



**DEPARTMENT OF HOMELAND SECURITY**

Chemical Facility Anti-Terrorism Standards Personnel Surety  
Program Implementation Notice

**AGENCY:** Cybersecurity and Infrastructure Security Agency  
(CISA), Department of Homeland Security (DHS).

**ACTION:** Notice Implementing the CFATS Personnel Surety  
Program at All High-risk Chemical Facilities.

**SUMMARY:** CISA is providing notice to the public and  
chemical facilities regulated under the Chemical Facility  
Anti-Terrorism Standards (CFATS) that it is commencing full  
implementation of the CFATS Personnel Surety Program at all  
high-risk chemical facilities. CFATS requires regulated  
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. The  
CFATS Personnel Surety Program enables regulated chemical  
facilities to meet this requirement.

**DATES:** This notice is applicable [**INSERT DATE OF  
PUBLICATION IN THE *FEDERAL REGISTER***].

**SUPPLEMENTARY INFORMATION:**

**TABLE OF CONTENTS**

- I. Notice of Full Implementation
- II. Statutory and Regulatory History of the CFATS Personnel Surety Program
- III. Contents and Requirements of the CFATS Personnel Surety Program
  - A. Who must be Checked for Terrorist Ties?
  - B. Checking for Terrorist Ties during an Emergency or Exigent Situation
  - C. High-Risk Chemical Facilities have Flexibility when Implementing the CFATS Personnel Surety Program
  - D. Options Available to High-Risk Chemical Facilities to Comply with RBPS 12(iv)
  - E. High-Risk Chemical Facilities may Use More Than One Option
  - F. High-Risk Chemical Facilities may Propose Additional Options
  - G. Security Considerations for High-risk Chemical Facilities to Weigh in Selecting Options
  - H. When the Check for Terrorist Ties must be Completed

IV. Additional Details about Option 1 and Option 2 (Which Involve the Submission of Information to CISA)

- A. Submission of a New Affected Individual's Information under Option 1 or Option 2
- B. Updates & Corrections to Information about Affected Individuals under Option 1 or Option 2
- C. Notification that an Affected Individual No Longer Has Access under Option 1 or Option 2
- D. What/Who is the Source of the Information under Option 1 and Option 2

V. CSAT User Roles and Responsibilities

VI. Privacy Considerations

- A. Privacy Act Requirements to Enable Option 1 and Option 2
- B. Redress
- C. Additional Privacy Considerations Related to Option 1 and Option 2
- D. Additional Privacy Considerations for Option 3 and Option 4

VII. Information a High-Risk Chemical Facility may Wish to Consider Including in its SSP

**I. NOTICE OF FULL IMPLEMENTATION**

CISA is publishing this notice to inform high-risk chemical facilities, in particular Tier 3 and Tier 4

facilities, regulated under CFATS of the full implementation of the CFATS Personnel Surety Program at all high-risk chemical facilities. CISA has previously implemented the Personnel Surety Program at Tier 1 and 2 facilities.<sup>1</sup> CISA will now implement the program in a phased manner at all high-risk chemical facilities, to include Tier 3 and 4 facilities.<sup>2</sup> High-risk chemical facilities will be individually notified when to begin implementing risk based performance standard (RBPS) 12(iv) in accordance with its Site Security Plan (SSP).<sup>3</sup> High-risk chemical facilities at which the CFATS Personnel Surety Program is already implemented are unaffected by this notice.

**II. STATUTORY AND REGULATORY HISTORY OF THE CFATS PERSONNEL SURETY PROGRAM**

Section 550 of the Department of Homeland Security

---

<sup>1</sup> On December 18, 2015 at 80 FR 79058, the Department published the initial implementation notice for the CFATS Personnel Surety Program. The initial implementation was limited to Tier 1 and Tier 2 high-risk chemical facilities. The initial implementation notice may be viewed at <https://www.federalregister.gov/d/2015-31625>.

<sup>2</sup> CISA is implementing in a phased manner based upon its experience implementing the CFATS Personnel Surety Program at Tier 1 and Tier 2 facilities, requests by commenters to the 60-day PRA notice and 30-day notice, and the terms of clearance within the Notice of Action issued by OMB when it approved the CFATS Personnel Surety Program Information Collection Request in May of 2019.

<sup>3</sup> Throughout this notice any reference to SSPs also refers to Alternative Security Programs submitted by high-risk chemical facilities as described in 6 CFR 27.235.

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. 72 FR 17688.

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 validate legal authorization to work; and (iv) Measures designed

to identify people with terrorist ties[.]6 CFR 27.230(a) (12).

The first three aspects of RBPS 12 (checks for identity, criminal history, and legal authorization to work) have already been implemented, and all high-risk chemical facilities have addressed these aspects of RBPS 12 in their Site Security Plans. This notice announces to the public and chemical facilities that it is commencing full implementation of the CFATS Personnel 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. 72 FR 17688, 17709 (April 9, 2007). Thus, under RBPS 12(iv), CISA 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 Title XXI of the Homeland Security Act of 2002, as amended<sup>4</sup>, the following options will be available to enable high-risk chemical facilities to facilitate terrorist-ties vetting of affected individuals.

Option 1. High-risk chemical facilities may submit certain information about affected individuals that CISA 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).<sup>5</sup>

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. See 72 FR 17688, 17709 (April 9, 2007). This will enable CISA to verify the

---

<sup>4</sup> 6 U.S.C. 621 et seq.

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

continuing validity of these credentials.

Option 3. High-risk chemical facilities may comply with RBPS 12(iv) without submitting to CISA information about affected individuals who possess Transportation Worker Identification Credentials (TWICs), 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).

Option 4. High-risk chemical facilities may visually verify certain credentials or documents that are issued by a Federal screening program that periodically vets enrolled individuals against the Terrorist Screening Database (TSDB). CISA 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.

Each of these options is described in further detail below in Section III.D.

### **III. CONTENTS AND REQUIREMENTS OF THE CFATS PERSONNEL SURETY PROGRAM**

The CFATS Personnel Surety Program enables CISA and high-risk chemical facilities to mitigate the risk that



certain individuals with or seeking access to restricted areas or critical assets at high-risk chemical facilities may have terrorist ties.

**A. WHO MUST BE CHECKED FOR TERRORIST TIES?**

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 CISA 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.

**B. CHECKING FOR TERRORIST TIES DURING AN EMERGENCY OR EXIGENT SITUATION**

In some emergency or exigent situations, access to restricted areas or critical assets by other individuals who have not had appropriate background checks under RBPS 12 may be necessary. For example, emergency responders who are not emergency responders at the state or local level may require such access as part of their official duties under appropriate circumstances. If high-risk chemical facilities anticipate that an individual will require access to restricted areas or critical assets without visitor escorts or without the background checks listed in RBPS 12 under exceptional circumstances (e.g., foreseeable but unpredictable circumstances), high-risk chemical facilities may describe such situations and the types of individuals who might require access in those situations in their SSPs. CISA will assess the situations described, and any security measures the high-risk chemical facility plans to take to mitigate vulnerabilities presented by these situations, as it reviews each high-risk chemical facility's SSP.

**C. HIGH-RISK CHEMICAL FACILITIES HAVE FLEXIBILITY WHEN  
IMPLEMENTING THE CFATS PERSONNEL SURETY PROGRAM**

A high-risk chemical facility will have flexibility to tailor its implementation of the CFATS Personnel Surety Program to fit its individual circumstances and, in this regard, to best balance who qualifies as an affected individual, unique security issues, costs, and burden. For example a high-risk chemical facility may, in its Site Security Plan:

- Restrict the numbers and types of persons allowed to access its restricted areas and critical assets, thus limiting the number of persons who will need to be checked for terrorist ties.
- Define its restricted areas and critical assets, thus potentially limiting the number of persons who will need to be checked for terrorist ties.
- Choose to escort visitors accessing restricted areas and critical assets in lieu of performing terrorist ties background checks under the CFATS Personnel Surety Program. The high-risk chemical facility may propose in its SSP traditional escorting solutions and/or innovative escorting alternatives such as video monitoring (which may

reduce facility security costs), as appropriate, to address the unique security risks present at the facility.

**D. OPTIONS AVAILABLE TO HIGH-RISK CHEMICAL FACILITIES TO COMPLY WITH RBPS 12 (IV)**

CISA has developed a CFATS Personnel Surety Program that provides high-risk chemical facilities several options to comply with RBPS 12 (iv). In addition to the alternatives expressly described in this notice, CISA will also permit high-risk chemical facilities to propose alternative measures for terrorist ties identification in their SSPs, which CISA will consider on a case-by-case basis in evaluating high-risk chemical facilities' SSPs. Of note, and as discussed further below, a high-risk chemical facility may choose one option or a combination of options to comply with RBPS 12 (iv).

**OVERVIEW OF OPTION 1**

The first option allows high-risk chemical facilities (or designee(s))<sup>6</sup> to submit certain information about affected individuals to CISA through a Personnel Surety Program application in an online technology system

---

<sup>6</sup> A designee is a third party that submits information about affected individuals to CISA on behalf of a high-risk chemical facility.

developed under CFATS 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)).

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.<sup>7</sup>

If Option 1 is selected by a high-risk chemical facility in its 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

---

<sup>7</sup> 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 on [www.dhs.gov/chemicalsecurity](http://www.dhs.gov/chemicalsecurity).

- o Date of Birth
- o Citizenship
- o 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<sup>8</sup>

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 CISA.

---

<sup>8</sup> For more information about Redress Numbers, please go to <http://www.dhs.gov/one-stop-travelers-redress-process#1>.

**Table 01: Affected Individual Required and Optional**

**Data Under Option 1**

<b>Data Elements Submitted to CISA</b>	<b>For A U.S. Person</b>	<b>For A Non-U.S. Person</b>
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 CISA through a Personnel Surety Program application.<sup>9</sup> This option allows high-risk chemical facilities and CISA 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, as well as the NEXUS, Secure Electronic Network for Travelers Rapid

---

<sup>9</sup> 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](http://www.dhs.gov/chemicalsecurity).

Inspection (SENTRI), Free and Secure Trade (FAST), and Global Entry Trusted Traveler Programs.

Under Option 2, high-risk chemical facilities (or designee(s)) may submit information to CISA about affected individuals possessing the appropriate credentials to enable CISA to electronically verify the affected individuals' enrollments in these other programs. CISA will subsequently notify the Submitter<sup>10</sup> of the high-risk chemical facility whether or not an affected individual's enrollment in one of these other DHS programs was electronically verified. CISA will also periodically re-verify each affected individual's continued 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 CISA would change the status of the affected individual in the CSAT Personnel Surety Program application and notify the Submitter).<sup>11</sup>

---

<sup>10</sup> 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).

<sup>11</sup> 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.



Electronic verification and re-verification ensure that both CISA 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 CISA 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; and
- 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 CISA:

- 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 CISA.

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

<b>Data Elements Submitted to CISA</b>	<b>For Affected Individual with a TWIC</b>	<b>For Affected Individual with an HME</b>	<b>For Affected Individual Enrolled in a Trusted Traveler Program (NEXUS, SENTRI, FAST, or Global Entry)</b>
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 CISA information about affected individuals in possession of TWICs, but rather will electronically verify and validate the affected individuals' TWICs<sup>12</sup> 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.

---

<sup>12</sup> Electronic verification and validation of an affected individual's TWIC requires authentication 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 biometric live sample matches the biometric template on the 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,<sup>13</sup>
- The high-risk chemical facility is presented<sup>14</sup> a credential or document by the affected individual,<sup>15</sup> and
- The high-risk chemical facility verifies the credential or document is current in accordance

---

<sup>13</sup> This requirement is derived from section 2102(d)(2)(B)(i) of the Homeland Security Act.

<sup>14</sup> 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.

<sup>15</sup> 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.

with its SSP.<sup>16</sup>

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, CISA encourages high-risk chemical facilities to consider any rules, processes, and procedures prescribed by the entity issuing the credential or document. CISA believes that visual verification has inherent limitations and provides less security value than the other options available under the CFATS Personnel Surety Program. CISA 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.

An example of Option 4 that could be implemented by a high-risk chemical facility is to leverage the vetting conducted by the Bureau of Alcohol, Tobacco, Firearms, and

---

<sup>16</sup> This requirement is derived from section 2102(d)(2)(B)(i)(II)(bb) of the Homeland Security Act.

Explosives (ATF) on affected individuals who are employee possessors of a Federal explosives licensee/permittee. For example, a high-risk chemical facility may rely on a "letter of clearance" issued by ATF when presented by an affected individual who is also an employee-possessor of explosives. The high-risk chemical facility should describe in its SSP the procedures it will use to verify the letter of clearance is current. CISA will consider high-risk chemical facilities' proposals in the course of evaluating individual SSPs.

**E. HIGH-RISK CHEMICAL FACILITIES MAY USE MORE THAN ONE OPTION**

High-risk chemical facilities have discretion as to which option(s) to use for an affected individual. For example, if an affected individual possesses a TWIC or some other credential or document, a high-risk chemical facility could choose to use Option 1 for that individual. Similarly, a high-risk chemical facility, at its discretion, may choose to use Option 1 or Option 2 rather than Option 3 or Option 4 for affected individuals who have TWICs or some other credential or document. High-risk chemical facilities also may choose to combine Option 1 with Option 2, Option 3, and/or Option 4, as appropriate, to ensure that adequate terrorist ties checks are performed

on different types of affected individuals (e.g., employees, contractors, unescorted visitors). Each high-risk chemical facility must describe how it will comply with RBPS 12(iv) in its SSP.

**F. HIGH-RISK CHEMICAL FACILITIES MAY PROPOSE ADDITIONAL OPTIONS**

In addition to the options described above for satisfying RBPS 12(iv), a high-risk chemical facility is welcome to propose alternative or supplemental options not described in this document in its SSPs. CISA will assess the adequacy of such alternative or supplemental options on a facility-by-facility basis, in the course of evaluating each facility's SSP.

**G. SECURITY CONSIDERATIONS FOR HIGH-RISK CHEMICAL FACILITIES TO WEIGH IN SELECTING OPTIONS**

CISA believes the greatest security benefit is achieved when a high-risk chemical facility selects either Option 1 and/or Option 2. Option 3 also provides significant security benefit. Option 4 provides some security benefit but less than Option 1, Option 2, or Option 3.

Option 1 and Option 2 provide the greatest security benefit because the information submitted about each affected individual will be recurrently vetted against the

TSDB. Recurrent vetting is a Department best practice and compares an affected individual's information against new and/or updated TSDB records as such records become available. Further, in the event that an affected individual with terrorist ties has or is seeking access to restricted areas or critical assets, if information about that affected individual is submitted to CISA under Option 1 or Option 2, CISA will be able to ensure that an appropriate Federal law enforcement agency is notified and that, as appropriate and consistent with law-enforcement and intelligence requirements, the facility receives notification as well.

Option 3 also provides significant security benefit because information about affected individuals with TWICs is recurrently vetted against the TSDB. However, since CISA does not receive information about these affected individuals from high-risk chemical facilities under Option 3, CISA cannot ensure that the appropriate Federal law enforcement agency is provided information about the high-risk chemical facility at which any such affected individual with terrorist ties has or is seeking access.

Finally, Option 4 provides a more-limited security benefit, as some Federal screening programs do not conduct recurrent vetting. Recurrent vetting compares an affected



individual's information against new and/or updated TSDB records as those new and/or updated records become available. Recurrent vetting is a Department best practice because often records about terrorists are either created or updated in the TSDB after the initial vetting has already occurred. Consequently, recurrent vetting results in additional matches and provides substantial security value.

In addition, relying on a visual inspection of a credential or document is not as secure as electronic verification because visual inspection may make it more difficult to ascertain whether a credential or document has expired, been revoked, or is fraudulent. For example, the visual verification of a TWIC will not reveal whether the TWIC has been revoked by the Transportation Security Administration. Similarly, visual verification of a Hazardous Material Endorsement on a commercial driver's license will not reveal if the endorsement has expired or been revoked.

Finally, since CISA will not receive from high-risk chemical facilities information about affected individuals whose credentials are visually verified, CISA will be unable to ensure the appropriate Federal law enforcement agency is provided information regarding the risks posed to

a high-risk chemical facility by any such affected individual with terrorist ties, nor will it be able to ensure that the facility receives appropriate notification of the risk.

For the reasons described above, Option 4 provides less security value than the other options available to high-risk chemical facilities under the CFATS Personnel Surety Program.

**H. WHEN THE CHECK FOR TERRORIST TIES MUST BE COMPLETED**

CISA will notify high-risk chemical facilities, individually, when it will require each to address RBPS 12(iv) in its SSP. After that notification, a facility must update or draft its SSP to address RBPS 12(iv), as appropriate, prior to authorization or approval by CISA. After authorization or approval, a high-risk chemical facility (as described in its authorized or approved SSP) must complete the terrorist ties check required to be conducted on a particular affected individual by 6 CFR 27.230(a)(iv) prior to the affected individual being granted access to any restricted area or critical asset. For affected individuals with existing access, CISA will expect, unless otherwise noted in an authorized or approved SSP or ASP, that the terrorist ties check will be completed within 60 days after receiving authorization or approval of

an SSP requiring the facility to implement measures to comply with RBPS 12(iv). A high-risk chemical facility may suggest an alternative schedule based on its unique circumstances in its SSP. Table 03 below outlines the four primary options, and the expected time a high-risk chemical facility will have to complete the required activity(ies) outlined in the authorized or approved SSP to comply with RBPS 12(iv) for new affected individual as well as affected individuals with existing access.

**Table 03. Summary of Options to Check For Terrorist Ties.**

<b>Option For Compliance</b>	<b>Facility Activity Description</b>	<b>Timeline for New Affected Individuals</b>	<b>Timeline for Affected Individuals With Existing Access</b>
<b>OPTION 1 - Direct Vetting</b>	Facility submits information to CISA	Unless otherwise noted in an authorized or approved SSP, CISA expects that this activity will be completed prior to the affected individual being granted access to any restricted area or critical asset	Unless otherwise noted in an authorized or approved SSP, CISA expects that this activity will be completed within 60 days after receiving authorization or approval of an SSP requiring the facility to implement measures to comply with RBPS 12(iv).
<b>OPTION 2 - Use of Vetting Conducted Under Other DHS Programs</b>	Facility submits information to CISA		
<b>OPTION 3 - Electronic Verification of TWIC</b>	Facility uses a TWIC Reader		
<b>OPTION 4 - Visual Verification of Credentials Conducting Periodic Vetting</b>	Facility conducts visual verifications by examining affected individuals' credentials or documents		
<b>Facility-Proposed Alternative</b>	Details about facility-proposed alternatives could vary significantly from facility to facility	Details about facility-proposed alternatives could vary significantly from facility to facility	Details about facility-proposed alternatives could vary significantly from facility to facility

**IV. ADDITIONAL DETAILS ABOUT OPTION 1 AND OPTION 2**

**(WHICH INVOLVE THE SUBMISSION OF INFORMATION TO CISA)**

**A. SUBMISSION OF A NEW AFFECTED INDIVIDUAL'S INFORMATION**

**UNDER OPTION 1 OR OPTION 2**

Under Option 1 or Option 2, a high-risk chemical facility may submit information about new affected individuals in accordance with its SSP. CISA encourages

high-risk chemical facilities to submit information about affected individuals as soon as possible after an individual has been determined to be an affected individual. As described earlier in this notice, the high-risk chemical facilities must submit information prior to a new affected individual obtaining access to any restricted area or critical asset.

**B. UPDATES & CORRECTIONS TO INFORMATION ABOUT AFFECTED INDIVIDUALS UNDER OPTION 1 OR OPTION 2**

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

CISA believes that there are substantial privacy risks if a high-risk chemical facility opts not to provide updates and corrections (e.g., updating or correcting a name or date of birth) about affected individuals. Specifically, the accuracy of an affected individual's personal data being vetted against the TSDB for terrorist ties may be affected. Accurate information both (1) increases the likelihood of correct matches against

information about known or suspected terrorists, and (2) decreases the likelihood of incorrect matches that associate affected individuals without terrorist ties with known and suspected terrorist identities. As a result, CISA encourages high-risk chemical facilities to submit updates and corrections as they become known so that the Department's checks for terrorist ties, which are done on a recurrent basis, are accurate. A lesson learned from the implementation of the CFATS Personnel Surety Program since December of 2015 was that high-risk chemical facilities could reduce the burden of continuous updates or corrections by reducing the frequency of updates or correction. For example, a high-risk chemical facility could conduct audits of submitted information on a regular basis such as quarterly or annually and then subsequently update or correct the information. If a high-risk chemical facility is either unable or unwilling to update or correct an affected individual's information, the affected individual may seek redress as described in the CFATS Personnel Surety Program Privacy Impact Assessment.

**C. NOTIFICATION THAT AN AFFECTED INDIVIDUAL NO LONGER HAS ACCESS UNDER OPTION 1 OR OPTION 2**

Section 2102(d)(2)(A)(i) of the Homeland Security Act also prohibits CISA from requiring a high-risk chemical

facility to notify CISA when an affected individual no longer has access to the restricted areas or critical assets of a high-risk chemical facility. Therefore, under Option 1 or Option 2, a high-risk chemical facility has the option to notify CISA when the affected individual no longer has access to any restricted areas or critical assets, but such notification is not required. 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. A lesson learned from the implementation of the CFATS Personnel Surety Program since December of 2015 was that high-risk chemical facilities could reduce the burden of immediately updating the affected individual's record within CSAT to reflect they no longer have access by reducing the frequency of these updates. For example, a high-risk chemical facility could conduct audits of submitted information on a regular basis such as quarterly or annually rather and then subsequently update the affected individual's information. Alternatively, a high-risk chemical facility could submit the date an individual will no longer have access (e.g., a badge expiration date of an

employee or contractor, or the date a contract expires for contractors). If a high-risk chemical facility is either unable or unwilling to notify CISA when an affected individual no longer has access to restricted areas or critical assets, the affected individual may seek redress as described in the CFATS Personnel Surety Program Privacy Impact Assessment.

**D. WHAT/WHO IS THE SOURCE OF THE INFORMATION UNDER OPTION 1 AND OPTION 2**

High-risk chemical facilities are responsible for complying with RBPS 12(iv). However, companies operating multiple high-risk chemical facilities, as well as companies operating only one high-risk chemical facility, may comply with RBPS 12(iv) in a variety of ways. A high-risk chemical facility, or its parent company, may choose to comply with RBPS 12(iv) by identifying and directly submitting to CISA the information about affected individuals. Alternatively, a high-risk chemical facility, or its parent company, may choose to comply with RBPS 12(iv) by outsourcing the information-submission process to third parties.

CISA also anticipates that many high-risk chemical facilities will rely on businesses that provide them with contract services (e.g., complex turn-arounds, freight



delivery services, landscaping) to identify and submit the appropriate information about affected individuals the contract services employ to CISA under Option 1 and Option 2.

Both third parties that submit information on behalf of high-risk chemical facilities and businesses that provide services to high-risk chemical facilities must be designated by the high-risk chemical facility within CSAT in order to submit appropriate information about affected individuals to CISA on behalf of the high-risk chemical facility.<sup>17</sup>

#### **V. CSAT USER ROLES AND RESPONSIBILITIES**

Under Options 1 and 2 (as described above), high-risk chemical facilities have wide latitude in assigning CSAT user roles to align with their business operations and/or the business operations of third parties that provide contracted services to them. CISA has structured the CSAT Personnel Surety Program application to allow designee(s) of high-risk chemical facilities to submit information about affected individuals directly to CISA on behalf of high-risk chemical facilities.

---

<sup>17</sup> Information about how to designate a third party within CSAT is explain in the CFATS Personnel Surety Program User Manual available on [www.dhs.gov/chemicalsecurity](http://www.dhs.gov/chemicalsecurity).

High-risk chemical facilities and designee(s) will be able to structure CSAT user roles to submit information about affected individuals to CISA in several ways, including but not limited to the following:

- A high-risk chemical facility may directly submit information about affected individuals, and designate one or more officers or employees of the facility with appropriate CSAT user roles; and/or
- A high-risk chemical facility may ensure the submission of information about affected individuals by designating one or more persons affiliated with a third party (or with multiple third parties); and/or
- A company owning several high-risk chemical facilities could consolidate its submission process for affected individuals. Specifically, the company could designate one or more persons to submit information about affected individuals on behalf of all or some of the high-risk chemical facilities within the company on a company-wide basis.

Third parties interested in providing information

about affected individuals to CISA on behalf of high-risk chemical facilities may request a CSAT user account from the high-risk chemical facility or company for which the third party will be working. Third parties will not be able to submit information about affected individuals until a high-risk chemical facility designates the third party within CSAT to submit information on its behalf.

CSAT Authorizers will receive access to the Personnel Surety application after the facility's SSP has been approved or authorized by CISA for RBPS 12(iv). The CSAT Authorizer user role creates and manages all other CSAT user roles on behalf of the high-risk chemical facility. A high-risk chemical facility (or designee(s)) may then submit information under Option 1 or Option 2.

One lesson learned since the implementation of the CFATS Personnel Surety Program in December of 2015 was that high-risk chemical facilities can benefit from organizing records about affected individuals within the Personnel Surety application. Organizing the records of affected individuals can be particularly useful when a CSAT Authorizer needs to transfer responsibility of some or all, records about affected individuals to another CSAT Authorizer (e.g., a company sells one or more high-risk chemical facilities to another company).

High-risk chemical facilities may organize submitted records about affected individuals through the use of "groups". Records about affected individuals within groups can be easily transferred. Groups also have the benefit of protecting against the unauthorized disclosure of records. For example, if a company uses third party or a contractor to submit records about affected individuals, a company can limit a third party or contractor access to certain groups (e.g., a contractor could only access the group of records for the affected individuals who are employees of the contractor) and prevent the third party or contractor designee from accessing the records of affected individuals from another contractor or employees of the facility. Additional information about groups and scenarios about how facilities may choose to implement groups may be found within the CSAT 2.0 User Manual.<sup>18</sup>

CSAT Authorizers can also organize submitted records about affected individual through the use of "user defined fields". CSAT Authorizers may add one or more "user defined fields" (e.g., facility location, badge number, employee type, employee status, or contract name/designation) that

---

<sup>18</sup> The CSAT 2.0 User Manual may be found at <https://www.dhs.gov/publication/csat-portal-user-manual>.

allow a record about an affected individual to be labeled in manner that best aligns with the high-risk chemical facilities business practices. CSAT Authorizers may use either or both methods (i.e., groups and "user defined fields") when considering how to organize submitted records of affected individuals.

Finally, CISA can provide assistance to CSAT Authorizers who must transfer responsibility for one or more facilities to another CSAT Authorizer, in which one or more of the facilities have affected individuals that have been submitted under Option 1 or Option 2. CSAT Authorizers may request assistance by contacting the CSAT Helpdesk.<sup>19</sup>

## **VI. PRIVACY CONSIDERATIONS**

High-risk chemical facilities (or designee(s)) may maintain information about an affected individual, for the purpose of complying with CFATS, which is not submitted to CISA as part of the CFATS Personnel Surety Program (e.g., for compliance with RBPS 12(i)-(iii), or for recordkeeping pertaining to Option 3 or Option 4). Information not in the possession of and not submitted to CISA is not covered under the Privacy Act of 1974. Nevertheless, CISA expects

---

<sup>19</sup> The CSAT Helpdesk may be contacted at 866-323-2957 (toll free) between 8:30 a.m. and 5 p.m. (ET), Monday through Friday. The CSAT Help Desk is closed for Federal holidays.

that high-risk chemical facilities and designee(s) will protect and safeguard any such information as outlined in their SSPs and in accordance with any other Federal, State, or local privacy laws that are applicable to the collection of the information, just as the high-risk chemical facilities would for other similar information collected under a their normal business practices for activities unrelated to CFATS.

**A. PRIVACY ACT REQUIREMENTS TO ENABLE OPTION 1 AND OPTION**

**2**

CISA complies with all applicable federal privacy requirements including those contained in the Privacy Act, the E-Government Act, the Homeland Security Act, and Departmental policy. The United States also follows international instruments on privacy, all of which are consistent with the Fair Information Practice Principles (FIPPs).<sup>20</sup> The Department:

- Published a System of Records Notice (SORN) for the CFATS Personnel Surety Program on June 14,

---

<sup>20</sup> See Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf) (December 29, 2008).

2011 as well as a SORN Update on May 19, 2014.<sup>21</sup>

- Issued a Final Rule<sup>22</sup> to exempt portions of the Chemical Facility Anti-Terrorism Standards Personnel Surety Program SORN from certain provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements on May 21, 2014.
- Published a CFATS Personnel Surety Program Privacy Impact Assessment (PIA) in May 2011, and CFATS Personnel Surety Program PIA Updates in May of 2014, November of 2015, and May of 2017. The PIA and the updates are available at <https://www.dhs.gov/publication/dhs-nppd-pia-018a-chemical-facilities-anti-terrorism-standards-personnel-surety>.

With the publication of these privacy documents, CISA has ensured that the CFATS Personnel Surety Program complies with the appropriate privacy laws and Department

---

<sup>21</sup> See DHS/NPPD-002 - Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records, published on May 19, 2014 at 79 FR 28752. DHS/NPOPD-002 may be viewed at <https://www.federalregister.gov/d/2014-11431>.

<sup>22</sup> See Implementation of Exemptions; Department of Homeland Security/National Protection and Programs Directorate--002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records, published on May 21, 2014 at 79 FR 29072. The final rule may be viewed at <https://www.federalregister.gov/d/2014-11433>.

of Homeland Security privacy policies.

**B. REDRESS**

The CFATS Personnel Surety Program complies with the requirement of section 2102(d)(2)(A)(iii) of the Homeland Security Act to provide redress to an individual: (1) whose information was vetted against the TSDB under the program; and (2) who believes that the personally identifiable information submitted to the Department for such vetting by a covered chemical facility, or its designated representative, was inaccurate. The Department has described how to seek redress in the CFATS Personnel Surety Program Privacy Impact Assessment.

**C. ADDITIONAL PRIVACY CONSIDERATIONS RELATED TO OPTION 1  
AND OPTION 2**

The Submitter(s) of each high-risk chemical facility (or designee(s)) will be required to affirm that, in accordance with its SSP, notice required by the Privacy Act of 1974 has been given to affected individuals before their information is submitted to CISA. The Department has made available a sample Privacy Act notice that complies with subsection (e)(3) of the Privacy Act (5 USC 552a(e)(3)) in the CFATS Personnel Surety Program PIA Update published on



November 10, 2015.<sup>23</sup> The sample notice, or a different satisfactory notice, must be provided by a high-risk chemical facility to affected individuals prior to the submission of Personally Identifiable Information (PII) to CISA under Option 1 and Option 2. This notice must: (1) notify those individuals that their information is being submitted to CISA for vetting against the TSDB, and that in some cases additional information may be requested and submitted in order to resolve a potential match; (2) instruct those individuals how to access their information; (3) instruct those individuals how to correct their information; and (4) instruct those individuals on procedures available to them for redress if they believe their information has been improperly matched by the Department to information contained in the TSDB. Individuals have the opportunity and the right to decline to provide information; however, if an individual declines to provide information, he or she may impact a high-risk chemical facility's compliance with CFATS.

---

<sup>23</sup> The November 20, 2015 CFATS Personnel Surety Program PIA Update, as well as other privacy related documents, are available at on the Department's website at <https://www.dhs.gov/publication/dhs-nppd-pia-018a-chemical-facilities-anti-terrorism-standards-personnel-surety>.

**D. ADDITIONAL PRIVACY CONSIDERATIONS FOR OPTION 3 AND  
OPTION 4**

A high-risk chemical facility will not submit information to CISA if the facility opts to electronically verify and validate affected individuals' TWICs through the use of TWIC readers (or other technology that is periodically updated with revoked card information) under Option 3. High-risk chemical facilities that opt to implement Option 3 are encouraged, but are not required, to provide notice to each affected individual whose TWIC is being verified and validated. Although Option 3 allows high-risk chemical facilities to comply with RBPS 12(iv) without submitting information to CISA, CISA feels that appropriate notice should still be given to those individuals so that they know their TWICs are now being used to comply with 6 CFR 27.230(a)(12)(iv). The Department has provided a sample privacy notice for high-risk chemical facilities to use in the CFATS Personnel Surety Program PIA Update, published on November 10, 2015.

In addition, a high-risk chemical facility will not submit information to CISA if the facility opts to utilize Option 4 and to visually inspect a credential or document for any Federal screening program that periodically vets individuals against the TSDB. High-risk chemical

facilities that opt to implement Option 4 are encouraged, but are not required, to provide notice to each affected individual whose Federal screening program credential or document is being visually inspected in order to comply with 6 CFR 27.230(a)(12)(iv).

**VII. INFORMATION A HIGH-RISK CHEMICAL FACILITY MAY WISH TO CONSIDER INCLUDING IN ITS SSP**

When writing, revising, or updating their SSPs, high-risk chemical facilities may wish to consider including information about the following topics to assist CISA in evaluating the adequacy of the security measures outlined in the SSP for RBPS12(iv):

1. GENERAL:

- Who does the facility consider an affected individual and how does the facility identify affected individuals?
  - Who does the facility consider facility personnel and how does the facility identify them?
  - Who does the facility consider unescorted visitors and how does the facility identify them?
- If the facility escorts any visitors, how does it escort them and does the facility have an escort

policy?

- How does the facility define its restricted areas and/or critical assets for the purposes of RBPS 12?
- Does the facility include computer systems or remote access as either a restricted area or critical asset?
- Which Option(s), or alternative approaches not described in this notice, will the facility or its designee(s) use to check for terrorist ties?
- Does the facility intend to use one or more Options for some affected individuals that it will not use for other affected individuals? If so, which Option(s) apply to which groups of affected individuals?
- Will the facility opt to have a designee(s) (e.g. third party company, contractor, co-located company) submit information about affected individuals? If so, what guidance will the high-risk chemical facility establish for designee(s) when it submits information (e.g., when are affected individuals considered to be "facility personnel" or "unescorted visitors", how will

submitted records by the designee about affected individuals be organized within the CSAT Personnel Surety application, how will the facility verify that notice has been provided to an affected individual before information about him/her is provided to CISA)?

- Does the high-risk chemical facility anticipate that any individuals will require access to restricted areas or critical assets without visitor escorts or without the background checks listed in RBPS 12 under exceptional circumstances (e.g., foreseeable but unpredictable circumstances)? If so, who? If so, which exceptional circumstances would warrant access without visitor escorts or without the background checks listed in RBPS 12?
- Will the facility be capable of implementing the options within the timeframes specified? If not, what timeframe does the facility propose for submission and what justification has been provided to CISA to allow for an extended timeframe?

2. WITH REGARD TO OPTION 1:

- How will notice be provided to affected

individuals that information is being provided to CISA? Does the facility plan to use the DHS sample privacy notice?

- Does the facility plan to organize submitted records about affected individuals using groups?
- Does the facility plan to organize submitted records about affected individuals using "user defined fields" If so, what "user defined fields" will be added?
- Does the facility intend to notify CISA when the affected individual no longer has access to any restricted areas or critical assets? If so, how and when?

3. WITH REGARD TO OPTION 2:

- How will notice be provided to affected individuals that information is being provided to CISA? Does the facility plan to use the DHS sample privacy notice?
- What credentials does the facility plan to use under Option 2? Are there credentials the facility has decided not to accept under Option 2?
- What will the facility do if CISA is unable to

verify an affected individual's enrollment in another Department TSDB vetting program?

- What will be the timeframe for this follow-on action?
- What will the facility do if CISA does verify the credential, but later during a periodic re-verification, is unable verify the credential?
- What will be the timeframe for this follow-on action?
- Does the facility describe how it will comply with RBPS 12(iv) for affected individuals without credentials capable of being verified under Option 2?
- Does the facility plan to organize submitted records about affected individuals using groups?
- Does the facility plan to organize submitted records about affected individuals using "user defined fields" If so, what "user defined fields" will be added?
- Does the facility intend to notify CISA when the affected individual no longer has access to any restricted areas or critical assets? If so, how and when?

4. WITH REGARD TO OPTION 3:

- How will the facility identify those affected individuals who possess TWICs?
- How will the facility comply with RBPS 12(iv) for affected individuals without TWICs?
- How will the facility electronically verify and validate TWICs of affected individuals?
- Which reader(s) or Physical Access Control System (PACS) will the facility be using? Or, if it is not using readers, how it will use the CCL or CRL?
- Where will the reader(s) or PAC(s) be located?
- What mode or modes (i.e., which setting on the TWIC Reader) will be used when verifying and validating the TWIC of an affected individual?<sup>24</sup>
- Will the TWIC of an affected individual be re-verified and re-validated with TWIC readers, and, if so, how often?
- What will the facility (or designee(s)) do if an affected individual's TWIC cannot be verified or

---

<sup>24</sup> See table 4.1 on page 18 of the TSA reader specification at [http://www.tsa.gov/sites/default/files/publications/pdf/twic/twic\\_reader\\_card\\_app\\_spec.pdf](http://www.tsa.gov/sites/default/files/publications/pdf/twic/twic_reader_card_app_spec.pdf).



if the TWIC reader is not functioning properly?

5. WITH REGARD TO OPTION 4:

- Upon which Federal screening program(s) does the facility or designee intend to rely?
- What document(s) or credential(s) issued by the Federal screening program(s) will the facility visually verify?
- What procedures will the facility use to allow affected individuals to present document(s) or credential(s)?
- How will the facility verify that the credential or document presented by affected individuals is not fraudulent?
- What procedures will the facility follow to visually verify that a credential or document is current and valid (i.e., not expired)?
- How frequently will the facility visually verify the credentials (e.g., upon each entry or on a recurring cycle)?
- Will the visual verification include the following?
  - Comparing any picture on a document or credential to the bearer of the credential

- o or document;
  - o Comparing any physical characteristics listed on the credential or document (e.g. height, hair color, eye color) with the bearer's physical appearance;
  - o Checking for tampering;
  - o Reviewing both sides of the credential or document and checking for the appropriate stock/credential material;
  - o Checking for an expiration date; and
  - o Checking for any insignia, watermark, hologram, signature or other unique feature.
- What will the facility do if it is unable to visually verify an affected individual's credential or document, if the credential or document fails visual verification, or if the credential or document appears invalid, expired, or fraudulent?

6. WITH REGARD TO OTHER OPTIONS:

- A facility that chooses to propose an option not listed above in its SSP should provide as much detail as possible to allow CISA to consider the potential option and evaluate whether or not it meets the RBPS 12(iv) standard.

**David Wulf**

Director,  
Infrastructure Security Compliance Division,  
Infrastructure Security Division,  
Cybersecurity and Infrastructure Security Agency,  
U.S. Department of Homeland Security.  
[FR Doc. 2019-14591 Filed: 7/8/2019 8:45 am; Publication Date: 7/9/2019]