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 authorized officials of the Internal Revenue Service, General Accountability Office (GAO), and the Civil Service Commission, as required, to address salary claims submitted by USCG military and civilian personnel.

I. 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 or in connection with criminal law proceedings or in response to a subpoena.

J. 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 claimant's name, employee ID (EMPLID), 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 individual 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:

Records are retained until adjudication and settlement. Most submissions are retained for present setting value, as required. Records are retained for 10 years, 3 months after the year in which the Government's right to collect first accrued. (AUTH: GRS 6, Item 10b(2)(a)) (Records Officer).

SYSTEM MANAGER AND ADDRESS:

Commandant (CG–12), United States Coast Guard, 2100 2nd Street SW., Washington, DC 20593–0001.

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 USCG, Commandant (CG–611), 2100 2nd St., SW., Attn: FOIA Coordinator, Washington, DC 20593–0001.

When seeking records about yourself from this system of records or any other USCG 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 to you 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 the USCG will 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:

Individual, USCG payroll offices, legal staff, investigators, Director of Personnel and Management, Comptroller General, GAO, and congressional correspondence.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: December 10, 2008.

Hugo Teufel III

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29810 Filed 12–18–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0143]

Privacy Act of 1974; United States Coast Guard–019 Non-Federal Invoice Processing 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 is giving notice that it proposes to update and reissue the following legacy record system DOT/CG 576 Non-Federal Invoice Processing System (April 11, 2000) as a Department of Homeland Security system of records notice titled, United States Coast Guard–019 Non-Federal Invoice Processing System. Non-Federal Invoice Processing System is a program that facilitates processing of active duty member and dependent dental claims. Categories of individuals, categories of records, and the routine uses of this legacy system of records notice have been reviewed and updated to better reflect the Department of Homeland Security and the United States Coast Guard's–019 Non-Federal Invoice Processing System record system. 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.

ADDRESSES: You may submit comments, identified by docket number DHS–2008–0143 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) and its components and offices have relied on preexisting Privacy Act systems of records notices for the maintenance of records that concern invoices processed by the United States Coast Guard (USCG) Non-Federal Invoice Processing System (NIPS).

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 invoices processed by NIPS. This record system will allow DHS/USCG to collect and preserve the records regarding invoices processed by NIPS. NIPS is an electronic database that provides for simple tracking and accounting of dental claims. The collection and maintenance of this information will assist DHS/USCG in meeting its obligation to record invoices processed by NIPS.

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 is giving notice that it proposes to update and reissue the following legacy record system DOT/CG 576 Non-Federal Invoice Processing System (NIPS) (65 FR 19476, April 11, 2000) as a Department of Homeland Security/United States Coast Guard system of records notice titled, Non-Federal Invoice Processing 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 Department of Homeland Security and the United States Coast Guard's—019 Non-Federal Invoice Processing System record system. This new system will be included in the Department of Homeland Security'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 which their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the NIPS System of Records.

III. Health Insurance Portability and Accountability Act

This system of records contains individually identifiable health information. The Health Insurance Portability and Accountability Act of 1996, applies to most of such health information. Department of Defense 6025.18–R may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974 or mentioned in this system of records notice.

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 and to Congress.

System of Records DHS/USCG–019

SYSTEM NAME:

United States Coast Guard—019 Non-Federal Invoice Processing System.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained at the United States Coast Guard Maintenance and Logistics Command Atlantic in Norfolk, VA.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this system include active duty, reserve, and retired members of the uniformed services and their eligible dependents, as well as non-Federal health care providers that have rendered services to eligible beneficiaries.

CATEGORIES OF RECORDS IN THE SYSTEM:

Categories of records in this system include:

- Individual's name;
- Social security number;
- Social security number of dependent's sponsor;
- Tax identification number of dental provider
- Correspondence, memoranda, and related documents concerning potential and actual health care invoices for processing by NIPS;
- Dental treatment and related medical records provided to the individual that are the subject of an invoice for non-Federal health care provided to an eligible beneficiary; and
- Automated data processing (ADP) records containing identifying data on individuals including: Units of

assignment and address, home address, and information necessary to process and monitor bills for payment.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 10 U.S.C. 1091; 14 U.S.C. 93.

PURPOSE(S):

The purpose of the USCG Non-Federal Invoice Processing System is to maintain an electronic record of dental invoices for Coast Guard active duty member, reserve, retired, and dependent, so that USCG can pay such invoices.

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

Note: This system of records contains individually identifiable health information. The Health Insurance Portability and Accountability Act of 1996, applies to most of such health information. Department of Defense 6025.18–R may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974 or mentioned in this system of records notice. Therefore, routine uses outlined below may not apply to such health information.

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 or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when:

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 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 healthcare professionals: medical information, including records of healthcare and medical invoices to support a government claim.

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 name, Social Security number of member or dependents sponsor, or name or tax identification number of non-Federal healthcare provider.

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. The system maintains a real-time auditing function of individuals who access the system. Additional safeguards may vary by component and program.

RETENTION AND DISPOSAL:

Records are retained for one year from date of service; transferred to a Federal Record Center and retained for an additional 5 years 3 months, and destroyed thereafter. (AUTH: GRS 6, Item 1a)

SYSTEM MANAGER AND ADDRESS:

United States Coast Guard Maintenance and Logistics Command Atlantic Health and Safety Division (MLC LANT (k)), 300 East Main Street, Suite 1000, Norfolk, VA 23510–9103.

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 USCG, Commandant (CG–611), 2100 2nd St., SW., Attn: FOIA Coordinator, Washington, DC 20593–0001.

When seeking records about yourself from this system of records or any other USCG 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 the USCG will 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:

From the individual, individual's spouse, parent or guardian. Medical facilities (United States Coast Guard, Department of Defense, uniformed Services Treatment Facility, or non-Federal, provider) where beneficiaries are treated. From Active Duty and Enlisted Personnel; DHS/USCG–005 Military Services Personnel. From Reserve personnel—the Official Coast Guard Reserve Service Record System, DHS/USCG–028. Investigations resulting from illness or injury.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: December 10, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8–29811 Filed 12–18–08; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2008–0097]

Privacy Act of 1974; Federal Emergency Management Agency—007 National Flood Insurance Program Marketing Files 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 consolidate three legacy record systems into a Department of Homeland Security system of records notice titled, Federal Emergency Management Agency National Flood Insurance Program Marketing Files: FEMA/FIMA–4 National Flood Insurance Program Marketing Records and Related Files (January 23, 2002), FEMA/FIMA–5 National Flood Insurance Program Telephone Response Center (TRC) Consumer and Policyholder Records and Related Documents Files (January 23, 2002), and FEMA/MIT–7 Flood Map Customer Records (June 8, 2001). This system will allow the Department of Homeland Security to market the Department of Homeland Security Federal Emergency Management Agency—006 National Flood Insurance Program. 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 National Flood Insurance Program marketing record systems. This system will be included in the Department'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–2008–0097 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: Federal Emergency Management Agency Privacy Officer, Federal Emergency Management Agency. 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)/Federal Emergency Management Agency (FEMA) have relied on preexisting Privacy Act systems of records notices for the collection and maintenance of records pertaining to the marketing of the National Flood Insurance Program, which is administered by DHS/FEMA.

In 1968, Congress created the National Flood Insurance Program (NFIP) in response to the rising cost of taxpayer funded disaster relief for flood victims and the increasing amount of damage caused by floods.

Nearly 20,000 communities across the United States and its territories participate in the NFIP by adopting and enforcing floodplain management ordinances to reduce future flood damage. In exchange, the NFIP makes federally-backed flood insurance available to homeowners, renters, and business owners in these communities.

Typically, a home or business owner will seek flood insurance from an insurance company that provides other lines of business such as traditional car insurance or property and casualty homeowners insurance. In other cases, a mortgage lender will require flood insurance in addition to regular homeowner's insurance. If a home owner's insurance company participates in the NFIP's Write-Your-Own (WYO) program, and the home or business owner's building is located in a participating NFIP community, the home or business owner can purchase flood insurance.

The NFIP Marketing Files SORN allows DHS/FEMA to market the NFIP program to home and business owners