-risk chemical facilities to implement security measures designed to ensure that certain individuals with or seeking access to the restricted areas or critical assets at those chemical facilities are screened for terrorist ties.

Identifying affected individuals who have terrorist ties is an inherently governmental function and requires the use of information held in government-maintained databases that are unavailable to high-risk chemical facilities.[3] Thus, under RBPS 12(iv), the Department and high-risk chemical facilities must work together to satisfy the "terrorist ties" aspect of the Personnel Surety performance standard. To implement the provisions of RBPS 12(iv), and in accordance with the Homeland Security Act as amended by the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (as amended),[4] the following options are available to enable high-risk chemical facilities to facilitate terrorist-ties vetting of affected individuals.

Options for Compliance with RBPS 12(iv)

Option 1. High-risk chemical facilities may submit certain information about affected individuals that the Department will use to vet those individuals for terrorist ties. Specifically, the identifying information about affected individuals will be compared against identifying information of known or suspected terrorists contained in the Federal Government's consolidated and integrated terrorist watchlist, the Terrorist Screening Database (TSDB), which is maintained by the Department of Justice (DOJ) Federal Bureau of Investigation (FBI) in the Terrorist Screening Center (TSC).[5]

Option 2. High-risk chemical facilities may submit information about affected individuals who already possess certain credentials that rely on security threat assessments conducted by the Department. This will enable the Department to verify the continuing validity of these credentials.

Option 3. High-risk chemical facilities may comply with RBPS 12(iv) without submitting to the Department information about affected individuals who possess Transportation Worker Identification Credentials (TWIC)[6], if a high-risk chemical facility electronically verifies and validates the affected individual's TWICs through the use of TWIC readers (or other technology that is periodically updated using the Canceled Card List[7]).

---

[3] *See* Interim Final Regulations (IFR) for the Chemical Facility Anti-Terrorism Standards Program, 72 FR 17688, 17709 (April 9, 2007).

[4] The CFATS Act of 2014 codified the CFATS program into the Homeland Security Act of 2002. *See* 6 U.S.C. 621 et seq.; *see also* The Chemical Facility Anti-Terrorism Standards Program Extension Act. Pub. L. 116-2 (2019).

[5] For more information about the TSDB, *see* DOJ/FBI-019 Terrorist Screening Records System, 72 FR 47073 (August 22, 2007).

[6] Additional information about the TWIC program may be found at https://www.tsa.gov/for-industry/twic.

[7] The term Canceled Card List (CCL) is defined in a U.S. Coast Guard final rule. CCL is a list of Federal Agency Smart Credential-Numbers (FASC-Ns) that have been invalidated or revoked because TSA has determined that the TWIC-holder may pose a security threat, or the card has been reported lost, stolen, or damaged. For more information

Option 4. High-risk chemical facilities may visually verify certain credentials or documents that are issued by a federal screening program[8] that periodically vets enrolled individuals against the Terrorist Screening Database (TSDB). The Department continues to believe that visual verification has significant security limitations and, accordingly, encourages high-risk chemical facilities choosing this option to identify in their Site Security Plans the means by which they plan to address these limitations.

Who is considered an affected individual?

RBPS 12(iv) requires that certain individuals with or seeking access to restricted areas or critical assets at high-risk chemical facilities be checked for terrorist ties. These individuals are referred to as "affected individuals." Specifically, affected individuals are facility personnel or unescorted visitors with or seeking access to restricted areas or critical assets at high-risk chemical facilities. High-risk facilities may classify particular contractors or categories of contractors either as "facility personnel" or as "visitors." This determination should be a facility-specific determination, and should be based on facility-security considerations, operational requirements, and business practices.

There are also certain groups of persons, which the Department does not consider to be affected individuals, such as (1) federal officials who gain unescorted access to restricted areas or critical assets as part of their official duties; (2) state and local law enforcement officials who gain unescorted access to restricted areas or critical assets as part of their official duties; and (3) emergency responders at the state or local level who gain unescorted access to restricted areas or critical assets during emergency situations.

Overview of Option 1

The first option allows high-risk chemical facilities (or designee(s))[9] to submit certain information about affected individuals to the Department through a Personnel Surety Program application in an online technology system developed under CFATS[10] called the Chemical Security Assessment Tool (CSAT). Access to and the use of CSAT is provided free of charge to high-risk chemical facilities (or their designee(s)).

about the CCL, *see* USCG Final Rule, 81 FR 57651 (August 23, 2016).

[8] Two federal screening programs that meet this statutory threshold are the TWIC and Hazardous Materials Endorsement (HME) program.

[9] A designee is a third-party that submits information about affected individuals to DHS on behalf of a high-risk chemical facility.

[10] *See* DHS/NPPD/PIA-009 Chemical Facility Anti-Terrorism Standards (CFATS), *available at* https://www.dhs.gov/privacy.

Under this option, information about affected individuals submitted by, or on behalf of, high-risk chemical facilities will be compared against identifying information of known or suspected terrorists contained in the TSDB.[11]

If Option 1 is selected by a high-risk chemical facility in its Site Security Plan (SSP), the facility (or its designee(s)) must submit the following information about an affected individual to satisfy RBPS 12(iv):

- For U.S. Persons (U.S. citizens and nationals as well as U.S. lawful permanent residents):
  - Full Name
  - Date of Birth
  - Citizenship or Gender
- For Non-U.S. Persons:
  - Full Name
  - Date of Birth
  - Citizenship
  - Passport information and/or alien registration number

To reduce the likelihood of false positives in matching against records in the Federal Government's consolidated and integrated terrorist watchlist, high-risk chemical facilities (or their designee(s)) are encouraged, but not required, to submit the following optional information about each affected individual:

- Aliases
- Gender (for Non-U.S. Persons)
- Place of Birth
- Redress Number[12]

If a high-risk chemical facility chooses to submit information about an affected individual under Option 1, the following table summarizes the biographic data that would be submitted to the Department.

[11] Detailed information about the submission of information about affected individuals under Option 1 to the Department for vetting purposes via CSAT can be found in the CSAT Personnel Surety Program User Manual available at www.dhs.gov/chemicalsecurity.

[12] For more information about Redress Numbers, *see* http://www.dhs.gov/one-stop-travelers-redress-process#1.

Table 01: Affected Individual Required and Optional Data Under Option 1

Data Elements Submitted to the Department	For a U.S. Person	For a Non-U.S. Person
Full Name	Required	
Date of Birth	Required	
Gender	Must provide Citizenship or Gender	Optional
Citizenship		Required
Passport Information and /or Alien Registration Number	N/A	Required
Aliases	Optional	
Place of Birth	Optional	
Redress Number	Optional	

Overview of Option 2

The second option also allows high-risk chemical facilities (or designee(s)) to submit certain information about affected individuals to the Department through the CSAT Personnel Surety Program application.[13] This option allows high-risk chemical facilities and the Department to take advantage of the vetting for terrorist ties already being conducted on affected individuals enrolled in the TWIC Program, Hazardous Materials Endorsement (HME) Program,[14] as well as the NEXUS, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), Free and Secure Trade (FAST), and Global Entry Trusted Traveler Programs.[15]

Under Option 2, high-risk chemical facilities (or designee(s)) may submit information to the Department about affected individuals possessing the appropriate credentials to enable the Department to electronically verify the affected individuals' enrollments in these other programs. The Department will subsequently notify the Submitter[16] of the high-risk chemical facility whether an affected individual's enrollment in one of these other DHS programs was electronically verified. The Department will also periodically re-verify each affected individual's continued

[13] Detailed information about the submission of information about affected individuals under Option 2 to the Department via CSAT can be found in the CSAT Personnel Surety Program User Manual available on www.dhs.gov/chemicalsecurity.

[14] *See* DHS/TSA/PIA-002 Hazardous Materials Endorsement (HME), available at www.dhs.gov/privacy.

[15] *See* DHS/CBP/PIA-002 Global Enrollment System (GES), *available at* www.dhs.gov/privacy.

[16] A Submitter is a person who is responsible for the submission of information through the CSAT system as required in 6 CFR 27.200(b)(3).

enrollment in one of these other programs, and notify the high-risk chemical facility and/or designee(s) of significant changes in the status of an affected individual's enrollment (e.g., if an affected individual who has been enrolled in the HME Program ceases to be enrolled, then the Department would change the status of the affected individual in the CSAT Personnel Surety Program application and notify the Submitter).[17] Electronic verification and re-verification ensure that both the Department and the high-risk chemical facility can rely upon the continuing validity of an affected individual's credential or endorsement. As a condition of choosing Option 2, a high-risk chemical facility must describe in its SSP what action(s) it, or its designee(s), will take in the event the Department is unable to verify, or no longer able to verify, an affected individual's enrollment in the other DHS program. The high-risk facility must take some action and not leave the situation unresolved.

If Option 2 is selected by a high-risk chemical facility in its SSP, the high-risk chemical facility (or designee(s)) must submit the following information about an affected individual to satisfy RBPS 12(iv):

- Full Name
- Date of Birth
- Program-specific information or credential information, such as unique number, or issuing entity (e.g., State for Commercial Driver's License (CDL) associated with an HME)

To further reduce the potential for misidentification, high-risk chemical facilities (or designee(s)) are encouraged, but not required, to submit the following optional information about affected individuals to the Department:

- Aliases
- Gender
- Place of Birth
- Citizenship

If a high-risk chemical facility chooses to submit information about an affected individual under Option 2, the following table summarizes the biographic data that would be submitted to the Department.

[17] When the Department notifies the Submitter of the high-risk chemical facility of significant changes in the status of an affected individual's enrollment, such a notification should not be construed to indicate that an individual has terrorist ties or be treated as derogatory information.

Table 02: Affected Individual Required and Optional Data Under Option 2

Data Elements Submitted to the Department	For Affected Individual with a TWIC	For Affected Individual with an HME	For Affected Individual Enrolled in a Trusted Traveler Program (NEXUS, SENTRI, FAST, or Global Entry)
Full Name	Required		
Date of Birth	Required		
Expiration Date	Required		
Unique Identifying Number	TWIC Serial Number: Required	CDL Number: Required	PASS ID Number: Required
Issuing State of CDL	N/A	Required	N/A
Aliases	Optional		
Gender	Optional		
Place of Birth	Optional		
Citizenship	Optional		

Overview of Option 3

Under Option 3 – Electronic Verification of TWIC, a high-risk chemical facility (or its designee(s)) will not submit to the Department information about affected individuals in possession of TWICs, but rather will electronically verify and validate the affected individuals' TWICs[18] through the use of TWIC readers (or other technology that is periodically updated with revoked card information). Any high-risk chemical facility that chooses this option must describe in its SSP the process and procedures it will follow if it chooses to use TWIC readers, including what action(s) it, or its designee(s), will take in the event the high-risk chemical facility is unable to verify the TWIC, or subsequently unable to verify an affected individual's TWIC. For example, if a TWIC cannot be verified through the use of a TWIC Reader, the high-risk chemical facility may choose to verify the affected individual's enrollment in TWIC under Option 2, or submit information about the affected individual under Option 1.

[18] Electronic verification and validation of an affected individual's TWIC means that the affected individual's TWIC (1) is a valid credential issued by TSA, and (2) has not been cancelled by the TSA, and (3) the TWIC is the affected individual's TWIC.

Overview of Option 4

Option 4 – Visual Verification of Credentials Conducting Periodic Vetting complies with section 2102(d)(2) of the Homeland Security Act and allows a high-risk chemical facility to satisfy its obligation under 6 CFR § 27.230(a)(12)(iv) to identify individuals with terrorist ties using any federal screening program that periodically vets individuals against the TSDB if:

- The federal screening program issues a credential or document,[19]
- The high-risk chemical facility is presented[20] a credential or document by the affected individual,[21] and
- The high-risk chemical facility verifies the credential or document is current in accordance with its SSP.[22]

As a result, a high-risk chemical facility may verify that a credential or document is current based upon visual inspection, if the processes for conducting such visual inspections are described in its SSP. When developing such processes, the Department encourages high-risk chemical facilities to consider any rules, processes, and procedures prescribed by the entity issuing the credential or document. The Department believes that visual verification has inherent limitations and provides less security value than the other options available under the CFATS Personnel Surety Program. The Department encourages every high-risk chemical facility to consider a means of verification that is consistent with its specific circumstances and its assessment of the threat posed by the acceptance of such credentials. If a facility chooses to use Option 4, in whole or in part, it should also identify in its Site Security Plan the means by which it plans to address these limitations.

Under the CFATS program, Congress required the Department to establish RBPS for high-risk chemical facilities. DHS promulgated 18 RBPS under CFATS, including RBPS 12 – Personnel Surety, which requires high-risk chemical facilities to perform appropriate background checks on, and ensure appropriate credentials for, facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets.[23]

---

[19] This requirement is derived from section 2102(d)(2)(B)(i) of the Homeland Security Act.

[20] The Department considers records of credentials or documents maintained by the high-risk chemical facility, or designee, as having been presented by the affected individual. For example, if high-risk chemical facility (or designee) has in its personnel or access control files a photocopy of an affected individual's CDL with an HME, the high-risk chemical facility may consider the copy in its files as having been presented by the affected individual.

[21] Section 2102(d)(2)(B)(i)(II)(aa) of the Homeland Security Act requires high-risk chemical facilities to accept the credential or document from any federal screening program that conducts periodic vetting against the TSDB. Under Option 4, a high-risk chemical facility may contact the Department when drafting its SSP to determine if a specific credential or document is from a federal screening program that conducts periodic vetting against the TSDB.

[22] This requirement is derived from section 2102(d)(2)(B)(i)(II)(bb) of the Homeland Security Act.

[23] *See* 6 CFR 27.230(a)(12).

The CFATS Personnel Surety Program provides the capability for high-risk chemical facilities to meet the RBPS 12 – Personnel Surety requirements by ensuring that all affected individuals[24] are recurrently vetted against the Federal Bureau of Investigation's (FBI) Terrorist Screening Database (TSDB).[25]

This PIA consolidates the original PIA published in May 2011 and its subsequent updates. This PIA also provides notice that CISA is commencing full implementation of the CFATS Personnel Surety Program at all high-risk chemical facilities, whereas previously the program was limited to only high-risk chemical facilities designated at the two highest risk tiers (Tier 1 and Tier 2).[26]

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Section 550 of the Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295 (2006) ("Section 550"), provided the Department with the authority to identify and regulate the security of high-risk chemical facilities using a risk-based approach. On April 9, 2007, the Department issued the CFATS Interim Final Rule (IFR) implementing this statutory mandate.[27]

Section 550 required that the Department establish risk-based performance standards for high-risk chemical facilities, and through the CFATS regulations the Department promulgated 18 RBPSs, including RBPS 12 -- Personnel Surety. Under RBPS 12, high-risk chemical facilities regulated under CFATS are required to account for the conduct of certain types of background checks in their Site Security Plans. Specifically, RBPS 12 requires high-risk chemical facilities to:

> Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including, (i) Measures designed to verify and validate identity; (ii) Measures designed to check criminal history; (iii) Measures designed to verify and

[24] Affected individuals are individuals that are subject to screening for terrorist ties under the CFATS program. These individuals are: (1) facility personnel who have or are seeking access, either unescorted or otherwise, to restricted areas or critical assets; or (2) unescorted visitors who have or are seeking access to restricted areas or critical assets. Individual high-risk facilities may choose to classify contractors as either "facility personnel" or as "visitors." This is a facility-specific determination and is based on individual facility security protocols, operational requirements, and business practices.

[25] *See* DOJ/FBI – 019 Terrorist Screening Records System, 72 FR 47073 (August 22, 2007).

[26] An overview of the risk-tiering methodology that CISA uses for chemical facilities that possess or plan to possess chemicals of interest to identify a facility's specific level of risk can be viewed here: https://www.cisa.gov/publication/cfats-tiering-methodology-fact-sheet.

[27] *See* 72 FR 17688.

validate legal authorization to work; and (iv) Measures designed to identify people with terrorist ties.[28]

On December 18, 2014, the President signed into law the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (also referred to as "the CFATS Act of 2014").[29] The CFATS Act of 2014 reauthorized the CFATS program for four years and added provisions related to CFATS to the Homeland Security Act of 2002, as amended.[30] These amendments to the Homeland Security Act of 2002 affirmed that the Department must implement a Personnel Surety Program for high-risk chemical facilities to comply with Risk- Based Performance Standard (RBPS) 12(iv) of CFATS.[31] On January 18, 2019, the President signed into law the CFATS Program Extension Act, extending the program for 15 months through April 2020.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The Department published the initial CFATS Personnel Surety Program SORN on June 14, 2011.[32] The Department published a revised SORN on June 18, 2014.[33]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

CSAT is certified and accredited at the sensitive but unclassified level per National Institute Standards & Technology (NIST) 800-53 specifications and DHS policy and guidance, including DHS Sensitive System Policy Directive 4300A. The CISA CIO granted an Authorization to Operate (ATO) for two years on July 10, 2018, with an expiration date of July 10, 2020.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

A NARA Records Retention Schedule is being developed for the CFATS Personnel Surety Program.

---

[28] See 6 CFR 27.230(a)(12)

[29] Pub. L. No. 113-254.

[30] The CFATS Act of 2014 codified the CFATS program into the Homeland Security Act of 2002. See 6 U.S.C. 621 et seq.; see also The Chemical Facility Anti-Terrorism Standards Program Extension Act. Pub. L. 116-2 (2019).

[31] The specific requirement of RBPS 12(iv) is found at 6 CFR 27.230(a)(12)(iv).

[32] DHS/NPPD-002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records, 76 FR 34732 (June 14, 2011).

[33] DHS/NPPD-002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records, 79 FR 28752 (May 19, 2014).

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected by the Department under the CFATS Personnel Surety Program is covered by the CFATS Personnel Surety Information Collection under 1670-0029.[34]

Section 2.0 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.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

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

If an affected individual is a non-U.S. person, CISA 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-issued redress number.

CISA 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.

CISA may collect information to verify that an individual is currently enrolled in a DHS program which includes a TSDB check equivalent[35] to the TSDB vetting performed as part of the

[34] The CFATS Personnel Surety Program Information Collection was initially approved by OMB in August 2015 and was limited to Tier 1 and Tier 2 high-risk chemical facilities. The Department submitted the subsequent Information Collection Request in August 2018. OMB approved the Information Collection Request on May 23, 2019. The approved Information Collection and the accompanying Notice of Action may be viewed at https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201806-1670-001.

[35] This is a term of art designated by DHS Screening Coordination Office at the start of the CFATS PS program to cover the variety of methods by which DHS conducts vetting against the TSDB. Each DHS component conducts 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. CISA 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.

CISA 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 in the previous paragraph; 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.

CISA 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, CISA may request information previously submitted to CISA about affected individuals from the high-risk chemical facilities to confirm its accuracy.

In addition, CISA 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, CISA 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.[36]

CISA 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.

vetting differently, but level of scrutiny is equivalent.

[36] *See* 6 CFR 27.300 – 6 CFR 27.345.

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.

2.2 What are the sources of the information and how is the information collected for the project?

High-risk chemical facilities will collect information about affected individuals and submit the individuals' information to CISA through CSAT, the secure web-based application maintained by CISA. 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 CISA on behalf of a facility. Each high-risk chemical facility will be responsible for ensuring that its submitter(s) appropriately provides proper information pertaining to affected individuals to CISA for vetting.

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

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

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

2.4 Discuss how accuracy of the data is ensured.

High-risk chemical facilities will be responsible for the accuracy of PII submitted to CISA. 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.[37] CISA 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.

Further, TSA will forward the results from potential TSDB matches to the FBI's TSC, which will then determine whether an individual's information is a match to a TSDB record. In certain instances, CISA may contact a high-risk chemical facility if additional information is

[37] *See* Attachment 1.

needed on an affected individual in order to resolve a potential match (e.g., in situations in which 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 are encouraged 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.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

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 CISA as part of the CFATS Personnel Surety Program.

Mitigation: CISA will seeks 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). CISA further mitigates the risk of misidentification by requiring Submitters to certify the accuracy, to the best of their knowledge, of the PII submitted to CISA.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

CISA 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 CISA may be used to facilitate operational, law enforcement, or intelligence responses, if appropriate, when affected individuals' identities match identities contained in the TSDB.

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

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

CISA 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.[38]

CISA 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.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

CISA will not use technology to conduct searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

Individuals in other DHS components are not assigned roles or have responsibilities within the CSAT Personnel Surety application.

The CSAT Personnel Surety application does exchange information with the Consolidated Screening Gateway, a system owned by TSA to 1) check for terrorist ties under Option 1, and 2) verify enrollment in the HME Program under Option 2.[39]

The CSAT Personnel Surety application does exchange information with Technology Infrastructure Modernization (TIM) Program, a system owned by TSA to verify enrollment in the TWIC Program under Option 2.[40]

---

[38] *See* 6 CFR 27.300 – 6 CFR § 27.345.

[39] *See* DHS/TSA/PIA-001 Vetter and Credentialing Screening Gateway System, *available at* https://www.dhs.gov/privacy.

[40] *See* DHS/TSA/PIA-042 TSA OIA Technology Infrastructure Modernization Program, *available at* https://www.dhs.gov/privacy.

The CSAT Personnel Surety application does exchange information with Global Enrollment Program (GEP), a system owned by CBP to verify enrollment in the NEXUS, SENTRI, and Trusted Traveler Programs under Option 2.[41]

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk of inappropriate use of the PII collected.

Mitigation: The risk is mitigated. PII collected by CISA 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. Because CSAT is the repository for PII submitted on affected individuals, as part of its technical safeguards, CSAT will employ role-based access controls and audit logging, to control and monitor the use of PII. Furthermore, all CISA 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 inappropriately used.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

High-risk chemical facilities and their designees are required to provide notice to affected individuals prior to any PII being submitted to CISA. The notice will 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, CISA 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. CISA 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

[41] *See* DHS/CBP/PIA-002 Global Enrollment System (GES), *available at* https://www.dhs.gov/privacy.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals may decline to provide information; however, the individual may impact a high-risk chemical facility's compliance with CFATS. CISA 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 CISA directly.

CISA will not regulate the relationships between high-risk chemical facilities and affected individuals. CISA, 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 CISA under the CFATS Personnel Surety Program.

After attempts to work with the facility, CISA may disapprove the SSPs of high-risk chemical facilities that fail to include provisions for participation in the CFATS Personnel Surety Program. Further, CISA 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.

4.3 Privacy Impact Analysis: Related to Notice

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

Mitigation: The risk is mitigated. Prior to submitting the PII of affected individuals to CISA, 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 CISA 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 CISA for the completion of the vetting process.

CISA has made available to high-risk chemical facilities a sample notice that complies with subsection (e)(3) of the Privacy Act, 5 U.S.C. 552a(e)(3). This notice provides information about access, correction, and redress to affected individuals.[42]

By providing a sample notice to high-risk chemical facilities, CISA 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.

[42] *See* Attachment 2.

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.

CISA has also provided notice through publication of a SORN[43] for the CFATS Personnel Surety Program.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

A proposed schedule for the retention and disposal of records collected under the DHS/NPPD-002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records is being developed by CISA for approval by NARA. Until approval is received by NARA for the records retention and disposition schedule, all CFATS Personnel Surety Records must be retained permanently. Once the schedule is approved by NARA, the records will be retained in accordance with the records schedule, and that proposed schedule is as follows:

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

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

2) Information pertaining to an individual who may originally have appeared to be a match 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 CISA that the individual no longer has or is seeking access to the restricted areas or critical assets of the facility, whichever is later; and

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

[43] *See* DHS/NPPD-002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records, 79 FR 28752 (May 19, 2014).

TSA 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 Trusted and Registered Traveler Programs.

CISA will also retain records to conduct inspections or audits in accordance to the CFATS Act of 2014, 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 the names of individuals with access to high-risk chemical facilities' restricted areas and critical assets, the periods of time during which high-risk chemical facilities indicate that such individuals have/had access, and any other information listed elsewhere in this notice, as appropriate.

The retention periods, described in the three categories above, for these records provide reasonable amounts of time for law enforcement, intelligence, or redress matters involving individuals who have or are seeking access to restricted areas or critical assets at high-risk chemical facilities.

5.2 Privacy Impact Analysis: Related to Retention

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: The risk is partially mitigated. The CFATS Act of 2014 precludes the Department from requiring that high-risk chemical facilities update records about affected individuals in the CSAT Personnel Surety Application. As a result, notice and transparency continue to be the Department's most valuable tools for encouraging the maintenance of accurate and relevant information under the Personnel Surety Program. CISA strongly encourages high-risk chemical facilities to notify CISA when an affected individual no longer has access to restricted areas or critical assets to ensure the accuracy of CISA's data and to stop the recurrent vetting on the person who is no longer an affected individual. Some past and present actions taken by the Department in an effort to mitigate risk using notice and transparency include: providing publicly available program documentation, particularly the Privacy Impact Assessment and subsequent updates, to provide notice to the public of the potential privacy risks associated with the Personnel Surety Program. The Department also issued communications to facilities that have been re-tiered, advising them that they may voluntarily update their records in CSAT. Updated and accurate records in CSAT may help to alleviate privacy concerns as well as limit costs incurred by the Department by reducing the number of individuals being unnecessarily vetted against the TSDB.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

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

CISA may externally share PII, matching analyses, and vetting results for appropriate action by federal law enforcement and intelligence agencies. CISA will also share information with the TSC, which maintains the Federal Government's consolidated and integrated terrorist watchlist (the TSDB).[44]

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The purpose of the CFATS Personnel Surety Program is to require that regulated chemical facilities implement measures designed to identify individuals with terrorist ties. The CFATS Personnel Surety Program shares information to determine if an affected individual's PII matches PII contained in the TSDB. CISA only collects and shares information for this program for that purpose.

6.3 Does the project place limitations on re-dissemination?

The CFATS Personnel Surety Program does not place any program specific limitations on re-dissemination.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

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. CISA will maintain a record when PII is shared externally from DHS.

[44] The TSC shares information in accordance with the routine uses in the Terrorist Screening Records System, Justice/FBI-019 SORN. See the amendment to the Federal Bureau of Investigation's Terrorist Screening Records System72 FR 47073 (August 22, 2007).

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: The risk is mitigated. 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 which 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,[45] E-Government Act,[46] and FISMA,[47] as appropriate.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

The CFATS Act of 2014 prohibits the Department from requiring high-risk chemical facilities to provide updated information about an affected individual by stating that high-risk chemical facilities only have to submit information about an affected individual to the Department one time. Although the Department continues to strongly encourage high-risk chemical facilities to update records as appropriate, it is important that individuals are made aware that they are able to contact the Department directly in the event that a high-risk chemical facility does not, or cannot provide updated information to the Department. Procedures for accessing and/or correcting information are described below and are found in DHS/NPPD-002 CFATS Personnel Surety Program System of Records.[48]

---

[45] *See* https://www.justice.gov/opcl/privacy-act-1974.

[46] *See* https://www.justice.gov/opcl/e-government-act-2002.

[47] *See* https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

[48] *See* DHS/NPPD-002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records, 79 FR 28752 (May 19, 2014).

7.1 What are the procedures that allow individuals to access 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. While any individual can submit a FOIA request, the Privacy Act only applies to U.S. Persons. FOIA/PA requests may be sent to the following address:

CISA FOIA Officer

245 Murray Lane, SW

Washington, D.C. 20528-0380

Additional information about Privacy Act/FOIA requests for CISA records is available at http://www.dhs.gov/xfoia/editorial_0316.shtm.

7.2 What procedures are in place to allow the subject individual to correct 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 CISA FOIA Officer at the address listed in Section 7.1 to have inaccurate or erroneous PII corrected.

7.3 How does the project notify individuals about the procedures for correcting their information?

As part of the CFATS Personnel Surety Program's notice requirements,[49] 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.

7.4 Privacy Impact Analysis: Related to Redress

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.

[49] See Section 4.0, above.

Mitigation: This risk is 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 CISA. CSAT, the system used to submit affected individuals' PII to CISA, require Submitters to check a box affirming that notification has been provided before each record can be transmitted to CISA. Furthermore CISA may conduct additional evaluation on a facility's notification procedures, as appropriate, under CFATS.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CISA 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.[50] CFATS Personnel Surety Program personnel will adhere to established internal information security policies, as well as those outlined in CISA information technology security documents. Periodic audits and evaluations will ensure continued compliance with CISA security and privacy requirements, including those that cover the internal sharing of PII.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All personnel granted access to the PII will have a confirmed need to know the information to perform their duties and are authorized to handle information collected by CISA under the CFATS Personnel Surety Program. These individuals will be required to complete DHS privacy training on at least an annual basis.

[50] Available at https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Upon notification from the Department, facilities will access the CSAT Personnel Surety application through CSAT using their existing usernames and passwords.[51] Within the CSAT Personnel Surety application, there are two mechanisms to add user accounts. The first method is to invite an existing CSAT user to an assigned role and the second is to create an account for a new user who currently does not have a CSAT account. User accounts are only created for individuals responsible for adding affected individuals (Authorizers and Personal Surety (PS) Submitters) in the CSAT Personnel Surety application.

User Roles and Responsibilities

There are two roles to which users are assigned in the CSAT Personnel Surety application: Authorizer and PS Submitter. These user roles have been established within the CSAT Personnel Surety application to ensure access control regarding the submission of information about affected individuals. The Authorizer can submit information about affected individuals, create and manage groups, and add or remove PS Submitters. The Authorizer is able to view, edit, and input data pertaining to all users under his/her purview within the system. The PS Submitter role is created by Authorizers and can be held by high-risk chemical facility employees or third-party individuals (vendors, contractors, etc.). PS Submitters can enter information about affected individuals and are only able to view information about affected individuals that they have submitted in the system.

Managing Groups

The Department provides high-risk chemical facilities with wide latitude in assigning user roles to align with their business operations and the business operations of third parties that provide services to facilities. The CSAT Personnel Surety application allows Authorizers to assign employees and third-party designees to submit information about affected individuals directly to the Department on behalf of high-risk chemical facilities. This flexibility provides high-risk chemical facilities the ability to create groups that directly align with their business structure. The group structure also ensures access control so that PS Submitters are only able to view affected individuals' data within their assigned group(s). Only individuals assigned to the corporate group are able to see affected individuals' data submitted under other groups. An individual must be a facility employee to be assigned to the corporate group. For further information about group structure and managing groups, reference the CSAT Personnel Surety Application User Guide.[52]

---

[51] *See* DHS/NPPD/PIA-009 Chemical Facility Anti-Terrorism Standards (CFATS), *available at* https://www.dhs.gov/privacy.

[52] *See* www.dhs.gov/chemicalsecurity.

Web Service

The Department offers a web service to high-risk chemical facilities (or their designee(s)) as an option for submitting information about affected individuals. The web service consists of a direct connection through which affected individual data can be transmitted from a high-risk chemical facility to the Department's CSAT Personnel Surety application. The web service provides high-risk chemical facilities with an automated process for submitting information to the Department in an effort to minimize the burden on high-risk chemical facilities.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All MOUs are reviewed by the component program manager, component Privacy Officer, and component counsel and then sent to DHS HQ for formal review.

Responsible Officials

David Wulf
Director, Infrastructure Security Compliance Division
Infrastructure Security Division
Cybersecurity and Infrastructure Security Agency

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting 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 Privacy Act Notice to Individuals Regarding a High-Risk Chemical Facility's Compliance with 6 CFR § 27.230(a)(12)(iv) and Participation in the CFATS Personnel Surety Program.

This is a sample Privacy Act notice, which high-risk chemical facilities or their designee(s) may choose to use to provide required notice to affected individuals. DHS may review notices for adequacy, as appropriate, under CFATS. This updated notice replaces the sample notice that was published as Attachment 1 in the previous PIA on May 1, 2014.

(To be provided by a high-risk chemical facility to affected individuals prior to the submission of PII to DHS under Option 1 and Option 2 for purposes of compliance with 6 CFR § 27.230(a)(12)(iv))

The Department of Homeland Security (DHS) requires [INSERT NAME OF CFATS COVERED FACILITY] to comply with DHS Chemical Facility Anti-Terrorism Standards (CFATS) program requirements to identify affected individuals with terrorist ties. [INSERT NAME OF CFATS COVERED FACILITY] has opted to comply with this requirement by collecting and submitting the personally identifiable information (PII) of affected individuals to DHS 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). Affected individuals are: (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. Affected individuals will undergo recurrent vetting against the TSDB.

In certain cases, DHS may request that [INSERT NAME OF CFATS COVERED FACILITY] 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 a situation in which an affected individual has a common name, additional information could assist DHS in distinguishing that individual from known or suspected terrorists with similar names). 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 CFATS Personnel Surety Program activities pursuant to section 2102 of the Homeland Security Act of 2002, 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 THEIR DESIGNEE(S) (IF APPLICABLE)] about you with law enforcement or intelligence agencies under its Privacy Act System of Records Notice published in the Federal

Register. To view this System of Records Notice (Department of Homeland Security/National Protection and Programs Directorate-002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records) 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 THEIR DESIGNEE(S) (IF APPLICABLE)]. Please note that DHS will not make available certain information about you that was not supplied by [INSERT NAME OF CFATS COVERED FACILITY, AND THEIR DESIGNEE(S) (IF APPLICABLE)], but may provide credential status to [INSERT NAME OF CFATS COVERED FACILITY, AND THEIR DESIGNEE(S) (IF APPLICABLE)] for affected individuals whose information was submitted by them to electronically verify and validate enrollment in a Trusted Traveler Program, the HME Program, or the TWIC Program.

ACCESS & CORRECTIONS:

If you would like access to the information provided by [INSERT NAME OF CFATS COVERED FACILITY, AND THEIR DESIGNEE(S) (IF APPLICABLE)] about you, 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]. If [INSERT NAME OF CFATS COVERED FACILITY, AND THEIR DESIGNEE(S) (IF APPLICABLE)] is either unable or unwilling to update or correct your information, you may also write to the CISA Freedom of Information Act (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.

REDRESS:

If you believe that the information submitted by [INSERT NAME OF CFATS COVERED FACILITY AND OF THEIR DESIGNEE(S) (IF APPLICABLE)] has been improperly matched by DHS to the identity of a known or suspected terrorist, you may write to the CISA FOIA Officer at 245 Murray Lane SW, Washington, D.C. 20528-0380. You may also request an administrative adjudication under CFATS.[53]

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

ATTACHMENT 3

Sample Notice to an Individual Whose Credential Is Being Verified For Purposes of Compliance with 6 CFR § 27.230(a)(12)(iv) and Participation in the CFATS Personnel Surety Program

Prior to verifying an affected individual's credential or document for purposes of compliance with 6 CFR § 27.230(a)(12)(iv), a high-risk chemical facility should provide notice to affected individuals informing them that their credential or document will now be used for compliance with 6 CFR § 27.230(a)(12)(iv).

(To be provided by a high-risk chemical facility to affected individuals prior to verifying an affected individual's credential under Option 3 and Option 4 for purposes of compliance with 6 CFR § 27.230(a)(12)(iv))

Notice to individuals regarding the use of [INSERT CREDENTIAL OR DOCUMENT] under the Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program:

The Department of Homeland Security (DHS) requires [INSERT NAME OF CFATS COVERED FACILITY] to comply with the DHS Chemical Facility Anti-Terrorism Standards (CFATS) program requirement to identify affected individuals with terrorist ties. [INSERT NAME OF CFATS COVERED FACILITY] has opted to comply with this requirement by verifying [INSERT CREDENTIAL OR DOCUMENT]. Affected individuals are: (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. If your [INSERT CREDENTIAL OR DOCUMENT] is successfully verified, no information about you will be submitted to DHS under the CFATS Personnel Surety Program. If your [INSERT CREDENTIAL OR DOCUMENT] cannot be successfully verified, [INSERT NAME OF CFATS COVERED FACILITY] will [DESCRIBE THE PROCEDURES THAT THE FACILITY HAS AGREED TO UNDERTAKE IN ITS ASP OR SSP IN THIS SITUATION].

DHS conducts CFATS Personnel Surety Program activities pursuant to section 2102 of the Homeland Security Act of 2002, and section 27.230(a)(12)(iv) of CFATS.