

REQUEST FOR RECORDS DISPOSITION AUTHORITY		LEAVE B. (NARA use only)	
		JOB NUMBER <i>NI-563-07-7</i>	
To: NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD, COLLEGE PARK, MID 20740-6001		Date Received <i>5/16/07</i>	
1. FROM (Agency or establishment) Department of Homeland Security		NOTIFICATION TO AGENCY	
2. MAJOR SUB DIVISION National Protection and Programs Directorate		In accordance with the provisions of 44 U.S.C 3303a, the disposition request, including amendments is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10.	
3. MINOR SUBDIVISION Chemical Security Compliance Division			
4. NAME OF PERSON WITH WHOM TO CONFER Kathy Schultz	5. TELEPHONE 202-447-5075	DATE <i>5/16/07</i>	ARCHIVIST OF THE UNITED STATES <i>[Signature]</i>
6 AGENCY CERTIFICATION I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached <u><i>X</i> 3</u> page(s) are not needed now for the business of this agency or will not be needed after the retention periods specified, and that written concurrence from the General Accounting Office, under the provisions of Title 8 the GAO Manual for Guidance of Federal Agencies, <input checked="" type="checkbox"/> is not required <input type="checkbox"/> is attached; or <input type="checkbox"/> has been requested.			
DATE 5/7/07	SIGNATURE OF AGENCY REPRESENTATIVE <i>Kathleen A. Schultz</i>		TITLE Senior Records Officer
7. ITEM NO.	8. DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9. GRS OR SUPERSEDED JOB CITATION	10. ACTION TAKEN (NARA USE ONLY)
1	See attached sheet(s) for: Chemical Security Assessment Tool (CSAT)		

SA 10/26/07 Copies sent to Agency, NWMW, &

**U.S. Department of Homeland Security
Headquarters Systems Schedules**

National Protection and Programs Directorate

Chemical Security Assessment Tool (CSAT)

NARA # N1-563-07-7

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. The Chemical Security Assessment Tool (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 (IP) 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.

CSAT's functionality revolves around the need to (1) collect data necessary to determine if a facility is regulated under the interim final rule, (2) determine the extent to which a facility may be regulated through its risk tier designation, (3) provide the facility with a means to conduct an in-depth Security Vulnerability Assessment (SVA) and (4) provide the facility with a means to prepare a Site Security Plan (SSP). All data collected through CSAT will be stored electronically on the CSAT back-end database.

Input:

1 The data is keyed in through an online questionnaire. Information is collected through the User Approval Process and may be input by one of two roles personnel at a facility may receive. The first is a "Submitter" who is an authorized individual who may send information to DHS on behalf of the company. The second is a "Preparer" who is authorized to complete the top screen or SVA but not send or submit the information. Some data may also be uploaded by the individual in files (Microsoft Word, Adobe Acrobat).

Once the information is input, the completed registration information is printed, signed and mailed to DHS by the requestor. The form with the original signature is maintained once it has been reviewed and approved by DHS personnel.

Disposition (Media Neutral):

TEMPORARY. Destroy/delete inactive file 6 years after user account is terminated or when no longer needed for investigative or security purposes, whichever is later.

**U.S. Department of Homeland Security
Headquarters Systems Schedules**

National Protection and Programs Directorate

Master File / Data:

2. The content consists of facilities specific data, in two forms: a Top Screen assessment (used to determine the level of risk of an individual facility) and a Security Vulnerability Assessment (used to determine specific vulnerabilities of an individual facility) The data is used to determine if a facility is required to develop and submit facility security plans to DHS for review and subsequent inspection.

The records are assigned unique identifiers and can be sorted and arranged for analysis and reporting purposes. The data collected will be stored in an Oracle database.

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 authorized personnel only.

Output:

3 Threat Assessment Reports

Results from the SVA are combined with government threat assessments. The threat assessments incorporate data provided by the intelligence and law enforcement communities. The resulting products will allow the facility to receive a final tier designation and support for the development of a facility security plan.

Disposition:

TEMPORARY. Destroy or delete 10 years from the date the facility is no longer active.

Disposition (Media Neutral):

TEMPORARY. Destroy or delete 10 years from the date the facility is no longer active.

U.S. Department of Homeland Security
Headquarters Systems Schedules

National Protection and Programs Directorate

Output:

~~All Other Reports~~

- ~~Status and User reports will be run for monitoring purposes~~
- ~~Workflow prioritization reports~~
- ~~Summary reports that do not involve sensitive information may be provided to the public~~
- ~~Ad hoc Reports responding to specific questions or queries~~

~~Disposition (Media Neutral):~~ GRS 20, item 05, 6 & 7

- ~~Delete when the agency determines that they are no longer needed for Administrative, legal, audit, or other operational purposes.~~

**U.S. Department of Homeland Security
Headquarter Offices, National Protection and Programs Directorate
Chemical Security Compliance Division, Chemical Security Assessment Tool**

Chemical Security Assessment Tool

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. The Chemical Security Assessment Tool (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 (IP) 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.

CSAT's functionality revolves around the need to (1) collect data necessary to determine if a facility is regulated under the interim final rule, (2) determine the extent to which a facility may be regulated through its risk tier designation, (3) provide the facility with a means to conduct an in-depth Security Vulnerability Assessment (SVA) and (4) provide the facility with a means to prepare a Site Security Plan (SSP). All data collected through CSAT will be stored electronically on the CSAT back-end database.

Unless otherwise noted, these disposition instructions are media neutral; they apply regardless of the media or format of the records.

1. Inputs

The data is keyed in through an online questionnaire. Information is collected through the User Approval Process and may be input by one of two roles personnel at a facility may receive. The first is a "Submitter" who is an authorized individual who may send information to DHS on behalf of the company. The second is a "Preparer" who is authorized to complete the top screen or SVA but not send or submit the information. Some data may also be uploaded by the individual in files (Microsoft Word, Adobe Acrobat).

Information is input directly to the Master File. See Item 2, Master File / Data for retention.

- a. User Access Information:** Once the information is input, the completed registration information is printed, signed and mailed to DHS by the requestor. The form with the original signature is maintained once it has been reviewed and approved by DHS personnel.

Disposition: TEMPORARY. Cutoff annually. Destroy or delete 10 years after cutoff.

2. Master File / Data

The content consists of facilities specific data, in two forms: a Top Screen assessment (used to determine the level of risk of an individual facility) and a Security Vulnerability Assessment (used to determine specific vulnerabilities of an individual facility). The data

is used to determine if a facility is required to develop and submit facility security plans to DHS for review and subsequent inspection.

The records are assigned unique identifiers and can be sorted and arranged for analysis and reporting purposes. The data collected will be stored in an Oracle database.

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 authorized personnel only.

Disposition: TEMPORARY. Destroy or delete 10 years from the date the facility is no longer active.

3. Outputs

- a. Results from the SVA are combined with government threat assessments. The threat assessments incorporate data provided by the intelligence and law enforcement communities. The resulting products will allow the facility to receive a final tier designation and support for the development of a facility security plan.

Disposition: TEMPORARY. Destroy or delete 10 years from the date the facility is no longer active.

- b. Status and User reports will be run for monitoring purposes
- c. Workflow prioritization reports
- d. Summary reports that do not involve sensitive information may be provided to the public
- e. Ad hoc Reports responding to specific questions or queries

Disposition: TEMPORARY. Destroy or delete when no longer needed for business purposes.