Privacy Impact Assessment Update
for the

Chemical Facility Anti-Terrorism Standards (CFATS)

DHS/NPPD/PIA-009(a)

August 12, 2016

Contact Point
David Wulf
Office of Infrastructure Protection
National Protection and Programs Directorate
(703) 603-4778

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

Abstract

The Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) is updating the Chemical Facility Anti-Terrorism Standards (CFATS) Program's Privacy Impact Assessment (PIA) to account for changes to the program since the publication of the program's most recent PIA on July 26, 2012. This PIA Update reflects changes to the Chemical Security Assessment Tool, statutory requirements of the *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014*, and updated records retention schedules.

Overview

The *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014*, commonly referred to as the Chemical Facility Anti-Terrorism Standards (*CFATS) Act of 2014*, replaces Section 550 of the Department of Homeland Security (DHS) Appropriations Act of 2007, authorizing DHS to regulate the security of covered chemical facilities.

The Department established a risk-based approach for identifying and securing covered chemical facilities. A covered chemical facility is one that the Department identifies as a chemical facility of interest[1] and meets the risk criteria developed under 2102(e)(2)(B) of title XXI of the Homeland Security Act of 2002 (as amended). If a facility is determined to be a covered facility, the facility must implement a Site Security Plan, Expedited Approval Program, or Alternative Security Program, which must be approved by the Department. Certain chemical facilities, such as facilities regulated under the Maritime Transportation Security Act of 2002, are exempt from CFATS.

Reason for the PIA Update

The reason for this PIA Update is to reflect updates to CFATS since the previous PIA for the program, published on July 26, 2012.[2] The following specific updates are based on enhancements to the Chemical Security Assessment Tool (CSAT) suite of applications, programmatic changes resulting from the *CFATS Act of 2014*, and general updates to the CFATS program.

---

[1] The term 'chemical facility of interest' means a facility that holds, or that the Department has a reasonable basis to believe holds, a chemical of interest, as designated under Appendix A to part 27 of title 6, Code of Federal Regulations, or any successor thereto, at a threshold quantity set pursuant to relevant risk-related security principles; and is not an excluded facility.

[2] *See* DHS/NPPD/PIA-009 – Chemical Facilities Anti-Terrorism Standards, *available at* www.dhs.gov/privacy. Note that the CFATS Personnel Surety program is addressed in a separate PIA. *See* DHS/NPPD/PIA-018 – Chemical Facilities Anti-Terrorism Standards Personnel Surety, *available at* www.dhs.gov/privacy.

1. The Chemical Facility Management System (CHEMS) was decommissioned and replaced by the Chemical Security Evaluation and Compliance System (CHEMSEC).
2. The *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014* (commonly referred to as the *CFATS Act of 2014)* now authorizes the CFATS program.
3. The *CFATS Act of 2014* requires the Department to establish and implement a procedure under which any employee or contractor of a chemical facility of interest may submit a report to the Department regarding a violation of a requirement under the CFATS program. Additionally, the Act prohibits any owner or operator of a chemical facility from retaliating against an employee for reporting a CFATS violation to the Department.
4. The CFATS Help Desk and Tip Line were originally covered under the National Archives and Records Administration (NARA) General Records Schedule (GRS) 20, *Electronic Records*, item 2b. That GRS has since been superseded by GRS 4.3, *Input Records, Output Records, and Electronic Copies*, item 020.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

The *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014* (December 18, 2014)[3], or the *CFATS Act of 2014* (Pub. L. No. 113-254, 6 U.S.C. 621, et seq.). The CFATS Act of 2014 amended the Homeland Security Act of 2002[4] (6 U.S.C. 101 et seq.) with the addition of Title XXI – Chemical Facility Anti-Terrorism Standards – authorizing the Department to regulate chemical facilities of interest.[5]

SORN coverage has not changed since the previous PIA was published on July 26, 2012, and is still provided by DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System and DHS/ALL-004 General Information Technology Access Account Records

[3] *See* Pub. L. 113-254, 128 Stat. 2898, Dec. 18, 2014, is available at: https://www.congress.gov/bill/113th-congress/house-bill/4007?q=%7B%22search%22%3A%5B%22HR+4007%22%5D%7D (CFATS Act of 2014).
[4] *See* Pub. L. 107-296 Stat. 2135, Nov. 25, 2002 is available at: https://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf (Homeland Security Act of 2002).
[5] *See* Section 2101(2) of the Homeland Security Act of 2002, as enacted on December 18, 2014, defined chemical facility of interest as a facility that holds, or that the Secretary has a reasonable basis to believe holds, a chemical of interest at a set threshold quantity pursuant to relevant risk related security principles and is not an excluded facility.

System.

Characterization of the Information

Though the *CFATS Act of 2014* requires the Department to establish and implement a procedure that will allow employees and contractors of a chemical facility of interest to submit reports regarding violations of CFATS programmatic requirements, the type of data collected under the CFATS Program has not changed since the previous PIA was published on July 26, 2012.

Uses of the Information

Implementation of CHEMSEC

CHEMSEC is the Government-facing case management tool that replaced CHEMS in December 2013. CHEMS was an individual stand-alone system, whereas CHEMSEC has been integrated into the CSAT[6] suite of applications. CHEMSEC provides users with a consolidated interface for tracking ongoing activities, documentation, and facility status as well as managing inspector activities such as facility visits, vehicle management, survey approval reviews, and other supporting processes. CHEMSEC also serves as the repository for information collected during interactions with covered chemical facilities**.**

Specifically, CHEMSEC:

- Receives routine transfers of information from CSAT such as names, phone numbers, and email addresses of facility POCs;
- Securely stores correspondence between NPPD and covered chemical facilities; and
- Serves as the repository for information collected by NPPD employees during personal interactions with covered chemical facilities

Compliance with updated whistleblower protection requirements

The *CFATS Act of 2014* requires the Department to provide an avenue for employees or contractors of chemical facilities of interest to report security violations. The Act prohibits any owner or operator of a chemical facility of interest from retaliating against an employee for reporting a CFATS violation to the Department. Individuals may report violations anonymously under CFATS to the CFATS Tip Line, which has proper procedures and protections in place to safeguard the identity of whistleblowers, should a whistleblower choose to disclose it.

The identity of an employee or contractor of a chemical facility of interest who reports a

[6] *See* DHS/NPPD/PIA-009 – Chemical Facilities Anti-Terrorism Standards, *available at* www.dhs.gov/privacy.

potential violation, should they choose to disclose it, will be kept confidential unless disclosure is unavoidable or is compelled by a court order. In these instances, the Department will attempt to contact the whistleblower to inform him or her of the disclosure.

Privacy Risk: There is a risk that the identities of whistleblowers may be inappropriately accessed or disclosed.

Mitigation: The Department's "Potential CFATS Violation Reporting Standard Operating Procedures" dictates that NPPD use a Whistleblower Checklist to record and track all actions taken related to each whistleblower report. In the interest of maintaining confidentiality, access control measures have been implemented on the whistleblower folders to restrict access to only DHS authorized personnel.

The risk of inappropriate access is mitigated through the use of access controls that restrict access to the whistleblower folders. Logical and physical security boundaries have also been put into place to safeguard the network. These protective boundaries include, but are not limited to, the use of a Trusted Internet Connection (TIC), which serves as an external firewall that encrypts data at the transport layer security (TLS) level.

Notice

There have been no changes regarding notice since the previous PIA, published on July 26, 2012.

Data Retention by the project

The CFATS Help Desk and Tip Line were covered under National Archives and Records Administration (NARA) General Records Schedule (GRS) 20, *Electronic Records*, item 2b. That GRS has since been superseded by GRS 4.3, *Input Records, Output Records, and Electronic Copies*, item 020. No additional changes have been made related to the retention of CFATS records. CFATS Help Desk and Tip Line data continues to be destroyed immediately after data have been entered or otherwise incorporated into the master file or database and verified, but longer retention may be authorized if required for business use.

Information Sharing

Information sharing practices have not changed since the previous PIA, published on July 26, 2012.

Redress

The procedures for accessing and/or correcting information have not changed since

the previous PIA, published on July 26, 2012.

Auditing and Accountability

Auditing and accountability procedures have not changed since the previous PIA, published on July 26, 2016.

Responsible Official

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

Approval Signature

Original signed copy on file at the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security