

(e.g., permitting electronic submissions of responses).

The Department is particularly interested in comments which:

1. Respond to the Department's interpretation of the population affected by RBPS-12 background checks, as outlined in 6 CFR 27.230(a)(12);

2. Respond to fact that the Department or a Federal law enforcement agency may, if appropriate, contact the high-risk chemical facility as a part of a law enforcement investigation into terrorist ties of facility personnel;

3. Respond to the Department's intention to collect information that identifies the high-risk chemical facilities, restricted areas and critical assets to which each affected individual has access; and

4. Respond to the Department on its intention to seek an exception to the notice requirement under 5 CFR 1320.8(b)(3).

#### Analysis

*Agency:* Department of Homeland Security, National Protection and Programs Directorate, Office of Infrastructure Protection, Infrastructure Security Compliance Division.

*Title:* CFATS Personnel Surety Program.

*Form:* Not Applicable.

*OMB Number:* 1670-NEW.

*Frequency:* As required by the DHS-approved schedule.

*Affected Public:* High-risk chemical facilities as defined in 6 CFR part 27, high-risk chemical facility personnel, and as appropriate, unescorted visitors with access to restricted areas or critical assets.

*Number of Respondents:* 354,400 individuals.

*Estimated Time per Respondent:* 0.59 hours (35.4 minutes).

*Total Burden Hours:* 210,351.7 annual burden hours.

*Total Burden Cost (capital/startup):* \$0.00.

*Total Burden Cost (operating/maintaining):* \$17,669,543.

Dated: March 6, 2010.

**Thomas Chase Garwood, III,**

Chief Information Officer, National Protection and Programs Directorate, Department of Homeland Security.

[FR Doc. 2010-8312 Filed 4-12-10; 8:45 am]

BILLING CODE 9110-9P-P

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

[Docket No. DHS-2009-0146]

#### Privacy Act of 1974; Department of Homeland Security Citizenship and Immigration Services Ombudsman-001 Virtual Ombudsman System of Records

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice of Privacy Act system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of Homeland Security is giving notice that it proposes to establish a new Department of Homeland Security system of records notice titled, "Department of Homeland Security Citizenship and Immigration Services Ombudsman-001 Virtual Ombudsman System of Records." This system of records will ensure the efficient and secure processing of information to aid the Citizenship and Immigration Services Ombudsman in providing assistance to individuals, employers, and their representatives in resolving problems with U.S. Citizenship and Immigration Services; identify areas in which individuals, employers, and their representatives have problems working with U.S. Citizenship and Immigration Services; and to the extent possible, propose changes to mitigate problems pursuant to 6 U.S.C. 272. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

**DATES:** Submit comments on or before May 13, 2010. This new system will be effective May 13, 2010.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2009-0146 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.

- *Fax:* 703-483-2999.

- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

- *Docket:* For access to the docket to read background documents or comments received go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general questions please contact: Raymond Mills (202-357-8100), Privacy Point of Contact, Office of the Citizenship and Immigration Services Ombudsman, Department of Homeland Security, Washington, DC 20528. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

#### SUPPLEMENTARY INFORMATION:

##### I. Background

Pursuant to the Privacy Act of 1974, (5 U.S.C. 552a), the Department of Homeland Security (DHS) Citizenship and Immigration Services Ombudsman (CISOMB) is giving notice that it proposes to establish a new DHS system of records notice titled, "DHS/CISOMB-001 Virtual Ombudsman System of Records." This system of records will ensure the efficient and secure processing of information to aid the CISOMB in providing assistance to individuals, employers, and their representatives in resolving problems with U.S. Citizenship and Immigration Services (USCIS); identify areas in which individuals, employers, and their representatives have problems working with USCIS; and to the extent possible, propose changes to mitigate problems pursuant 6 U.S.C. 272.

CISOMB has developed the DHS/CISOMB-001 Virtual Ombudsman System of Records to ensure the efficient and secure processing of information and to aid the Ombudsman in assisting individuals and employers in making systemic recommendations to USCIS. The core of the DHS/CISOMB-001 Virtual Ombudsman System of Records is CISOMB's Web form 7001 which is a user interface Web-based form which will automatically convert information submitted by an individual or employer into a case within CISOMB's account within Internet Quorum/Enterprise Correspondence Tracking (IQ/ECT) system. IQ/ECT is the Department's enterprise-wide correspondence and case management tracking system. This system allows the Department's headquarters and components to manage cases and resolve issues in a coordinated and timely manner. For more information on IQ/ECT, please view the Enterprise Correspondence Tracking System PIA at <http://www.dhs.gov/privacy>. The system also enables CISOMB to segregate data into several categories to generate internal reports, provide customized feedback to individuals and employers, and supply real-time aggregated

statistical information for the CISOMB to assist individuals and employers with their problems with USCIS.

The purpose of this system is to provide efficient and secure case management and processing of information related to individuals and employers problems allowing the Ombudsman to make systemic recommendations to USCIS. The Department's authority for this collection is primarily Section 452 of the Homeland Security Act of 2002. This system will collect individuals' personal information to support the Ombudsman's efforts to make recommendations to USCIS pursuant to 6 U.S.C. 272. Efforts have been made to safeguard records in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The routine uses posted cover sharing with the Department of Justice for legal representation; to Congress at the request of a constituent; to the National Archives and Records Administration for records retention and disposal; to agencies, organizations, and individuals for purposes of audit as well as for security breaches; to contractors of the Department in performance of their contractual duties; to appropriate agencies and entities for investigations and prosecutions; and to an attorney or representative who is acting on behalf of an individual. This system collects information under the Paperwork Reduction Act using the following form: DHS Form 7001, Case Problem Submission Worksheet and Supporting Statement Case Problem Submission, OMB Control Number 1601-0004, Expiration Date 01/01/2013.

This newly established system will be included in DHS's inventory of record systems.

## II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by

the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the DHS/CISOMB-001 Virtual Ombudsman System of Records.

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

### System of Records:

DHS/CISOMB-001

### SYSTEM NAME:

Citizenship and Immigration Services Ombudsman—001 Virtual Ombudsman System of Records.

### SECURITY CLASSIFICATION:

Unclassified.

### SYSTEM LOCATION:

Records are maintained at Citizenship and Immigration Services Ombudsman Headquarters in Washington, DC.

### CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include: any member of the general public, including individuals, employers, and their representatives seeking assistance from the Citizenship and Immigration Services Ombudsman in resolving general matters, issues, or problems with USCIS.

### CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Individual's full legal name including any aliases;

- Individual's date and country of birth;
- Individual's legal citizenship;
- Individual's alien ("A") number;
- Full legal name of person preparing form if other than the individual named in the case;
- Applications and petitions filed;
- Receipt number located on the top left hand corner of Notice of Action (Form I-797) received from USCIS in response to the application/petition filed;
- Immigration status or interim benefit applied or petitioned for;
- Type of case problem;
- Source of case problem;
- Description of case problem;
- Prior actions taken to remedy the problem;
- Designated attorney/representative;
- Consent of the petitioner for USCIS to disclose information in the file to the designated representative;
- Verification statement signed and dated by the individual of the inquiry or the authorized representative; and
- Declaration by the individual or the attorney or representative submitting the case problem.

### AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 452 of the Homeland Security Act of 2002.

### PURPOSE(S):

The purpose of this system is to provide efficient and secure case management and processing of information related to individuals and employers problems with USCIS.

### ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3), and in accordance with 6 U.S.C. 272, as follows:

A. To the Department of Justice (including United States Attorney Offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;
2. any employee of DHS in his/her official capacity;
3. any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or

4. the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individual that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish a CISOMB function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face

or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To an attorney or representative who is acting on behalf of an individual covered by this system of records to obtain the individual's information submitted to the Virtual Ombudsman System.

**DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

None.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD-ROM.

**RETRIEVABILITY:**

Records may be retrieved by CISOMB Case Number, Alien Registration Number, or by the individuals' name.

**SAFEGUARDS:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**RETENTION AND DISPOSAL:**

In accordance with National Archives and Records Administration approved retention and disposal policy N1-563-08, processed case files are cut off at the final disposition of the case and are deleted or destroyed ten years after cutoff. Uncompleted case files are the record copy of cases where additional information is requested, but not received. Cases are closed 30 days after the request for additional information. These records are cut off 30 days from date of request if no response, and are deleted or destroyed 5 years after cutoff.

**SYSTEM MANAGER AND ADDRESS:**

CISOMB VOS Project Manager (202-357-8100), Office of the Citizenship and Immigration Services Ombudsman,

Department of Homeland Security, Washington, DC 20528.

**NOTIFICATION PROCEDURE:**

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the CISOMB's FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "contacts." When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief FOIA Officer at <http://www.dhs.gov> or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

**RECORD ACCESS PROCEDURES:**

See "Notification procedure" above.

**CONTESTING RECORD PROCEDURES:**

See "Notification procedure" above.

**RECORD SOURCE CATEGORIES:**

Information originates from stakeholders and customers who contact the CISOMB.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

Dated: March 19, 2010.

**Mary Ellen Callahan,**  
Chief Privacy Officer, Department of  
Homeland Security.

[FR Doc. 2010-8313 Filed 4-12-10; 8:45 am]

BILLING CODE 9110-9B-P

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

[Docket No. DHS-2010-0017]

### Privacy Act of 1974, Department of Homeland Security Transportation Security Administration—013 Federal Flight Deck Officer Record System

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice to alter an existing  
Privacy Act system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974 the Department of Homeland Security proposes to update and reissue an existing Department of Homeland Security system of records notice titled, Transportation Security Administration—013 Federal Flight Deck Officer Record System, previously published on August 18, 2003. The Federal Flight Deck Officer Record System contains records necessary for assessment, acceptance, training, participation, and recertification of deputized pilots of commercial air carriers who participate in the Flight Deck Officer Program designed to defend aircraft flight decks against acts of criminal violence or air piracy.

As a result of the biennial review of this system, modifications are being made to the system of records' routine uses, record sources, retention and disposal, notification procedures, and system manager and address.

Portions of this system are exempt under 5 U.S.C. 552a(k)(1), (k)(2) and (k)(6) as reflected in the final rule published in the **Federal Register** on June 25, 2004.

This updated system will continue to be included in the Department of Homeland Security's inventory of record systems.

**DATES:** Submit comments on or before May 13, 2010. The system will be effective May 13, 2010.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2010-0017 by one of the following methods:

- *Federal e-Rulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.
- *Fax:* 703-483-2999.

- *Mail:* Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

- *Instructions:* All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

*Docket:* For access to the docket to read background documents or comments received go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general questions please contact: Peter Pietra, Privacy Officer, Transportation Security Administration, TSA-36, 601 South 12th Street, Arlington, VA 20598-6036 or [TSAPrivacy@dhs.gov](mailto:TSAPrivacy@dhs.gov). For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

#### SUPPLEMENTARY INFORMATION:

##### I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) Transportation Security Administration (TSA) proposes to update and reissue a DHS/TSA system of records notice titled, DHS/TSA-013 Federal Flight Deck Officer Record System (FDORS), previously published on August 18, 2003 (68 FR 49496).

TSA's mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. To achieve this mission, TSA is required to develop and adapt its security programs to respond to evolving threats to transportation security. In accordance with the biennial review of this system, the following modifications are being made:

- DHS/TSA is updating the system of records to incorporate five Department of Homeland Security (DHS) standard routines uses. One routine use will allow the release of information to appropriate agencies, entities, and persons when DHS/TSA suspects or has confirmed that the security or confidentiality of an information system of records has been compromised. Another routine use permits the release of information to the media when there exists a legitimate public interest in disclosing information. Release under this routine use will require the approval of the DHS Chief Privacy officer in consultation with counsel. The third routine use allows the release of information to a court, magistrate,

administrative tribunal or opposing counsel or parties where a federal agency is a party or has an interest in the litigation or administrative proceeding. The fourth routine use allows DHS/TSA to release information to a former employee when it is necessary to consult with the former employee regarding a matter that is within that person's former area of responsibility. The fifth routine use allows DHS/TSA to release information to appropriate entities where it would assist in the enforcement of civil or criminal laws.

- DHS/TSA is revising a routine use currently in by adding indirect air carriers and other facility operators as potential recipients of information from these systems when appropriate to address a threat or potential threat to transportation security or national security, or when required for administrative purposes related to the effective and efficient administration of transportation security laws.

- DHS/TSA is also revising a current routine use by adding indirect air carriers and other facility operators as potential recipients of information about individuals who are their employees, job applicants, or contractors, or persons to whom they issue identification credentials or grant clearances to secured areas in transportation facilities when relevant to such employment, application, contract, training or the issuance of such credentials or clearances.

- Finally, DHS/TSA has removed as a routine use the sharing of information with the Attorney General of the United States concerning violations of the Brady Handgun Violence Prevention Act as it is duplicative.

- The record source categories are being updated to reflect the use of commercial and public record databases and Web sites to obtain information regarding the identity of individuals who attempt to gain access to the sterile areas of the airport and for whom identity needs to be verified or individuals who are being vetted to qualify as federal flight deck officers.

- The retention and disposal section is updated to reflect the records retention schedules approved by the National Archives and Records Administration (NARA).

- The notification section was changed to reflect that inquiries regarding whether the applicable system contains records about an individual should be directed to TSA's Freedom of Information Act (FOIA) Office.

- The system manager and address were revised to reflect the current system manager.