

TABLE 2—ESTIMATES OF AVERAGE ANNUALIZED HOUR BURDEN TO RESPONDENTS FOR THE SECOND AND THIRD YEARS—Continued

[One reporting period per year]

Component	Source of funding	Number of respondents	Responses per grantee	Total responses	Hours to complete/coordinate receipt of data reports	Total burden hours
	Subtotal		646			983
Component		Number of respondents	Responses per provider	Total responses	Hours to develop/adjust CLD system	Total burden hours
Service Provider Response Burden						
CLD Collection System		583	1	583	92.80	54,102
Component		Number of respondents	Responses per provider	Total responses	Hours per response	Total burden hours
Provider Report		2,253*	1	2,253	2.35	5,295
Component	Providers' electronic data systems capability	Number of respondents	Responses per provider	Total responses	Hours to collect/report data per response	Total burden hours
Client Report (client-level data).	No	63	1	63	106.25	6,694
	Yes	2,049	1	2,049	3.75	7,684
	Subtotal		** 2,112			14,378
TOTAL BURDEN, YEAR 2						74,758
TOTAL BURDEN, YEAR 3						20,656

[†] All providers, including direct service providers and administrative support service-only providers.

^{††} All direct service providers, including those outpatient/ambulatory medical care, medical case management, and/or nonmedical case management providers that will submit a Client Report in 2009 as well as other direct service providers that will submit a Client Report in 2010.

^a There is no CLD Collection system adjustment in Year 3, so the total burden is less.

Written comments and recommendations concerning the proposed information collection should be sent within 30 days of this notice to the desk officer for HRSA, either by e-mail to OIRA_submission@omb.eop.gov or by fax to 202-395-6974. Please direct all correspondence to the "attention of the desk officer for HRSA."

Dated: November 7, 2008.

Alexandra Huttinger,

Director, Division of Policy Review and Coordination.

[FR Doc. E8-27115 Filed 11-13-08; 8:45 am]

BILLING CODE 4165-15-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2008-0084]

Privacy Act of 1974; Department of Homeland Security Internal Affairs System of Records

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, and as part of the Department of Homeland Security's ongoing effort to review and update legacy system of records notices, the Department of Homeland Security proposes to consolidate two legacy record systems titled, Treasury/CS.127 Internal Affairs Records System, and Justice/INS.002 INS Office of Internal Audit Investigations Index and Records into one Department of Homeland Security-wide system of records notice titled Internal Affairs. This system will allow the Department of Homeland Security to collect and maintain records on applicants, past and present employees, contractors, and contractor applicants relating to investigations conducted by Department of Homeland Security Headquarters or its components with the exception of investigations conducted by the Office of the Inspector General, which are covered by DHS/OIG-002 Investigations Data Management System. Categories of individuals, categories of records, and the routine uses of this legacy system of records notices have been consolidated and updated to better reflect the Department's internal affairs

record systems. Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) concurrent with this SORN elsewhere in the **Federal Register**. The exemptions for the legacy system of records notices will continue to be applicable until the final rule for this SORN has been completed. This consolidated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before December 15, 2008. This new system will be effective December 15, 2008.

ADDRESSES: You may submit comments, identified by docket number DHS-2008-0084 by one of the following methods:

- **Federal e-Rulemaking Portal:** <http://www.regulations.gov>. Follow the instructions for submitting comments.
- **Fax:** 1-866-466-5370.
- **Mail:** Hugo Teufel III, 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 and may be read at

<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 and privacy issues please contact: Hugo Teufel III (703–235–0780), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107–296, Section 1512, 116 Stat. 2310 (November 25, 2002), the Department of Homeland Security (DHS) and its components and offices have relied on preexisting Privacy Act systems of records notices for the collection and maintenance of records that concern internal affairs records.

As part of its efforts to streamline and consolidate its Privacy Act record systems, DHS is establishing a new agency-wide system of records under the Privacy Act (5 U.S.C. 552a) for DHS internal affairs records. This will ensure that all components of DHS follow the same privacy rules for collecting and handling internal affairs records. DHS will use this system to collect and maintain internal affairs records submitted by DHS personnel and others.

In accordance with the Privacy Act of 1974, and as part of DHS's ongoing effort to review and update legacy system of records notices, DHS proposes to consolidate two legacy record systems titled, Treasury/CS.127 Internal Affairs Records System (66 FR 52984 October 18, 2001) and Justice/INS.002 INS Office of Internal Audit Investigations Index and Records (67 FR 64136 January 3, 2002), into one DHS-wide system of records notice titled Internal Affairs. This system will allow DHS to collect and maintain records on applicants, past and present employees, contractors, and contractor applicants relating to investigations conducted by DHS Headquarters or its components with the exception of investigations conducted by the Office of the Inspector General (OIG), which are covered by DHS/OIG–002 Investigations Data Management System. Categories of individuals, categories of records, and the routine uses of these legacy system of records notices have been consolidated and updated to better reflect the Department's internal affairs record systems. Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) concurrent with

this SORN elsewhere in the **Federal Register**. The exemptions for the legacy system of records notices will continue to be applicable until the final rule for this SORN has been completed. This consolidated 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 from 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 legal 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 of their records, and to assist individuals to more easily find such files within the agency. Below is the description of the Internal Affairs System of Records.

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

SYSTEM OF RECORDS:

DHS/ALL–020.

SYSTEM NAME:

Department of Homeland Security Internal Affairs Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained at several Headquarters locations and in

component offices of DHS, in both Washington, DC, and field locations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Any applicants for Federal employment, past and present employees, contractors, and contractor applicants, or any other individual who is subject to, or involved in, an integrity or disciplinary inquiry or investigation not handled by OIG.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Individual identifying data, which may include some or all of the following: full name, date of birth, social security number, addresses, duty station, grade, job series, and entrance on duty date;
- Allegations received and method received;
- Relevant information from background investigations;
- Integrity investigations;
- Investigation files;
- Incident location;
- Case agent/officer or supervisor;
- Case/prosecution status;
- Photographic images, videotapes, voiceprints, DVDs;
- Letters, e-mails, memoranda and reports;
- Exhibits, evidence, statements and affidavits; and
- Any other information gathered in the course of an integrity or disciplinary inquiry or investigation.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; the Federal Records Act, 44 U.S.C. 3101; Executive Order 9397.

PURPOSE(S):

The purpose of this system is to collect and maintain records on applicants, past and present employees, contractors, and contractor applicants relating to integrity or disciplinary inquiries or investigations conducted by DHS Headquarters or its components, except for those investigations conducted by OIG.

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 of information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) 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 the Department of Justice 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 who relies 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 an

agency 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 disclose information to a Federal, State, or local agency, maintaining civil, criminal or other relevant enforcement information or other pertinent information, which has requested information relevant to or necessary to the requesting agency's or the bureau's hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit.

I. To disclose information to a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, in response to a subpoena from a court of competent jurisdiction.

J. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

K. To an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee.

L. To provide information to unions recognized as exclusive bargaining representatives under the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114, and in circumstances when union officials represent employees in investigations and personnel actions.

M. To a court, prosecutor, and/or defense attorney in satisfaction of the agency's obligations under the Giglio, Jenks, or Brady decisions;

N. To management officials at Federal, State or local agencies who may

be in a position to take disciplinary or other corrective action and to boards and panels who may be charged with making recommendations or proposals regarding remedial action.

O. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

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 the individual's name, date of birth, or social security number.

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:

The file records are maintained as long as the subject of the investigation is employed by DHS, and then one year after the subject terminates employment. The files are then transferred to the Federal Records Center for a period of 25 years, after which they are destroyed.

SYSTEM MANAGER AND ADDRESS:

For Headquarters and components of DHS, the System Manager is the Director of Departmental Disclosure, Department of Homeland Security, Washington, DC 20528. For components of DHS, the System Manager can be found at <http://www.dhs.gov/foia> under "contacts."

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 Headquarters' or component's FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW., Building 410, STOP-0550, Washington, DC 20528.

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 Director, Disclosure and FOIA, <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,
- 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:

Sources of information include: individuals who are the subject of the investigation or inquiry, employers, law enforcement organizations, members of the public, witnesses, education institutions, government agencies, credit bureaus, references, neighborhood checks, confidential sources, medical service providers, personal interviews, photographic images, military, financial institutions, citizenship, birth and tax records, and the applicant's, employee's or contractor's personnel history and application forms.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (5), and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). In addition, the Secretary of Homeland Security has exempted this system from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1), (2), (k)(3), and (5).

Dated: November 6, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-27091 Filed 11-13-08; 8:45 am]

BILLING CODE 4410-10-P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

Privacy Act of 1974; Retirement of System of Records

AGENCY: Privacy Office, DHS.

ACTION: Notice of the retirement of one Privacy Act system of records notice.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security is giving notice that it proposes to retire the following Privacy Act system of records notice, Treasury/CS.064 (October 18, 2001), from its inventory of record systems and rely upon the Government-wide system of records notice issued by the General Services Administration, GSA/GOVT-6 GSA SmartPay Purchase Charge Card Program (November 3, 2006), which is

written to cover all Federal government purchase charge card record systems.

DATES: These changes will take effect on December 15, 2008.

FOR FURTHER INFORMATION CONTACT:

Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, by telephone (703) 235-0780 or facsimile (703) 235-0442.

SUPPLEMENTARY INFORMATION: Pursuant to the provisions of the Privacy Act of 1974, 5 U.S.C. 552a, and as part of its ongoing integration and management efforts, the Department of Homeland Security (DHS) is retiring the system of records notice, Treasury/CS.064 Purchase Card Files (66 FR 52984 October 18, 2001), that was issued by the Customs Service, Department of the Treasury prior to the creation of the Department of Homeland Security.

DHS will continue to collect and maintain records regarding individuals who are in possession of Department purchase cards and will rely upon the existing Federal Government-wide system of records notice titled GSA/GOVT-6 GSA SmartPay Purchase Charge Card Program (71 FR 64707 November 3, 2006), which is written to cover all Federal purchase charge card record systems.

Eliminating this notice will have no adverse impacts on individuals, but will promote the overall streamlining and management of DHS Privacy Act record systems.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-27096 Filed 11-13-08; 8:45 am]

BILLING CODE 4410-10-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2008-0112]

Review and Revision of the National Infrastructure Protection Plan

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Notice and request for comments.

SUMMARY: This notice informs the public that the Department of Homeland Security (DHS) is currently revising the 2006 National Infrastructure Protection Plan (NIPP) and, as part of a comprehensive national review process, solicits public comment on issues or language in this draft document that need to be updated during this triennial review cycle.