Privacy Impact Assessment Update
for the

Chemical Security Assessment Tool (CSAT)

May 25, 2007

Contact Point
Matt Bettridge
Infrastructure Partnership Division
703-235-5495

Reviewing Official
Hugo Teufel, III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

This is an update to the previous Chemical Security Assessment Tool Privacy Impact Assessment (PIA) in order to describe the additional web site functionality, the new eligibility requirements for CSAT users, and the deployment of the CSAT Help Desk. CSAT collects personally identifiable information from CSAT users and/or CVI web site users. Further, the CSAT Help Desk may collect contact information from both CSAT users requesting basic CSAT IT support or from the general public inquiring about the CSAT program.

Introduction

The Department of Homeland Security/National Protection & Programs Directorate (NPPD) (formerly Preparedness Directorate)/Chemical Security Assessment Tool (CSAT) is a suite of applications for use by applicable chemical sector entities as described in Section 550 of Public Law 109-295, which provides DHS the responsibility and authority to regulate high risk chemical facilities. This is an update to the previous Chemical Security Assessment Tool Privacy Impact Assessment (PIA) in order to describe the additional web site functionality, the new eligibility requirements for CSAT users, and the deployment of the CSAT Help Desk. The updates to CSAT include the following: Chemical-Terrorism Vulnerability Information (CVI) Training; the CVI Website; the Security Vulnerability Assessment (SVA); the Site Security Plan (SSP); new CSAT user roles – Reviewer, and Authorizer; the CSAT security policy revision which allows U.S. Persons to become CSAT users; and the CSAT Help Desk.

CVI Website

The CVI Website is a new component of the CSAT suite of tools. The CVI Website will host general CVI materials. The CVI Website provides these materials to support CSAT users completing the Top Screen, Security Vulnerability Assessment (SVA), and Site Security Plan (SSP). CSAT will comply with encryption requirements and use Secure Sockets Layer (SSL) for users accessing the system. CSAT will host the CVI Website on CSAT servers. The CSAT servers are protected as are all other parts of the CSAT database (as described in the CSAT PIA). Access to the CVI Website requires a valid user ID, password, granted exclusively by the Chemical Security Compliance Division (CSCD). Only CVI trained and authorized individuals, as well as CSAT users, may access the CVI Website. The CVI Website itself does not collect any Personally Identifiable Information (PII); however, only the authorized CVI web site users who have taken required training and submitted necessary documentation may access the CVI Website.

CVI Training

The CVI Training is an HTML based online training module accessible through the DHS website, http://www.dhs.gov/chemicalsecurity. Upon completion of the CVI Training a blank, user information form will be provided so that the individual may fill out name and business contact information, but CVI will not maintain this information in this format. CVI Training is required of all CVI web site users. The CVI web site allows potential CSAT users additional resources for filling out required assessments. Potential CVI web site users include chemical facility/entity personnel; federal, state, and local government employees; and contractors. Potential CVI website users will access the training module via the web, launch the training, and click through a series of screens that provide the necessary CVI information for a user to learn and become authorized.

Upon completion of the online training, individuals will enter their data (using SSL) into a certificate of completion, a non-disclosure agreement, and a coversheet. The non-disclosure agreement requires potential CVI web site users to submit their name and the Authorized Entity to which they are affiliated. Part of the non-disclosure agreement is the CVI Authorized User Information form. Information collected on this form is more detailed and includes the following:

First Name:
Middle Initial: (optional)
Last Name:
Organization:
Organization Type:
Business Address:
- City:
- State:
- Zip Code:
- Telephone:
- E-mail:

Describe Official Duties:
Direct Supervisor's Name:
Supervisor's Telephone Number:
Government Agency: (If applicable)

The individual must enter the data, then email, or print and fax these forms to the CSCD CVI Security Officer. CSCD will then authorize the individual to be a CVI user. The CSCD CVI Security Officer will send an email (to the email address submitted by the individual) with a software token, username, and password for the CVI Website to all individuals who complete the CVI Training and submit the information to the CSCD CVI Security Officer.

The Security Vulnerability Assessment (SVA)

The Security Vulnerability Assessment (SVA) is a new application of the CSAT. The SVA is a tool used for the evaluation of the potential consequences and vulnerabilities of specific critical facility assets against a standard set of potential attack scenarios. The CSAT Top-Screen collects

information, but not PII, and uses it to identify critical assets selected for the SVA. CSAT uses the SVA results to assign the facility a tier level and identify security gaps that the facility will need to address in the SSP.

The Site Security Plan (SSP)

The Site Security Plan (SSP) is a new application of the CSAT. The SSP is a tool that facilitates the collection of security measures, activities, and systems for judging compliance against the Risk Based Performance Standards (RBPS). SSP does not collect PII. DHS, in compliance with Section 550, will use the SSP to determine if CSAT covered facilities are managing their risks according to their tier level. DHS will evaluate the security measures provided in the SSP by using backend analytics based on the facility tier, identified security gaps from the SVA, and specific security measures reported in the SSP as compared to the RBPS. These analytic capabilities result in the ability to prioritize SSPs that may require further review by subject matter experts.

New CSAT Roles Reviewer & Authorizer

CSAT has added the two new user roles: Reviewer; and Authorizer. These new user roles are being added to the following CSAT applications: Top Screen; SVA; and SSP. Adding the new role of Reviewer, allows a facility to designate an individual who can review the assessment for quality and accuracy. The role of Authorizer allows a facility to designate an individual who not only reviews the responses for quality and accuracy, but is also able to make any necessary changes or updates to the assessments prior to submitting to DHS.

Reviewer – The Reviewer role exists in the CSAT Top Screen; SVA; and SSP applications and has "read only" access. In CSAT, the Preparer and/or Submitter has the option to designate any number of individuals to review facility specific information prior to its submission into CSAT. This role is known as the Reviewer. Any number of Reviewers may be designated for one facility; but Reviewers must be designated to a facility.

PII collected for the Reviewer is identical to that collected for the Preparer and includes the following:

-Name (First, Middle Initial, Last)
-Business Mailing Address
-Business Phone Number (including extension if required)
-Business Email address
-Acknowledgement of U.S. Citizenship (U.S. Citizens may participate)
-Confirmation Reviewer is domiciled in the U.S. (Non-U.S. Citizens who are legally domiciled in U.S. may be Reviewers).

Authorizer – The CSAT role of "Authorizing Person" as described in the CSAT PIA shall be known hence forth as the "Authorizer." The Authorizer's original responsibilities were to

designate an individual to submit the assessment to DHS, the Authorizer has CSAT user access and update functionality.

PII collected for the Approver is identical to that of the Submitter and includes the following:

-Name (First, Middle Initial, Last)
-Business Mailing Address
-Business Phone Number (including extension if required)
-Business Email address
-Acknowledgement of U.S. Citizenship (U.S. Citizens may participate)
-That the Authorizer is, or is designated by, an Officer of the Corporation
-Confirmation that the Authorizer is domiciled in the U.S. (Non-U.S. Citizens who are legally domiciled in the U.S. may be Authorizers).

CSAT Security Policy

The CSAT applications now allow anyone who is legally domiciled in the U.S. or is a U.S. Citizens (USC) no matter whether he is domiciled in the U.S. or not, to become a CSAT user. CSAT is now consistent with Section 550 of Public Law 109-295. Previously, the CSAT Security Policy only allowed USCs to be CSAT users.

CSAT Help Desk

The CSAT Help Desk is a newly established call center that provides CSAT technical support, and CSAT program information. The CSAT Help Desk is provided for CSAT users and general public inquiries.

The Help Desk is staffed by DHS personnel, who are either federal employees or contractors, and a third party vendor, who is under contract with the Department of Energy and pursuant to a memorandum of understanding (MOU) with DHS. The CSAT Help Desk responds to callers using a tiered system in order to manage the work most effectively. Initially, all calls to the CSAT Help Desk are received by a third party vendor trained to respond to questions and provide information as scripted. The vendor makes a record of the call by opening a Help Desk Ticket via a web-based software program.

A third party vendor is also utilized to provide scripted information for basic CSAT IT support and general CSAT inquiries. The third party vendor that supports the CSAT Help Desk is neither part of CSAT nor has internal access to CSAT. Only onsite CSAT personnel (DHS employees and contractors) have internal access to CSAT.

If the information being requested is beyond the scope of this vendor, the call is escalated to onsite CSAT staff (DHS employee or contractor). The onsite CSAT staff may then access the ticket information via the web and address the Help Desk ticket. If at this point the CSAT staff is unable to resolve the Help Desk ticket, the issue may again be escalated to the CSAT Program Manager (by the same means) for resolution.

The CSAT Help Desk may collect contact information from any caller regardless of CSAT registration/participant status. This information is collected for follow up purposes and is provided voluntarily by the individual caller. CSAT Help Desk collects the information using an industry standard, web-based software application designed for help desk ticket tracking and contact support. Information collected includes the following:

- Account Information (Facility)
  - Company Name
  - E-mail Address (of caller)
  - CSAT Registration Number (if they already have one)
  - Phone Number
  - Fax Number
  - Industry (usually Chemical)
  - Physical Address
    - Street Address
    - City
    - State
    - Zip Code
    - Country
  - Website
- Contact Information
  - First Name
  - Last Name
  - E-mail Address
  - Phone Number
  - Mailing Address
    - Street Address
    - City
    - State
    - Zip Code
    - Country
- Case (Ticket) Information
  - Case Number
  - User Category (Preparer, Submitter, etc.)
  - Case Status (Open, Closed, Escalated. etc.)
  - Case Origin (Phone, E-mail, Fax)
  - Priority
  - Subject
  - Description
  - Case Reason
  - Solution Title
  - Solution Details

Reason for the PIA Update

This CSAT PIA Update addresses the potential collection of PII by DHS as a result of CSAT's added applications and functionality, security policy change, and deployment of the CSAT Help Desk. Additionally, CSAT has two new user roles, the Reviewer and Authorizer, for which individuals must register with CSAT and provide PII in order to utilize. The CSAT Help Desk may also collect contact information from callers in order to most effectively service those requesting IT support or CSAT program information.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

The CSAT application and functionality update affects the amount, but not the type of personally identifiable information (PII) collected. Because there are added user roles and applications, CSAT will collect a larger volume of PII. Some PII may be collected more than once from the same individual in order to handle the given request; however, no new types of PII will be collected.

The CSAT Help Desk may collect PII from CSAT users or non-user individuals inquiring about the CSAT. The caller must submit information voluntarily and the information is used for contact and support purposes. Contact information collected may include any the following: first and last name; phone number; email address; and postal mailing address. The CSAT Help Disk will open a Help Desk Ticket (assign a case (tracking) number) for each call (incident) received.

DHS will employ the use of a third party vendor to support certain basic functions of the CSAT Help Desk. This third party division of the Help Desk is neither part of the internal CSAT system, nor will they have internal access to CSAT. Any information collected by the third party vendor is property of DHS and may not be disseminated. CSAT has not changed its policy on internal or external sharing, or data mining.

Uses of the System and the Information

CSAT collects PII from individuals attempting to become CSAT users and may also collect PII from individuals calling the Help Desk requesting technical assistance with or further information about the program. DHS uses this information for contact and support purposes. Anyone calling the Help Desk may also submit contact information (PII) for contact, general support purposes, and for follow-up.

CSAT now has the added functionality of two new user roles (Reviewer and Authorizer), and a supporting CSAT Help Desk. The individuals participating as Reviewer or Authorizer must register with CSAT and therefore provide PII.

Adding the new role of Reviewer, allows a facility to designate an individual who can review the assessment for quality and accuracy. The role of Authorizer allows a facility to designate an individual who not only reviews the responses for quality and accuracy, but is also able to make any necessary changes or updates to the assessments prior to submitting to DHS.

Retention

The retention schedule for CSAT data, both CSAT user information and Help Desk contact information will remain consistent with the proposed NARA retention schedule as described in the published CSAT PIA.

Internal Sharing and Disclosure

CSAT Internal Sharing and disclosure policies will remain consistent with the existing CSAT PIA. No new changes to internal sharing or disclosure exist at this time.

External Sharing and Disclosure

The third party vendor only shares first tier Help Desk information with DHS personnel or contractors. This third party vendor may not use this information for any purpose beyond the first tier responses to Help Desk Inquiries. CSAT User information will not be shared with the third party vendor. All information collected via the CSAT Help Desk is DHS property and is not disseminated.

Notice

Potential CSAT users and authorized users will be provided with a Privacy Act Statement (5 U.S.C. § 552a(e)(3)) on the forms collecting personally identifiable information. The Help Desk Information is maintained under the DHS/All-002 Privacy Act System of Records Notice, DHS mail lists and contact information, 69 FR 70460 published on September 22, 2004. As previously noted in the original CSAT PIA, the CSAT user information is covered by the DHS/All – 004 Privacy Act System of Records Notice, General Information Technology Access and Account Records, 71 FR 78449 published on December 29, 2006.

Individual Access, Redress, and Correction

Individual access, redress, and correction (including the addition of the CSAT Help Desk) will remain consistent with the current CSAT PIA. Individual access, redress, and correction procedures and policy have not changed as a result of this update.

Technical Access and Security

CSAT technical access and security will remain consistent with the current CSAT PIA. CSAT technical access and security has not changed as a result of this update.

DHS NPPD IT Security as well as the Department of Energy (DOE) Oak Ridge National Laboratory (ORNL) IT Security has properly reviewed and approved the third party vendor (Help Desk) contract, statement of work, and non-disclosure or confidentiality agreements, and all other aspects of physical and data security. The third party vendor (Help Desk) does not have access to any other part of CSAT information technology. All information collected by the third party vendor (Help Desk) may not be used by the third party vendor for any purpose beyond responding to first tier Help Desk issues. This CSAT system has been Certified and Accredited by the NPPD CIO and has an Authority to Operate as of March 31, 2007.

Technology

CSAT has added applications and functionality based on its existing framework. CSAT Help Desk collects the information using an industry standard, web-based software application designed for help desk ticket tracking and contact support.

Responsible Official

Matt Bettridge

National Protection & Programs Directorate

Department of Homeland Security

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security