Privacy Impact Assessment
for the

Chemical Security Assessment Tool (CSAT)

March 27, 2007

Contact Point
Matthew Bettridge
DHS/PREP/IP
(703) 235-5495

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Abstract

The Department of Homeland Security / Preparedness Directorate / Infrastructure Protection Division (DHS/PREP/IP) will deploy and maintain the Chemical Security Assessment Tool (CSAT). The CSAT is designed to be a web-based self-assessment tool for use by chemical facilities. The CSAT will collect and maintain information for a Point of Contact (POC) for each participating facility. This PIA covers the new CSAT system.

Introduction

Section 550 of Public Law 109-295 provided the Department of Homeland Security (DHS) the responsibility and authority to regulate high risk chemical facilities. Further, it requires the Secretary of the Department of Homeland Security (the Secretary) to identify high risk facilities and provide for the protection of the information regarding and provided by those facilities. Currently, the federal government does not possess the asset specific risk data to regulate high risk chemical facilities. CSAT has been identified by DHS/PREP/IP as the Information Technology (IT) system to obtain and quantify this key risk data from facilities covered under the Statute. It is the intent of the Secretary to begin the assessment of the chemical sector upon the issuance of the interim final regulations. Interim final regulations are required to be issued 6 months from the date of enactment, or April 4, 2007. In conjunction with the release of the interim final regulation that will be published in the Federal Register, Infrastructure Protection will inform the public and private sector of its goals and purpose via public announcements, participation in trade shows, and other means of public relations.

To complete their duties under Section 550, Infrastructure Protection compiled a list of chemical companies that could potentially be considered to have high risk chemical facilities. Companies may receive a letter informing them of their potential risk under the new Section 550 of Public Law 109-295. The letter will include a notification code, to be used in the registration process. If a company independently determines that it needs to complete the assessment for a high risk chemical facility, but has not received a mailing with a notification code, the company may presumptively register its facility by accessing the CSAT website[1].

Two parts of the CSAT may be used to collect Personally Identifiable Information (PII). The first part is the User Registration and the second part is the Top Screen, a self-assessment tool. In order to gain access to the Top Screen, the User Registration must be completed and approved by Infrastructure Protection. An internal CSAT database then maintains the User Registration information and is accessible only through onsite, DHS, authorized personnel.

The User Registration part of CSAT collects information on three different individuals given their relationship with CSAT. The three individuals are the Submitter, the Preparer, and the Authorizing Person. The Submitter is an individual that is certified by the company or corporation to formally submit the regulatory data to DHS. The Submitter must be a United States (U.S.) Citizen, an officer of the company (or equivalent), and domiciled in the United States. The Preparer must also be a U.S. Citizen and is the individual authorized to enter data into the CSAT

[1] http://www.dhs.gov/chemicalsecurity

Top Screen (on-line screening tool); however, the Preparer is not authorized to formally submit the data on the company's behalf. The Preparer should be a person familiar with the facility in question. The Authorizing Person is the official company representative that identifies and verifies the individuals who will maintain the CSAT user roles, the Submitter and the Preparer, on behalf of the company. A facility may choose to designate a single person to be both the Submitter and Preparer. Many chemical companies are multinational corporations. Knowingly providing incomplete or false information is a punishable offense, and therefore the program has required that the Submitters and Preparers be US Citizens and be subject to US law.

The Submitter must complete the User Registration form found on the CSAT website. When the Submitter submits the form online, a Portable Document Format (PDF) file is automatically generated. The PDF must then be printed in hard copy and signed by the Submitter and Authorizing Person. Then, the printed and signed User Registration form must either be faxed or mailed to the CSAT program for confirmation. Upon receipt, CSAT will scan the form and verify that it has been signed. Once CSAT scans and confirms the form, unique usernames and temporary passwords are generated and assigned: one to the Submitter and one to the Preparer. The Preparer will then access the Top Screen portion of the CSAT website and provide information on the specifics of the chemical company, including but not limited to types of chemicals stored and produced, location of company, and safety measures. The Submitter then logs into the Top Screen and submits the completed form. Based on the information submitted, a chemical risk level is determined using a tier designation system. CSAT generates a letter with the final tier designation (risk level) and mails it to the Submitter.[2]

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

The CSAT collects Personally Identifiable Information (PII) on the three following individuals: the Submitter, the Preparer, and the Authorizing Person.

Information collected by the CSAT to issue access for the Submitter includes:

-Name (First, Middle Initial, Last)

-Business Mailing Address

-Business Phone Number (including extension if required)

-Business Email address

-Acknowledgement of US Citizenship (only US Citizens may participate)

-Whether or not the Submitter is an Officer of the Corporation

-Confirmation Submitter is domiciled in US,

[2] A final tier designation is determined. If the company believes the tier determination is incorrect they can petition CSAT for a change.

Information collected by the CSAT to issue access for the Preparer includes:

-Name (First, Middle Initial, Last)

-Business Mailing Address

-Business Phone Number (including extension if required)

-Business Email address

-Acknowledgement of US Citizenship (only US Citizens may participate)

Information collected by the CSAT for the Authorizing Person includes:

-Name (First, Middle Initial, Last)

-Job Title

-Business Phone Number (including extension if required)

The CSAT program creates unique usernames and assigns temporary passwords for CSAT users, such as the Submitter and Preparer, when their accounts are created.

1.2 From whom is information collected?

Information will be collected from individuals who are labeled the Submitter; the Preparer; and the Authorizing Individual. The Submitter is the person who approves the information to be submitted to CSAT. The Preparer provides information on the running of the chemical facility. Facilities may include but are not limited to chemical manufacturing plants, petroleum refineries, liquid natural gas terminals and short storage facilities. The official company representative, known as the Authorizing Individual, verifies that the Submitter and Preparer are authorized to represent their company.

1.3 Why is the information being collected?

Contact information is collected to allow for communications between CSAT and the participant. Acknowledgement of U.S. Citizenship will also be required and collected. Many chemical companies are multinational corporations. In the event that a company knowingly provides incomplete or false information, the Submitters and Preparers will be US Citizens and subject to US law.

1.4 How is the information collected?

The information will be collected only through a web-based registration. Users will be asked to complete the registration, print and sign the form, and mail or fax the form to DHS.

The data collected by the CSAT registration form will be saved electronically by the CSAT web-server and matched against the hard copy once received.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

The Chemical Security Assessment Tool (CSAT) is the system responsible for executing the risk data collection and risk-level determinations under Section 550 of the DHS 2007 Appropriations Statute. Section 550 grants DHS the responsibility and authority to regulate high risk chemical facilities. Interim final regulations are required to be issued 6 months from the date of enactment, or April 4, 2007. It is the intent of the Secretary of Homeland Security to begin the assessment of the chemical sector upon the issuance of the interim final regulations.

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The system was designed to use as little personally identifiable information as possible and still be able to contact those individuals responsible for regulating both the submitted Acknowledgement of U.S. Citizenship will also be required and collected. Many chemical companies are multinational corporations. Knowingly providing incomplete or false information is a punishable offense, and therefore the program has required that the Submitters and Preparers be US Citizens and be subject to US law. Submissions to the CSAT will be protected as allowed by the Section 550 through the enactment of interim final regulations. DHS may classify data on an as-needed basis.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

The PII collected may be used as reference in case further communication is required between CSAT and the chemical facility.

CSAT collects acknowledgement of U.S. citizenship as mentioned in the Advanced Notice of Proposed Rules Making (ANPRM) issued by DHS in December. It was determined that the individual(s) fulfilling the role(s) of the Submitter and/or of the Preparer must be a U.S. citizens. Many chemical companies are multinational corporations. Knowingly providing incomplete or false information is a punishable offense, and therefore the program has required that the Submitters and Preparers be US Citizens and be subject to US law.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Submitter information will not be verified prior to access being granted. The process to issue access will ensure that users solicited by CSAT will have a higher degree of confidence than the users who submit information of their own volition. Specifically, a letter will be mailed to a very broad base of known chemical facilities notifying them that they may be regulated under Section 550. The letter will contain a randomly generated notification code. During the user registration process the facility will be asked to enter the notification code if they have been provided one. Those entities that are not provided a notification code may also be issued access but may be more rigorously scrutinized, prior to the issuance of access.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

CSAT collects a minimum amount of personally identifiable information to reduce the risk that the information may be used improperly. Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable Infrastructure Protection and DHS automated systems security and access policies. Strict controls have been imposed to minimize the risks of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals specifically authorized and granted access by DHS regulations, who hold appropriate access credentials, and who have a need to know the information in the performance of their official duties. The system also maintains a real-time auditing function of individuals who access the system. Classified information is appropriately stored in a secured facility, in secured databases and containers, and in accordance with other applicable requirements, including those pertaining to classified information. Access is limited to properly authorized personnel only. Acknowledgement of U.S. Citizenship will also be required and collected so in the event that a company knowingly provides incomplete or false information, the Submitters and Preparers will be US Citizens and subject to US law.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

Preparedness has proposed a ten year retention schedule for these records.

Until the records in the system have a NARA-approved disposition schedule, the records must be considered permanent and nothing may be deleted.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

An approval request is in process. The Office of Infrastructure Protection/Preparedness is currently working with the DHS Senior Records Officer to develop a disposition schedule which will be sent to NARA for approval.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The proposed records retention schedule is based on the fact that regulatory requirements and company representatives may change over time. The on-going process of DHS regulating (applicable) chemical facilities requires that regular communication be maintained between CSAT and those chemical facilities. Because of the continual regulation over time, extensive records maintenance is critical to the program in order to ensure proper compliance, litigation, and redress as necessary. Retention and destruction policies have been determined in strict accordance with the appropriate guidelines. This ensures that Preparedness retains data no longer than necessary, thereby minimizing any risks associated with the retention of personally identifiable information.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The system will be utilized solely by the Infrastructure Protection division of the Preparedness Directorate of the Department of Homeland Security.

PREP/IP chemical facility regulators and analysts will be the internal entities utilizing the CSAT system.

PREP may share information with the DHS Office of General Counsel (OGC) on an as needed basis for such necessary reasons as litigation.

4.2 For each organization, what information is shared and for what purpose?

If an objection or appeal to the CSAT tier determination occurs, OGC will be privy to the information for litigation and legal purposes.

4.3 How is the information transmitted or disclosed?

Information is shared as printouts and written reports that have first been cleansed to provide only the information that is necessary for the purposes of the report. Information shared will not

include personally identifiable data unless there is a specific requirement to do so, such as litigation. There is currently no expectation that information will be shared for a purpose other than litigation.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Internal sharing of personally identifiable information would only occur in certain instances when the information is required for litigation and other legal purposes. The privacy risks involved with this sharing are mitigated by the controls in place as a function of legal jurisprudence and laws governing information used in legal actions.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

The CSAT will share Submitter's and Preparer's personally identifiable information with the organization submitting the form in order to confirm these individuals are the appropriate people to represent the company.

5.2 What information is shared and for what purpose?

The CSAT will share Submitter's and Preparer's personally identifiable information with the organization submitting the form in order to confirm these individuals are the appropriate people to represent the company.

5.3 How is the information transmitted or disclosed?

CSAT will transmit very limited personally identifiable information to the originating facility via email (i.e. usernames and passwords) and letters (e.g. tier determinations sensitive communications between DHS and the covered facility).

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

User agreements are signed by all individuals that request and receive access to CSAT. The user agreements will reflect the scope of the information shared

5.5 How is the shared information secured by the recipient?

Users agreements will require that PII be secured in accordance with DHS requirements. In the event MOU, contracts, or any other agreement is made it will require that PII be secured in accordance with DHS requirements.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

There is currently no CSAT specific training related to the protection of PII. All information collected through CSAT will have the SBU protections pursuant to Section 550 of P.L 109-295. Specific training is being developed and will be required prior to access being provided.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

At this point in time there is no intention or arrangement for any regular or routine external sharing of information.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Notice is provided in the Systems of Records Notice (71 FR 78446) published in the Federal Register on December 29, 2006. The language is in accordance with the Chemical Facility Anti-Terrorism Standards Proposed Rule, regarding how to obtain a user name and password. A Privacy Act notice will be provided on the webpage.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

To receive access to CSAT, individuals must provide the personal information required to grant access.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

The individual does have the right to consent to using their information for contact purposes. Consent of the individual is implicit. The use of an individual's information is for contact purposes only. Personal information will not be used in any other way.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Due to the limited information required of any Point of Contact (POC), PREP/IP determined that the privacy risk for any individual is minimal with regard to the collection of personally identifiable information for the CSAT.

Collecting information necessary for communication between PREP/IP and a facility submitter or other facility POCs is the primary objective. Notice of an individual's right to privacy, including but not limited to a posted copy of the Privacy Act of 1974, will be provided to all Submitters and Preparers of information. Contact information collected from the CSAT participants will be maintained in a secure database and will not be disseminated.

All submissions to the CSAT will be considered "chemical-terrorism vulnerability information (CVI)", a category of sensitive but unclassified information (SBU), for security purposes by DHS classifications standards; this is a necessary step even when operating on a government portal. The application and its components must adhere to DHS and Preparedness security standards as well as Federal Regulations regarding the types of data collected and stored in CSAT.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures which allow individuals to gain access to their own information?

Any individual may submit a request in writing through the Freedom of Information Act (FOIA) in order gain access to the information collected and maintained on oneself. The procedures for submitting FOIA requests are available in 6 C.F.R. Part 5. A request may also be sent directly to CSAT.

7.2 What are the procedures for correcting erroneous information?

A copy of the submissions to CSAT may be saved as an electronic file on the submitting computer. If the submitter or facility requests a copy of their submission, it will be sent to them in hard copy.

Further, in the event that a facility's information is found to be incorrect, the facility will be required to resubmit the correct information.

7.3 How are individuals notified of the procedures for correcting their information?

The information entered into CSAT by the company will be displayed on the confirmation screen prior company's submission with instructions on how to correct erroneous information.

7.4 If no redress is provided, are alternatives available?

Redress is provided for by a facility completing the top screen or submitting a new user access request.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

The procedural rights of the individual are rudimentary and include the ability to request a copy of the data maintained through FOIA. Correcting any erroneous information may be done so simply by submitting information to CSAT pertaining to the appropriate facility which will consequently be updated.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

The following user communities within IP will have routine and regular end user privileges to CSAT:

- Chemical Security Office (or title to be determined), with Access to Privacy Information

- Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), with Potential Access to Privacy Information

8.2 Will contractors to DHS have access to the system?

Argonne and Oak Ridge National Laboratories are contracted to assist with system production and maintenance, and as such will have access to the system. There is currently an MOU in place with the Department of Energy, for the utilization of both Argonne and Oak Ridge National Labs for the development and maintenance of this system.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, the system is role-based and users will only have access to data determined by their roles. The role(s) given to a user dictates what he/she can see and do within the system.

8.4 What procedures are in place to determine which users may access the system and are they documented?

An individual review and approval process for each user will occur and be documented. Access roles for any non-chemical sector entities or those users who will not maintain a user role as a Submitter or Preparer will be strictly reviewed and considered on a case by case basis.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Submitters and Preparers will not have access to the CSAT database. All other roles will follow an established procedure that will be documented and audited.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

The CSAT system was developed using DHS 4300 policy and guidelines to ensure a high level of data protection. The system will audit all users and audit logs will be analyzed to determine if any misuse or incident is occurring. All users will authenticate using standards set forth by DHS 4300 policy. The CSAT database will be accessible only to those with access to the SIPRNET (SECRET LAN). All users accessing these databases will be cleared to the highest level of classified data stored on the system. These networks have implemented security precautions inherent to the level of classified data and will following hardening procedures set forth in the DHS 4300B. All users are required to sign non-disclosure agreements prior to access to the system.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

There is no privacy related training provided for users in regard to this system. General privacy and security training is, however, part of mandatory training for all DHS employees and contractors.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

The system will be certified and accredited at the SBU and Secret levels prior to implementation and per NIST 800-53 specifications and DHS guidance and regulations. Prior to implementing the system, the IP security office will conduct independent testing of the CSAT system and will complete a Security Assessment Report identifying security control weaknesses. The developer, after consulting with the DHS Program Manager, will verify an Independent Verification & Validation and usability review process and identify an organization to carry that process out.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The CSAT system includes components with different user and data sets. The system design includes access to collected data and system performance data as well. The complete system includes collected infrastructure data and is a high sensitivity system. The limited public access parts of the system would be used to accept submissions of data and maintain in-progress partial submissions (but not to store completed submissions). The IT security requirements will be outlined in detail in the System Security Plan and in accordance with DHS Policy 4300A and DISA specifications. The system will be FIPS 199 and FIPS 200 compliant.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

CSAT is a custom system that leverages available Commercial off the Shelf and Government off the Shelf software wherever possible to reduce costs without negatively impacting the performance and functionality of the system.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The CSAT system was designed around the principles of compartmentalization and redundant layers of security to mitigate the risks inherent in any automated system. In particular, access authorization was partitioned to protect all data in the system including privacy data. The CSAT system implements independent directory services using different technologies to reduce the impact of single failures on the confidentiality of private data.

CSAT must support a large number of participants from multiple organizations, many of which have not undergone an extended and rigorous background check. CSAT users authenticate to Oracle Internet Directory (OID), which accounts can access only the CSAT application, helping to reduce threats to the operating system

CSAT accounts are further limited to working only on CSAT self assessments for their organization. The administration and analysis accounts that have rights to view and modify the OID accounts authenticate to a separate system that uses Active Directory as an authentication service.

Traffic to the system is protected by layered security as follows:

- A firewall that protects the systems from attempts to access ports other than those that have been designated for the application's use.
- A hardware security device that isolates the encryption of the data stream from the applications and from the firewall. The use of a dedicated external device further protects the application from attempts to compromise it through hacker techniques like "hidden" field injections.
- A dedicated Intrusion Detection System/Intrusion Prevention System (IDS/IPS) which monitors the decrypted traffic flowing between the hardware encryption devices and the application. By using a dedicated Secure Sockets Layer/Transport Layer Security (SSL/TLS) appliance and not running an https web server, we eliminate the issue of the traffic going through the IDS/IPS being encrypted and therefore not capable of supporting a security scan.
- Applications reside on hardened servers that have dedicated external log servers to support additional assurance that only proper access is being made to the systems.

9.3 What design choices were made to enhance privacy?

Beyond the physical security restrictions and the network security restrictions, the CSAT system has multiple security mechanisms that have been implemented to provide additional security features. Utilization of login restrictions, session tracking and monitoring, data labeling/tagging of classified information, role based access controls, and advanced auditing ensure proper security of the application. The system hardware and software in place meet all requirements for system and data protection.

Conclusion

The Department of Homeland Security/Preparedness Directorate/Infrastructure Protection Division will deploy and maintain the Chemical Security Assessment Tool (CSAT). The CSAT is designed to be a web-based self-assessment tool for use by chemical facilities to quantify asset specific risk data variables. The system's objective is to obtain and quantify the key risk data from facilities covered under Section 550 to inform the assessment of high risk chemical sites as required under Section 550. Data collected by the system is primarily based on the aspects of facilities, only Points of Contact (POCs) for facilities will provide personal information in order to maintain contact data for communication purposes with the CSAT. Beyond the physical security restrictions and the network security restrictions, the CSAT system has multiple security mechanisms that have been implemented to provide additional security features. It has been determined that because of the system architecture, security features, and the primary nature of data collection and analysis, there is a nominal level of impact to the privacy of the American public.

Responsible Officials

Sandy Ford Page

Privacy Officer, Preparedness

Department of Homeland Security

Matt Bettridge

Project Manager

Approval Signature Page

_____

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security