Privacy Impact Assessment Update
for the

Chemical Facility Anti-Terrorism Standards (CFATS) Program

DHS/NPPD/PIA-009

July 26, 2012

Contact Point
David Wulf
NPPD/IP/ISCD
(703) 603-4778

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

Abstract

The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD) is consolidating and updating the Privacy Impact Assessment (PIA) for the Chemical Facility Anti-Terrorism Standards (CFATS) regulations, 6 CFR Part 27. This PIA replaces the former PIAs for the Chemical Security Assessment Tool (CSAT) and CFATS, in order to provide a unified analysis of the collection and use of personally identifiable information (PII) as part of CFATS. CFATS is the DHS regulation that governs security at high-risk chemical facilities and represents a national-level effort to minimize terrorism risk to such facilities.

Overview

Section 550 of the Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295 ("Section 550"), authorizes DHS to regulate the security of high-risk chemical facilities. NPPD implements this statutory authority through CFATS.

CFATS establishes a risk-based approach to identifying and securing chemical facilities determined by NPPD to be "high-risk." To assist in making "high-risk" determinations, NPPD published Appendix A to the CFATS regulation. Appendix A identified over 300 chemicals of interest (COI) and established a screening threshold quantity (STQ) for each chemical based on the potential adverse consequences for human life or health if the chemicals were intentionally released or detonated, stolen and converted into weapons, or mixed with other readily available materials as a contaminate.

CFATS requires facilities in possession of any COI at or above the applicable STQ to complete and submit to NPPD a Top-Screen questionnaire. After reviewing the facility information[1] submitted through the Top-Screen, and other available information, NPPD initially determines which facilities are high-risk. NPPD then notifies each such facility, preliminarily assigns each facility to a risk-based tier (Tiers 1–4)[2], and requires each preliminary high-risk facility to submit a Security Vulnerability Assessment (SVA).[3] Tier 4 facilities may submit an Alternative Security Program (ASP)[4] in lieu of an SVA. Each facility still considered high-risk

[1] This PIA differentiates between facility information (which does not contain PII) and PII.

[2] Consistent with Section 550, the CFATS regulation follows a risk-based approach that allows NPPD to focus its resources on high-risk chemical facilities in accordance with their specific level of risk. NPPD places facilities in one of four risk-based tiers. Tiers range from Tier 1, which contains the highest-risk facilities, to Tier 4, which contains the lowest-risk facilities.

[3] The SVA is used to identify the critical assets at the facility and to evaluate the facility's security vulnerabilities in light of the security issues identified in its preliminary tier notification letter. The SVA provides more in-depth information that allows NPPD to make a final decision as to whether a facility is high-risk and if it is, to assign a final risk tier ranking to the facility.

[4] A Tier 4 facility may submit an ASP in lieu of an SVA. Any facility may submit an ASP in lieu of a Site Security Plan.

after NPPD reviews its SVA (or ASP, where applicable), and other available information is provided a final determination of high-risk status and assigned to a final tier. Each final high-risk facility is then required to complete a Site Security Plan (SSP)[5] or ASP that meets the applicable risk-based performance standards (RBPS)[6] specified in the CFATS regulation. Certain chemical facilities, such as facilities regulated under the Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, are exempt from CFATS under Section 550.

Among other requirements, CFATS also: (1) establishes a protection regime for certain information designated as Chemical-terrorism Vulnerability Information (CVI); (2) provides for inspections and audits of covered facilities; and (3) imposes certain recordkeeping requirements upon chemical facilities.

To support the implementation of CFATS, NPPD has developed and deployed the following:

- **CSAT:** CSAT is an information technology (IT) system primarily designed to collect facility information through specific applications for submitting Top-Screens, SVAs, SSPs, and ASPs. CSAT also contains applications designed to support other portions of the CFATS Program such as:
  - **CFATS Share:** CFATS Share is an application that allows designated DHS, federal, state (including Homeland Security Advisors (HSAs)), local, territorial and tribal government officials access to a reporting and mapping tool which contains aggregated CSAT survey data restricted to their geographic area of interest.
  - **CVI Authorized User Training:** CVI Authorized User Training is a public-facing application for training in the handling and marking of CVI.
- **Chemical Facility Management System (CHEMS):** CHEMS is a case management tool that allows NPPD to process additional information about specific chemical facilities as they move through the regulatory process. Specifically, CHEMS: (1) receives routine transfers of information (some of which is PII) from CSAT; (2) securely stores correspondence between NPPD and high-risk chemical facilities; and (3) serves as the repository for information collected (potentially including some PII) during personal interactions with high-risk chemical facilities.

---

[5] The SSP identifies site-specific security measures that address the identified risk-based performance standards. DHS determines whether a facility's SSP satisfies the applicable performance standards and, if it does, approves the SSP. DHS may disapprove any SSP that does not meet the applicable standards.

[6] Section 550 directed the Department to issue regulations "establishing risk-based performance standards for the security of high-risk chemical facilities." CFATS currently has 18 RBPS, addressing areas such as: perimeter security; shipping, receipt, and storage; cybersecurity; personnel surety; training; and recordkeeping.

- **CFATS Help Desk and Tip Line:** The CFATS Help Desk and Tip Line help individuals and chemical facilities comply with CFATS requirements and allow NPPD to respond to inquiries from the public. The CFATS Help Desk provides live assistance, as well as online assistance via a Web Form to submit an issue for CFATS inquiries regarding the submission of chemical facility information, CVI training, or CSAT login and user account issues. The CFATS Tip Line allows for individuals associated with the chemical facility or any member of the general public to report security concerns involving the CFATS regulation at a chemical facility.

CFATS impacts privacy through the collection, use, and sharing of PII provided by individuals for the purposes of complying with various provisions of CFATS.[7] This PIA evaluates the collection of PII in support of the CFATS Program and supersedes the original CSAT PIA from March 27, 2007, and its four subsequent updates.[8] It also describes CFATS Program processes as they currently function within a changing program environment. As the program changes NPPD will review and update the PIA as appropriate.

CFATS Program Collection of PII

Under the features of CFATS described in this PIA, NPPD potentially collects the following types of information[9]:

- Personal information (e.g., name, U.S. Citizenship, etc.)
- Business contact information (e.g., business address, email address, phone number, etc.)
- Job-related information (e.g., job title/position, organization name, description of official duties, supervisor name and phone number, etc.)
- CFATS Program-related information (e.g., CVI Authorized User Number, CSAT User Role, etc.)
- Other information (e.g., any other PII contained in correspondence or obtained during interactions between NPPD and the chemical facility)

---

[7] This Privacy Impact Assessment (PIA) does not cover collection of PII under subsection (iv) of RBPS 12 of CFATS (6 CFR 27.230(a)(12)(iv)). For more information on potential privacy impacts of subsection (iv) of RBPS 12, see DHS/NPPD/PIA-018 Chemical Facility Anti-Terrorism Standards Personnel Surety Program, May 4, 2011.

[8] DHS/NPPD/PIA-009, Chemical Facility Anti-Terrorism Standards (CFATS) Update, June 11, 2009; DHS/NPPD/PIA-009(a), Chemical Facility Anti-Terrorism Standards (CFATS) Update June 5, 2009; DHS/NPPD/PIA-009(b), Chemical Security Assessment Tool (CSAT) Update, October 27, 2008; DHS/NPPD/PIA-009(c), Chemical Security Assessment Tool Update, May 25, 2007; DHS/NPPD/PIA-009(d), Chemical Security Assessment Tool, March 27, 2007.

[9] See section 2.1 for a complete list of PII collected under the features of CFATS described in this document.

CFATS Program Users

Under the features of CFATS described in this PIA, NPPD potentially collects information from the following individuals:

- Individuals who register to be **CSAT** Users. CSAT Users include individuals designated to act on behalf of a chemical facility (including individuals in the roles of "Authorizer," "Preparer," "Reviewer," and "Submitter"), collectively known as "designated individuals." These designated individuals may also submit information on facility points-of-contact who do not have access to CSAT. CSAT Users also include DHS employees and contractors. Users of CSAT applications include:
    - Individuals who register to be **CFATS Share** Users. CFATS Share Users include designated DHS, federal, state (e.g., HSAs), local, territorial and tribal government officials with an official interest in certain CFATS information.
    - Individuals who have completed **CVI Authorized User Training** and submitted applications to become CVI Authorized Users. Any person may apply to be a CVI Authorized User. Access to or disclosure of CVI requires that an individual both have a "need-to-know" and be registered with DHS as a CVI Authorized User.
- Individuals who register to be **CHEMS** Users. CHEMS Users include only DHS employees and contractors.
- Individuals who contact the **CFATS Help Desk or Tip Line**. While any member of the general public may contact the CFATS Help Desk, NPPD anticipates only those individuals who are associated with chemical facilities or those with the intent of supporting CFATS compliance will provide their personal information. The Tip Line, however, allows members of the general public to leave an anonymous message or to leave basic contact information if a return call is desired. If the caller decides to leave contact information, a name and phone number are requested. However, whether any PII is collected is ultimately the decision of the individual calling.
- In addition to the categories listed above, information may also be collected from **other individuals associated with a covered chemical facility**, for example:
    - During the inspection process, NPPD Chemical Inspectors may have limited contact with some PII while carrying out activities ensuring facility compliance with the content of the facility's SSP (e.g., an

Inspector may review a facility's training records, which may contain PII, to ensure that the facility is in compliance with the security training requirements contained in the SSP); or

- In the event that a high-risk facility does not meet CFATS requirements, NPPD may issue an administrative compliance order to the facility. If the facility does not comply with this order, NPPD may issue an order assessing a civil penalty, an order to cease operations, or both. In an instance where payment is required as a result of a civil penalty, DHS may need to collect additional PII, potentially including business contact information, credit card information, or information appearing on checks (e.g., name, address and bank account information).

CSAT User Roles

Designated individuals may perform a number of different roles within CSAT including: Authorizer, Preparer, Reviewer, and Submitter.

- An Authorizer is the official facility representative who identifies and verifies the individuals who will maintain the CSAT user roles on behalf of the facility.
- A Preparer is an individual familiar with the facility in question who is authorized to enter data into the CSAT Top-Screen, but is not authorized to formally submit the data on the facility's behalf.
- A Reviewer has "read only" access and can review facility-specific information prior to its submission.
- A Submitter is an individual who is: (1) certified by the facility or company to formally submit regulatory data to NPPD, (2) an officer of the company (or designated by an officer of the company), and (3) domiciled in the United States.[10]

CFATS Compliance Process

When a chemical facility not exempt under Section 550 possesses any COI at or above the applicable STQ, it is required to submit a Top-Screen. To submit a Top-Screen, a chemical facility must first identify the designated individual(s) (i.e., the Preparer and Submitter) who will input and submit facility information on behalf of the facility through

[10] To complete and submit a Top-Screen, the facility must designate a person who is responsible for the submission of information through the CSAT system and who attests to the accuracy of the information contained in any CSAT submissions. Such a submitter must be an officer of the corporation or other person designated by an officer of the corporation and must be domiciled in the United States (6 CFR § 27.200(b)(3)).

CSAT. The facility may choose to designate a single person to be both the Preparer and Submitter. A chemical facility Authorizer registers his/her designated individual(s) through the CSAT registration process.[11] To access the Top-Screen, a CSAT User must agree to safeguard the facility information in accordance with CVI requirements. The Submitter submits information into CSAT about the facility that includes, but is not limited to, types of chemicals stored and produced, and location of the facility. Upon submission of the Top-Screen to NPPD, one of two outcomes is possible:

- A preliminary determination that a chemical facility is not high-risk; or
- A preliminary determination that a chemical facility is high-risk and preliminary placement in a risk-based tier (Tier 1-4), typically based on specific chemicals of interest and related security issues that require further analysis.

If NPPD determines that the facility is preliminarily high-risk, NPPD then requires the chemical facility to complete an SVA through CSAT. The SVA collects detailed information necessary to allow NPPD to make a final determination regarding whether or not the facility presents a high-risk. A CSAT User must be a CVI Authorized User to access the SVA.

Following a chemical facility's submission of the SVA to CSAT, SVA information is then analyzed using a classified IT system, known as CSAT-Classified (CSAT-C). NPPD uses CSAT-C to conduct a risk analysis and to help determine whether a chemical facility is or is not high-risk.

If NPPD makes the final determination that the chemical facility is a high-risk facility, that facility must develop and submit an SSP to NPPD for review and approval, or ASP in lieu of an SSP that satisfies the applicable RBPS. During the review process, NPPD compares specific security measures reported in the SSP against the RBPS to determine whether the SSP adequately addresses the applicable RBPSs in a manner commensurate with the facility's risk-based tier and other circumstances.

Once NPPD has determined that the SSP appears to be adequate, NPPD authorizes the SSP, and NPPD Chemical Inspectors conduct on-site authorization inspections to validate the content of the SSP. Upon completion of authorization inspections, the results will help inform NPPD's decision to approve or disapprove the SSP. Facilities with approved SSPs will undergo compliance inspections.

During the inspection process, NPPD Chemical Inspectors may have limited contact with some PII while carrying out activities ensuring facility compliance with the content of the facility's SSP (e.g., an Inspector may review a facility's training records, which may contain PII, to ensure that the facility is in compliance with the security training requirements contained in the SSP).

[11] See Section 8.3 of this PIA for more information on the registration process.

Copies of correspondence between NPPD and chemical facilities; information related to a Chemical Inspector's interactions with a chemical facility, including notes from face-to-face meetings, site visits, phone calls, emails, etc.; information on individuals authorized by chemical facilities to have access to CSAT and their respective roles/responsibilities; and contact information of designated individuals and their status as CVI Authorized Users are all maintained in CHEMS. Some of this information is or may contain CVI.

In the event that a high-risk facility does not meet CFATS requirements, NPPD may issue an administrative compliance order to the facility. If the facility does not comply with this order, NPPD may issue an order assessing civil penalty, an order to cease operations, or both. In an instance where payment is required as a result of a civil penalty, DHS may need to collect additional PII, potentially including business contact information, credit card information, or information appearing on checks (e.g., name, address and bank account information).

CFATS Information Sharing

Through CFATS Share, NPPD shares certain facility information (e.g., CSAT survey data restricted by geographic area) collected under CFATS with designated DHS, federal, state (e.g., HSAs), local, territorial and tribal government officials with an official interest in such information.

NPPD may also share business contact information of designated individuals (including, but not limited to, facility addresses/locations and phone numbers, as well as facility points-of-contact' identities, phone numbers, and email addresses), as appropriate, with federal, state, local, tribal, and territorial government officials who demonstrate a need to know the information to carry out their official duties. For example, contact information may be provided to appropriate officials to respond to or notify facilities of natural or manmade disasters in a specific geographic area. NPPD may also share contact information of designated individuals and facility points-of-contact with select non-government entities, such as first responders, regulated chemical facilities, private sector working groups and other designated individuals, who demonstrate a need-to-know to carry out essential national security, chemical security and/or infrastructure security functions.

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 Pub. L. No. 109-295 grants DHS the responsibility and authority to identify and regulate the security of high-risk chemical facilities. DHS implements its authority through the CFATS regulations, 6 CFR Part 27.

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

The following Department-wide SORNs apply to the information collected under the features of CFATS described in this PIA:

- CSAT (including CFATS Share and CVI Authorized User Training) and CHEMS user information is covered by the DHS/All—004 Privacy Act System of Records Notice, General Information Technology Access Account Records System (GITAARS), 74 Fed. Reg. 49882 (Sep. 29, 2009), http://edocket.access.gpo.gov/2009/E9-23513.htm.
- The CFATS Help Desk and Tip Line information is maintained under the DHS/All-002—Privacy Act System of Records Notice, Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (Nov. 25, 2008), http://edocket.access.gpo.gov/2008/E8-28053.htm.

Other information collected under the features of CFATS described in this PIA is not retrieved by personal identifier and therefore no SORN is required for it under the Privacy Act.

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

Both CSAT and CHEMS have completed system security plans. CSAT is secured in accordance with Federal Information Security Management Act (FISMA) requirements. In June 2012, CSAT was issued a three-year Authority to Operate (ATO). CSAT is certified and accredited at the sensitive but unclassified (SBU) level, consistent with the National Institute of Standards and Technology (NIST) 800-53 specifications and DHS policy and guidance, including DHS Sensitive System Policy Directive 4300A.

CSAT-C is certified and accredited at the Secret level in accordance with DHS National Security System Policy Directive 4300B, which uses the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).

CHEMS is separately accredited and its current three-year ATO was issued in January 2012.

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

NPPD has a retention schedule (N1-563-07-7) approved by NARA for data submitted into CSAT. The CFATS Help Desk and Tip Line are covered under General Records Schedule (GRS) 20, Electronic Records, item 2b (N1-GRS-87-5 item 2b). NPPD is also currently working on an overarching records schedule for the CFATS Program.

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.

OMB Collection #1670-0007 (Agency Tracking No: 0012) issued on March 19, 2010, includes: CSAT User Registration, CSAT Top-Screen, CSAT Security Vulnerability Assessment and Alternative Security Program submitted in lieu of the CSAT Security Vulnerability Assessment, CSAT Site Security Plan and Alternative Security Program submitted in lieu of the CSAT Site Security Plan, CVI Authorization, and CFATS Help Desk and Tip Line.

OMB Collection #1670-0014 (Agency Tracking No: 0015) issued on March 19, 2010, is used by facilities to communicate with or notify the Department regarding:

- Request for Redetermination for a facility that has made material alterations to its operations;
- Request for an Extension for submission of a Top-Screen, SVA, or SSP;
- Notification of New Top-Screen for a facility that needs to submit a revised Top-Screen due to a change from the previous submission (e.g., when a facility closes, sells, adds new COI, deletes existing COI, or changes the amount of COI); and
- Request for a Technical Consultation (e.g., when a facility seeks a consultation and/or technical assistance).

OMB Collection #1670-0015 (Agency Tracking No: 0013) issued on March 19, 2010, is used for CFATS Share User Registration and to manage the CVI program in support of CFATS. All three OMB Collections will expire on March 31, 2013.

The following is a list of DHS Forms associated with each OMB Collection:

- OMB Collection #1670-0007: DHS Form 9002, 9002.1, 9002.2, 9002.3, 9002.4, 9002.5, 9002.6, 9007, 9010, 9010-1, 9012, 9015, 9019.
- OMB Collection #1670-0014: DHS Form 9034, 9035, 9036, 9037.
- OMB Collection #1670-0015: DHS Form 9012, 9024, 9025, 9026, 9027, 9028.

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.

The PII collected under the features of CFATS described in this document may include:

- First Name, Last Name
- Middle Initial (optional)
- Phone Number
- Business Email Address
- Business Address (Street, City, State, Zip Code)
- Job Title/Position
- U.S. Citizenship
- Domiciled in the U.S.? (Yes/No)
- Is the individual an Officer of the Corporation or designated by an Officer of the Corporation? (Yes/No)
- Organization Name & Type (chosen from drop down menu)
- Description of Official Duties
- Direct Supervisor's Name
- Direct Supervisor's Telephone
- Agency/Affiliation
- CVI Authorized User Number (to verify that the user has completed CVI Training)
- CSAT User Role
- DHS Supervisor Name
- Information necessary to collect and process civil penalties, such as: business contact information, credit card numbers or information appearing on checks (e.g., name, address and bank account information)
- Any other PII contained in correspondence or obtained during interactions between NPPD and the chemical facility

The Help Desk vendor may also collect information from callers or via web form, such as:

- Facility Name
- First Name, Last Name
- Phone Number
- Fax Number

- Facility Address
- Email Address
- Registered CSAT User? (Yes/No)
- Facility ID (if applicable)
- User Registration Form ID (if applicable)
- CVI Authorized User Number (a Customer Service Representative may require the CVI Number to validate that a caller is a CVI Authorized User before proceeding)

The CFATS Tip Line allows for the reporting of security concerns involving the CFATS regulation at a chemical facility. CFATS Tip Line voicemails are transcribed and tracked as a support ticket for further NPPD inquiry. The caller is encouraged to leave an anonymous message or to leave basic contact information if a return call is desired. If the caller decides to leave contact information, a name and phone number are requested. However, what PII is collected is ultimately the decision of the individual calling.

Under CFATS, NPPD also collects information regarding a chemical facility, which includes, but is not limited to types of chemicals stored and produced, location of the facility, and security measures.

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

Individuals designated to act on behalf of chemical facilities are the primary source of PII and chemical facility information. PII is collected through CSAT, including CFATS Share and the CVI Authorized User Training application. The sources of CHEMS information about individuals are: (1) the CSAT web-based applications, and/or (2) correspondences and personal interactions with the high-risk chemical facility or other representatives. PII may be collected through the CFATS Help Desk via e-mail, mail, fax, or telephone, and through the CFATS Tip Line via telephone (voicemail). PII may also be collected from other individuals associated with a chemical facility. For example, during the inspection process, an individual associated with the facility may provide the Inspector with training records, which may contain PII, to demonstrate the facility's compliance with the security training requirements contained in its SSP. Additionally, an individual associated with the facility may provide PII (such as business contact information, credit card numbers, or information appearing on checks) when making a payment as a result of a civil penalty.

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

CFATS uses commercial and publicly available data to detect situations, such as bankruptcy, which may affect the security at CFATS covered facilities.

2.4 Discuss how accuracy of the data is ensured.

Information collected directly from designated individuals or provided from chemical facilities is assumed to be accurate. Additionally, CFATS only uses commercially or publically available data from reliable, widely-accepted sources of business information.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: The principal privacy risks associated with the elements of CFATS described in this document are the over-collection of PII and the unauthorized use of that PII.

Mitigation: NPPD mitigates the risk of over-collection by focusing the collection of PII on business contact-related information. NPPD mitigates the risk of unauthorized use of PII by using the information collected only to facilitate compliance with CFATS, for example, to enable communication between NPPD and the chemical facility, to assign appropriate user roles in CSAT and CHEMS (DHS employees and contractors only), and to determine whether the individual is trained and authorized to handle CVI.

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.

Section 550 of Pub. L. No. 109-295 provides DHS with the authority to regulate the security of high-risk chemical facilities. The information collected under CFATS enables NPPD to execute DHS' responsibilities to reduce the risk of a terrorist attack against high-risk chemical facilities or the use of chemicals from a high-risk chemical facility in the commission of a terrorist attack. Personal information is collected in order to:

- Provide and adjudicate access to CSAT, CFATS Share and CHEMS;
- Ensure that NPPD can contact the individuals responsible for security or CFATS-related activities at or around high-risk chemical facilities;

- Process and adjudicate applications to be CVI Authorized Users, validate association with a high-risk chemical facility or entity, assist in researching or verifying need-to-know, and verify CVI Authorized User status;
- Provide quality support when contacting the CFATS Help Desk/Tip Line;
- Ensure that a high-risk chemical facility is in compliance with its SSP during inspections or audits; and
- Collect payment as a result of a civil penalty.

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.

CFATS does not use technology to conduct electronic searches, queries, or analyses 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?

DHS components may have user access to CSAT through the CFATS Share. This access is restricted to aggregated survey data in a defined geographic area, such as a Federal Emergency Management Agency region after a natural disaster.

Only DHS employees and contractors with a need-to-know have access to CSAT-C and CHEMS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: The privacy risks include the misuse of the information collected, unauthorized access to the information collected, and the risk of unauthorized use/disclosure and loss of this information.

Mitigation: NPPD ensures that PII is handled in accordance with the described uses by integrating administrative, technical, and physical security controls that limit the collection of PII and protect information against unauthorized disclosure, use, modification or destruction. PII will only be disclosed to, and used by, authorized individuals who have a need-to-know the information in order to perform their duties. As part of the technical safeguards employed, CSAT and CHEMS use role-based access controls and audit logging, as described in Section 8.0 of this PIA, to control and monitor the use of PII.

Furthermore, all DHS personnel authorized to handle PII under CFATS are required to complete DHS privacy training and IT security training on an annual basis. These safeguards further minimize the potential privacy risk that PII may be improperly 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.

NPPD provides notice through this PIA and relevant System of Records Notices: DHS/All—004 Privacy Act System of Records Notice, General Information Technology Access Account Records System (GITAARS), 74 Fed. Reg. 49882 (Sep. 29, 2009), and DHS/All-002—Privacy Act System of Records Notice, Department of Homeland Security (DHS) Mailing and Other Lists System, 73 Fed. Reg. 71659 (Nov. 25, 2008).

NPPD also provides a Privacy Act Statement[12] on certain forms that collect PII under CFATS[13].

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

Individuals do not have the right to consent to particular uses of their information.

Individuals are not required to provide their information in certain circumstances. A log-in banner is displayed on the CSAT registration site that states there is no expectation of privacy when using the system and that all users are subject to monitoring. If individuals do not want to be subject to monitoring, individuals can opt out of providing their information. If individuals do not provide their information, however, they will not be able to obtain an account to access the CSAT applications (including CFATS Share) or to apply to be a CVI Authorized User. The same rules apply to DHS employees and contractors who seek access to CHEMS. Likewise, individuals are not required to provide their information to the CFATS Help Desk vendor or Tip Line. Without the ability to verify the individuals who are contacting the CFATS Help Desk or Tip Line, however, only limited support may be provided to these individuals.

[12] See 5 U.S.C. § 552a(e)(3)
[13] OMB Collections #1670-0007, #1670-0014 and #1670-0015

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that inadequate notice will be provided.

Mitigation: NPPD provides a Privacy Act Statement (see 5 U.S.C. § 552a(e)(3)) on certain forms collecting PII under CFATS (OMB Collections #1670-0007, #1670-0014 and #1670-0015). Notice is also provided via this PIA, the applicable SORNs, and a log-in banner on CSAT.

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.

NPPD has a retention schedule approved by NARA for data submitted into CSAT[14] and is currently working on a comprehensive records schedule for all records generated under CFATS. NARA job number N1-563-07-7 specifies that:

- NPPD will destroy/delete inactive files in CSAT six years after a user account is terminated or when a file is no longer needed for investigative or security purposes (i.e., as part of an ongoing investigation or a security incident), whichever is later.
- NPPD retains records associated with Top-Screen assessments, SVAs, and SSPs in CSAT for 10 years from the date the facility is no longer active (i.e., no longer covered under CFATS regulations).

The CFATS Help Desk and Tip Line are covered as input/source records under GRS 20, Electronic Records, item 2b (N1-GRS-87-5 item 2b). CFATS Help Desk phone calls are recorded for training purposes and to ensure the issues presented during the call are preserved completely and accurately. CFATS Tip Line voicemails are transcribed and tracked as a support ticket for further NPPD inquiry. All recordings are deleted after 90 days. The voicemail system used by the CFATS Tip Line, like most modern voicemail systems, will automatically record the phone number from which the call originated. Because the CFATS Tip Line is designed to collect tips from the public anonymously, the phone number is deleted permanently from the voicemail system after the verbal message is transcribed. The phone number recorded by the automated system is not otherwise transcribed, saved, or maintained.

[14] NARA job number: N1-563-07-7.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: The retention of PII for a longer time period than is relevant and necessary can introduce privacy risks such as the unauthorized use or disclosure of PII.

Mitigation: NPPD is consolidating its records retention schedules to reflect the ongoing regulatory process and recognizes that regulation requires regular communication be maintained between DHS and chemical facilities. To mitigate the risk of excessive retention of PII associated with CFATS records, NPPD maintains PII only as long as necessary to properly track, record, and manage efforts of DHS to ensure that chemical facilities comply with Section 550 requirements. Section 8.0 of this PIA details the security measures used to safeguard the information. These security measures protect information throughout its lifecycle.

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.

NPPD does not share PII outside of DHS on a routine basis. However, as appropriate, NPPD does share facility information collected under CFATS with designated DHS, federal, state (e.g., HSAs), local, territorial and tribal government officials. These designated officials can access CSAT survey data (e.g., data extracted from the CSAT Top-Screen and SVA) aggregated into a reporting and mapping tool, the CFATS Share application, based on their geographic area of interest.

As appropriate, NPPD does share the contact information of designated individuals (including, but not limited to facility addresses/locations and phone numbers, as well as facility points-of-contact' identities, phone numbers and email addresses) with federal, state, local, tribal and territorial government officials who demonstrate a need-to-know to carry out their official government responsibilities related to national security, chemical security, and/or infrastructure security. This sharing enables federal, state, local, tribal and territorial government officials to engage in appropriate infrastructure security efforts, such as responding to natural or man-made disasters in a specific geographic area, and collaborating with NPPD and high-risk chemical facilities.

NPPD also shares contact information of designated individuals and facility points-of-contact with select non-government entities, such as first responders, regulated chemical facilities, private sector working groups and other designated individuals who demonstrate a

need-to-know to carry out essential national security, chemical security and/or infrastructure security functions. This sharing of contact information of designated individuals and facility points-of-contact enables appropriate national security, chemical security and infrastructure security collaboration.

Additionally, PII of CSAT Users is shared with other CSAT Users from the same facility who have access to facility-specific information. This is done to ensure that access to CSAT, CSAT registered user roles and entity user lists are accurate and up-to-date. A CVI Authorized User's Status will be shared with other CVI Authorized Users.

Finally, NPPD makes available basic user information of CSAT Users and CVI Authorized Users to the CFATS Help Desk vendor in order to provide better customer service in a more time-efficient manner. Information collected via the CFATS Tip Line is not shared externally on a routine basis.

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

The sharing of contact information, and the status of CSAT Users and CVI Authorized Users outside of DHS, are compatible with the Routine Uses described in DHS/All—004 Privacy Act System of Records Notice, General Information Technology Access Account Records System.

6.3 Does the project place limitations on re-dissemination?

NPPD does not share PII outside of DHS on a routine basis; however, when PII is shared, the Department expects recipients to re-disseminate only with individuals that have a need-to-know. All DHS users of IT systems supporting the CFATS Program are required to comply with written rules of behavior. These rules of behavior are consistent with IT security policy and procedures set forth in DHS Directive 140-1 (Information Technology Systems Security), DHS Sensitive Systems Policy Directive 4300A, and the DHS 4300A Sensitive Systems Handbook, and include rules to protect against the disclosure of sensitive information to unauthorized persons or groups. Additionally, the third party vendor for the CFATS Help Desk, all Call Center Service agents and user management staff, are required to sign non-disclosure agreements as a condition of their contracts.

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

PII will not be routinely shared outside of the Department. NPPD will vet and analyze any non-routine requests for PII on a case-by-case basis as necessary prior to dissemination. NPPD will clearly document each instance of external information sharing in a report.

Moreover, CSAT has detailed audit logs that show users' activities while logged into the system; the logs may be used to identify unauthorized disclosures of information outside of the Department.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Privacy risks identified include the risk of unauthorized disclosure and subsequent misuse of PII.

Mitigation: All DHS users of IT systems supporting the CFATS Program are required to comply with written rules of behavior regarding system access, passwords and other access controls, data protection, incident reporting, and accountability. PII will not be routinely shared outside of the Department; however, if PII is shared externally with non federal individuals, the risk will be mitigated by limiting data to only what is minimally required and to individuals with a need-to-know. Except in exigent and emergency circumstances, CVI may only be provided to CVI Authorized Users who have completed CVI Authorized User Training and who have a need to know the specific CVI. The third-party vendor supporting the Help Desk may not use CFATS information for any purpose beyond responses to Help Desk inquiries. The third-party vendor for the CFATS Help Desk, all Call Center Service agents and user management staff, are required to sign non-disclosure agreements as a condition of their contracts. Additionally, NPPD will vet and analyze any requests for external sharing of information on a case-by-case basis, as necessary, prior to dissemination. NPPD will clearly document each instance of external information sharing in a report.

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.

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

Individuals may have access to certain PII that they have provided to NPPD under CFATS. For example:

- CSAT and CHEMS users can access their PII by logging in to the relevant system.
- CVI Authorized Users can access their PII by retaking the CVI Authorized User Training and creating a new record.

To request access to all other PII held by NPPD under CFATS, individuals may request a copy of their PII by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to the NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 25028. Individuals may obtain directions on how to submit a FOIA/PA request 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?

Users can correct certain inaccurate or erroneous PII by logging in to the relevant system or writing to the NPPD FOIA Officer at 245 Murray Lane SW, Washington, D.C. 25028. CVI Authorized Users can correct inaccurate or erroneous PII by retaking the CVI Authorized User Training and creating a new record.

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

Individuals are notified of the procedures to correct information through this PIA and applicable SORNs. Individuals are also able to review the procedures for correcting their information in the CSAT system in publicly available CSAT User Guides, or by calling the CFATS Help Desk for instructions.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Individuals may be unaware of or not understand their redress options.

Mitigation: Many risks associated with redress are mitigated by the individuals' ability to update their information by accessing the relevant system or retaking the CVI Authorized User Training. A CVI Authorized User Account Management application is in development and will allow a CVI Authorized User to update his/her CVI training record, obtain an additional copy of his/her CVI certificate and submit CVI-related forms. Once the CVI Authorized User Account Management application is deployed, it will eliminate the need to duplicate records in order to update user information. As described in part 7.1 above, individuals may correct their PII at any time during which NPPD possesses and uses their contact information. Both CSAT and CVI Authorized User information are synchronized with CHEMS on a daily basis, so any corrections made in those systems will also be reflected in CHEMS.

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?

All CFATS systems are protected against misuse and were developed under Directive DHS 4300, in which DHS identifies specific techniques and procedural safeguards for DHS systems. These systems are capable of auditing all users and NPPD analyzes the audit logs regularly to determine if any misuse or incident has occurred. The audit trails are protected from actions such as unauthorized access, modification, and destruction that would negate the forensic value of the audit trails. Any security or privacy incidents are reported to and managed by NPPD.

All DHS users of IT systems supporting the CFATS Program are required to comply with written rules of behavior regarding system access, passwords and other access controls, data protection, incident reporting and accountability. These rules of behavior are consistent with IT security policy and procedures within DHS Directive 140-1 (Information Technology Systems Security), DHS Sensitive Systems Policy Directive 4300A, and the DHS 4300A Sensitive Systems Handbook.

The third-party vendor supporting the Help Desk may not use CFATS information for any purpose beyond responses to Help Desk inquiries. The third-party vendor for the CFATS Help Desk, all Call Center Service agents and user management staff, are required to sign non-disclosure agreements as a condition of their contracts. The CFATS Help Desk uses role-based access, and uses a Secure Sockets Layer (SSL)-encrypted web-form. Moreover, the CFATS Tip Line voicemail recordings are only accessible to authorized Help Desk personnel.

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

All federal personnel with access to CFATS Share receive privacy and security training by their respective agency. Within NPPD, all personnel undergo privacy training, which includes a discussion of Fair Information Practice Principles (FIPPs) and instructions on handling PII in accordance with FIPPs and DHS privacy policies. Adherence to DHS privacy training requirements is audited by the appropriate DHS Privacy Officer. The NPPD Office of Privacy also conducts ad hoc privacy training for NPPD personnel. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting PII which is being processed. All IT security training is reported as required by FISMA.

All individuals who want to become CVI Authorized Users must complete an HTML-based online training program that is accessible through CSAT.

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

The systems supporting CFATS have controls in place to limit access to PII based on user roles and responsibilities, need-to-know, least privilege and separation of duties.

Representatives of chemical facilities need to complete the User Registration process to obtain access to CSAT (https://csat-registration.dhs.gov). Once the user completes the registration form, he or she must send the completed form via fax or mail to NPPD for approval and account creation. Rules which govern a user's access to the system are applied by the system automatically, based on the user's assigned role. Categories of user roles will be approved by the CSAT Information Systems Security Officer (ISSO), and any changes in user roles will need approval by the CSAT ISSO prior to access.

CSAT has no capability to support remote access through dial-in connections. Remote access from the Internet for CSAT system administration involves first connecting to the Virtual Private Network (VPN) capability, which complies with this remote access control in the following ways:

- VPN connections;
- Two-factor authentication; and
- Prohibiting split tunnel operation.

Following a successful VPN connection, CSAT system administrators are further restricted and comply with controls such as:

- Restrict remote access from specific computers to the CSAT Juniper SSL VPN Appliance by the CSAT firewall; and
- Require two-factor authentication for connections from the CSAT Juniper SSL VPN Appliance (a Federal Information Processing Standard (FIPS) 140-2 compliant solution) to specific CSAT computers.

To protect against unauthorized access to the data during a routine transfer of PII from CSAT to CHEMS, CHEMS employs several security measures, such as enhanced Cisco Intrusion Detection System/Intrusion Prevention System (IDS/IPS) and Juniper FIPS 140-2 SSL VPN encryption.

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?

There are Memoranda of Agreement (MOA) governing the services between DHS/NPPD and the Department of Energy's national research laboratories, which currently operate the systems supporting the CFATS Program.

Responsible Officials

David Wulf, Director
Infrastructure Security Compliance Division
National Protection and Programs Directorate
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security