

**DEPARTMENT OF HOMELAND SECURITY****Office of the Secretary****Privacy Act of 1974; System of Records**

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice of removal 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 will remove one system of records notice from its inventory of record systems because the United States Secret Service no longer requires the system. The obsolete system is Treasury/IRS 46.016 Secret Service Details, Criminal Investigation Division (66 FR 63783 December 10, 2001).

**DATES:** *Effective Date:* January 20, 2009.

**FOR FURTHER INFORMATION CONTACT:** Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, by telephone (703) 235-0780 or facsimile 1-866-466-5370.

**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 removing one United States Secret Service (USSS) system of records notice from its inventory of record systems.

DHS inherited this record system upon its creation in January of 2003. Upon review of its inventory of records systems, DHS has determined it no longer needs or uses this system of records and is retiring Treasury/IRS 46.016 Secret Service Details, Criminal Investigation Division (66 FR 63783 December 10, 2001).

Treasury/IRS 46.016 Secret Service Details, Criminal Investigation Division was originally established to collect and maintain the USSS's Criminal Investigation Division records, which are now covered but a different system of records.

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

Dated: December 10, 2008.

**Hugo Teufel III,**

*Chief Privacy Officer, Department of Homeland Security.*

[FR Doc. E8-29790 Filed 12-18-08; 8:45 am]

**BILLING CODE 4410-10-P**

**DEPARTMENT OF HOMELAND SECURITY****Office of the Secretary****Privacy Act of 1974; System of Records Notice**

**AGENCY:** Privacy Office, DHS.

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

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of Homeland Security is giving notice that it will remove one system of records from its inventory of record systems because the United States Secret Service is consolidating system of records notices. The obsolete system of records notice is USSS.004 Financial Management Information System (August 28, 2001).

**DATES:** *Effective Date:* January 20, 2009.

**FOR FURTHER INFORMATION CONTACT:** Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, by telephone (703) 235-0780 or facsimile 1-866-466-5370.

**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 removing one United States Secret Service (USSS) system of records from its inventory of record systems.

DHS inherited this record system upon its creation in January of 2003. Upon review of its inventory of records systems, DHS has determined that records within this legacy system are covered by Department system of records DHS/ALL-007 Accounts Payable Records (73 FR 61880 October 17, 2008) covering general accounts payable records, budget preparation and presentation materials, apportionment records, payroll records, pay administration records, expenditure accounting records, tax ID records, and records containing information on current and projected accounts payable; DHS/ALL-008 Accounts Receivable Records (73 FR 61885 October 17, 2008) covering general accounts receivable records, records on individuals involved in payments with DHS, and records containing information on current and projected accounts receivable; DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records (73 FR 63172 October 23, 2008) covering employee and individual records, employer records, records containing information compiled for the purpose of pay, travel, expenses incurred other than travel, and

retirement annuities and taxes, and time and attendance records; DHS/ALL-013 Claims Records (73 FR 63987 October 28, 2008) covering records containing information compiled for the purpose of property damage, records containing information on tort claims dealing with USSS property; DHS/ALL-021 Contractors and Consultants Records (73 FR 63179 October 23, 2008) covering contractor and vendor records; DHS/ALL-011 Biographies and Awards Records (73 FR 66654 November 10, 2008) covering individuals who are recipients of awards and are retiring USSS.004 Financial Management Information System (66 FR 45362 August 28, 2001).

USSS.004 Financial Management Information System (66 FR 45362 August 28, 2001) was originally established to record, track, and maintain USSS financial accounting information, which are now covered by different systems of records. Eliminating this system of records notice will have no adverse impacts on individuals, but will promote the overall streamlining and management of DHS Privacy Act system of record notices.

Dated: December 10, 2008.

**Hugo Teufel III,**

*Chief Privacy Officer, Department of Homeland Security.*

[FR Doc. E8-29791 Filed 12-18-08; 8:45 am]

**BILLING CODE 4410-10-P**

**DEPARTMENT OF HOMELAND SECURITY****Office of the Secretary**

[Docket No. DHS-2008-0154]

**Privacy Act of 1974; U.S. Customs and Border Protection—009 Nonimmigrant Information System**

**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 record notices, the Department of Homeland Security proposes to update and reissue the following legacy record system, Justice/INS-036 Nonimmigrant Information System, January 31, 2003, as a Department of Homeland Security system of records notice titled, U.S. Customs and Border Protection Nonimmigrant Information System. Categories of individuals, categories of records, and the routine uses of this legacy system of records notice have

been reviewed updated to better reflect the Department of Homeland Security U.S. Customs and Border Protection Nonimmigrant Information System. Concurrent with this System of Records Notice, DHS is issuing a notice of proposed rulemaking to exempt this system for certain aspects of the Privacy Act. This reissued system will be included in the Department of Homeland Security's inventory of record systems.

**DATES:** Written comments must be submitted on or before January 20, 2009.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2008-0154 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 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: Laurence E. Castelli (202-325-0280), Chief, Privacy Act Policy and Procedures Branch, U.S. Customs and Border Protection, Office of International Trade, Regulations & Rulings, Mint Annex, 799 Ninth Street, NW., Washington, DC 20001-4501. For privacy issues contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

#### **SUPPLEMENTARY INFORMATION:**

##### **I. Background**

Pursuant to 6 U.S.C. 552(a)(1), the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) have maintained the Nonimmigrant Information System (NIIS) in conformance with the terms of the previous NIIS SORN, 68 FR 5048.

As part of its efforts to streamline and consolidate its record systems, DHS is updating and reissuing a DHS/CBP system of records under the Privacy Act (5 U.S.C. 552a) to reflect CBP's current and future practices regarding the processing of foreign nationals entering

the U.S. CBP inspects all persons applying for admission to the U.S. As part of this inspection process, CBP establishes the identity, nationality, and admissibility of persons crossing the border and may create a border crossing record, which would be covered by DHS/CBP-007 Border Crossing Information System of Records Notice (73 FR 43457 published on July 25, 2008), or additional CBP records, which would be covered by the TECS System of Records Notice (re-published concurrently with this notice) during this process. Similarly, CBP has authority to keep records of departures from the U.S.

In addition to information collected from the alien during the inspection process, CBP primarily uses two immigration forms to collect information from nonimmigrant aliens as they arrive in the U.S.: The I-94, Arrival/Departure Record and, for aliens applying for admission under the visa waiver program, the I-94W Nonimmigrant Visa Waiver Arrival/Departure Form. Separately, Canadian nationals, who travel to the U.S. as tourists or for business, and Mexican nationals, who possess a nonresident alien Mexican Border Crossing Card, are not required to complete an I-94 upon arrival, but their information will also be maintained in NIIS. Additionally, DHS/CBP has been implementing an Electronic System for Travel Authorization (ESTA) to permit nationals of VWP countries to submit their biographic and admissibility information online in advance of their travel to the U.S. Applicants under this program will have access to their accounts so that they may check the status of their ESTA and make limited amendments. ESTA is covered by privacy documentation including a SORN published on June 10, 2008, 73 FR 32720.

In accordance with the Privacy Act of 1974 and as part of DHS's ongoing effort to review and update legacy system of record notices, DHS/CBP proposes to update and reissue the following legacy record system, Justice/INS-036 Nonimmigrant Information System (68 FR 5048 January 31, 2003), as a DHS/CBP system of records notice titled, U.S. Customs and Border Protection Nonimmigrant Information System. Categories of individuals and categories of records have been reviewed, and the routine uses of this legacy system of records notice have been updated to better reflect the DHS/CBP Nonimmigrant Information System. Additionally, the exemptions for this legacy system of records notice transfer from the system's legacy agency to DHS.

This reissued system will be included in the 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 U.S. 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 the 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 U.S. 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 to make agency recordkeeping practices transparent, to notify individuals regarding the uses of their records, and to assist the individual to more easily find such files within the agency. Below is a description of the NIIS System of Records.

In accordance with 5 U.S.C. 552a(r), a report concerning this record system has been sent to the Office of Management and Budget and to the Congress.

##### **SYSTEM OF RECORDS:**

DHS/CBP-009.

##### **SYSTEM NAME:**

U.S. Customs and Border Protection—009 Nonimmigrant Information System.

##### **SECURITY CLASSIFICATION:**

Unclassified.

##### **SYSTEM LOCATION:**

This computer database is located at the U.S. Customs and Border Protection (CBP) National Data Center. Computer terminals are located at customhouses, border ports of entry, airport inspection facilities under the jurisdiction of the Department of Homeland Security and other locations at which DHS authorized personnel may be posted to

facilitate DHS's mission. Terminals may also be located at appropriate facilities for other participating government agencies that have obtained system access pursuant to a Memorandum of Understanding.

**CATEGORIES OF INDIVIDUALS COVERED BY THIS SYSTEM:**

Categories of individuals covered by this system are nonimmigrant aliens entering and departing the U.S.

**CATEGORIES OF RECORDS IN THIS SYSTEM:**

NIIS is a dataset residing on the CBP Information Technology (IT) platform and in paper form. It contains arrival and departure information collected from foreign nationals entering and departing the U.S. on such forms as the I-94, I-94W, or through interviews with CBP officers. This information consists of the following data elements, where applicable:

- Full Name (first, middle, and last);
- Date of birth;
- E-mail address, as required;
- Travel document type (e.g., passport information, permanent resident card, etc.), number, issuance date, expiration date and issuing country;
- Country of citizenship;
- Date of crossing both into and out of the U.S.;
- Scanned images linked through the platform;
- Airline and flight number;
- City of embarkation;
- Address while visiting the U.S.;
- Admission number received during entry into the U.S.;
- Whether the individual has a communicable disease, physical or mental disorder, or is a drug abuser or addict;
- Whether the individual has been arrested or convicted for a moral turpitude crime, drugs, or has been sentenced for a period longer than five years;
- Whether the individual has engaged in espionage, sabotage, terrorism, or Nazi activity between 1933 and 1945;
- Whether the individual is seeking work in the U.S.;
- Whether the individual has been excluded or deported, or attempted to obtain a visa or enter the U.S. by fraud or misrepresentation;
- Whether the individual has ever detained, retained, or withheld custody of a child from a U.S. citizen granted custody of the child;
- Whether the individual has ever been denied a U.S. visa or entry into the U.S., or had a visa cancelled (if yes, when and where);
- Whether the individual has ever asserted immunity from prosecution; and

- Any change of address while in the U.S.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

5 U.S.C. 301; the Federal Records Act, 44 U.S.C. 3101; The legal authority for NIIS comes from 8 U.S.C. 1103, 8 U.S.C. 1184, Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, The Immigration and Nationality Act, 8 U.S.C. 1354, and the Homeland Security Act of 2002, Public Law 107-296.

**PURPOSE(S):**

NIIS is a repository of records for persons arriving in or departing from the U.S. as nonimmigrant visitors and is used for entry screening, admissibility, and benefits purposes. The system provides a central repository of contact information for such aliens while in the U.S. and also captures arrival and departure information for determination of future admissibility.

**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) as follows:

- A. To the Department of Justice 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 U.S. 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 appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

H. 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 or criminal discovery, litigation, or settlement negotiations, or in response to a subpoena from a court of competent jurisdiction.

I. 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.

J. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

K. To an appropriate Federal, State, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

L. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations, for purposes of assisting such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or for combating other significant public health threats.

M. To Federal and foreign government intelligence or counterterrorism agencies or components where CBP becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

N. 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.

O. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental

organizations where DHS is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance national security or identify other violations of law

**DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

None.

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

**STORAGE:**

The data is stored electronically at the CBP and DHS Data Center for current data and offsite at an alternative data storage facility for historical logs, system backups and in paper form.

**RETRIEVABILITY:**

These records may be searched on a variety of data elements including name, addresses, place and date of entry or departure, or country of citizenship as listed in the travel documents used at the time of entry to the U.S. An admission number, issued at each entry to the U.S. to track the particular admission, may also be used to identify a database record.

**SAFEGUARDS:**

All NIIS records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include all of the following: restricting access to those with a "need to know"; using locks, alarm devices, and passwords; compartmentalizing databases; auditing software; and encrypting data communications.

NIIS information is secured in full compliance with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules, which will be applied to component systems, communications between component systems, and at interfaces between component systems and external systems.

One aspect of the DHS comprehensive program to provide information security involves the establishment of rules of behavior for each major application, including NIIS. These rules of behavior require users to be adequately trained regarding the security of their systems. These rules also require a periodic assessment of technical, administrative and managerial controls to enhance data

integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. System users must also complete annual privacy awareness training to maintain current access.

NIIS transactions are tracked and can be monitored. This allows for oversight and audit capabilities to ensure that the data is being handled consistent with all applicable federal laws and regulations regarding privacy and data integrity.

**RETENTION AND DISPOSAL:**

NIIS data is subject to a retention requirement. The information collected and maintained in NIIS is used for entry screening, admissibility, and benefits purposes and is retained for seventy five (75) years from the date obtained.

However, NIIS records that are linked to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases will remain accessible for the life of the law enforcement activities to which they may become related. The current disposition for paper copy is 180 days from date of departure.

**SYSTEM MANAGER AND ADDRESS:**

Assistant Commissioner, Office of Information Technology, U.S. Customs and Border Protection Headquarters, 1300 Pennsylvania Avenue, NW., Washington, DC 20229.

**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 CBP's FOIA Officer, 1300 Pennsylvania Avenue, NW., Mint Annex, Washington, DC 20229.

When seeking records about yourself from this system of records or any other CBP 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,

- Specify when you believe the records would have been created,

- 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 CBP 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:

The system contains certain data received on individuals, passengers and crewmembers that arrive in, depart from, or transit through the U.S. This system also contains information collected from carriers that operate vessels, vehicles, aircraft and/or trains that enter or exit the U.S. and from the individuals upon crossing the U.S. border.

Basic information is obtained from individuals, the individual's attorney/representative, CBP officials, and other federal, state, local, and foreign agencies.

#### EXEMPTIONS CLAIMED FOR THE SYSTEM:

No exemption shall be asserted with respect to information maintained in the system that is collected from a person or submitted on behalf of a person, if that person, or his or her agent, seeks access or amendment of such information.

This system, however, may contain information related to an ongoing law enforcement investigation because the information regarding a person's travel and border crossing was disclosed to appropriate law enforcement in conformance with the above routine uses. As such pursuant to 5 U.S.C. 552 a (j)(2) and (k)(2), DHS will claim exemption from (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information.

Dated: December 10, 2008.

#### Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-29792 Filed 12-18-08; 8:45 am]

BILLING CODE 4410-10-P

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

[Docket No. DHS-2008-0108]

### Privacy Act of 1974; United States Coast Guard—014 Military Pay and Personnel 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 record notices, the Department of Homeland Security giving notice that it proposes to add a system of records to its inventory of record systems titled United States Coast Guard Military Pay and Personnel. This system is a compilation of nine legacy record systems: DOT/CG 534 Travel and Transportation of Household Effects (April 11, 2000); DOT/CG 537 FHA Mortgage Insurance for Servicemen in lieu of VHA Mortgage Insurance for Servicemen; DOT/CG 573 United States Public Health Services, Commissioned Officer Corps Staffing and Recruitment Files (April 11, 2000); DOT/CG 622 Military Training and Education Records (April 11, 2000); DOT/CG 623 Military Pay and Personnel System (April 11, 2000); DOT/CG 625 Officer Selection and Appointment System (April 11, 2000); DOT/CG 626 Official Officer Service Records (April 11, 2000); DOT/CG 629 Enlisted Personnel Record System (April 11, 2000); DOT/CG 630 Coast Guard Family Housing (April 11, 2000); and DOT/CG 640 Outside Employment of Active Duty Coast Guard Personnel (April 11, 2000). This record system will allow the Department of Homeland Security/United States Coast Guard to collect and maintain records regarding military pay and personnel. Categories of individuals, categories of records, and routine uses of these legacy system of records notices have been consolidated and updated to better reflect the United States Coast Guard's military service personnel record systems. This new system will be included in the Department of Homeland Security's inventory of record systems.

**DATES:** Written comments must be submitted on or before January 20, 2009. This new system will be effective January 20, 2009.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2008-0108 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 please contact: David Roberts (202-475-3521), Privacy Officer, United States Coast Guard. For privacy issues please contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. 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)/United States Coast Guard (USCG) have relied on preexisting Privacy Act systems of records notices for the collection and maintenance of records that concern active duty, reserve, and retired active duty and retired reserve, as well as eligible dependent's military pay and personnel processing.

As part of its efforts to streamline and consolidate its record systems, DHS is updating and reissuing a USCG system of records under the Privacy Act (5 U.S.C. 552a) that deals with active duty, reserve, retired active duty, and retired reserve, as well as eligible dependent's military pay and personnel processing. This record system will allow DHS/USCG to collect and maintain records regarding military pay. The collection and maintenance of this information will assist DHS/USCG in meeting its obligation pay active duty, reserve, retired active duty, and retired reserve military personnel, as well as eligible dependents for their service.

In accordance with the Privacy Act of 1974, and as part of the DHS Privacy Office's ongoing effort to review and update legacy system of record notices DHS is giving notice that it proposes to add a system of records to its inventory