[Federal Register: December 11, 2008 (Volume 73, Number 239)]
[Notices]
[Page 75442-75445]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr11de08-82]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2008-0121]

Privacy Act of 1974; United States Coast Guard--029 Notice of Arrival and Departure System of Records Notice

AGENCY: Privacy Office; DHS.

ACTION: Notice of Privacy Act system of records.

SUMMARY: Pursuant to the Privacy Act of 1974, the Department of Homeland Security (DHS), United States Coast Guard (USCG) gives notice that it is establishing a system of records for retaining certain biographical information on all passenger and crew members on board U.S. and foreign vessels bound for or departing from ports or places in the United States. The system of records is for the collection and processing of Notice of Arrival and Departure (NOAD) information pursuant to 33 CFR part 160, subpart C.

This information is maintained within the Ship Arrival Notification System (SANS) as well as other USCG systems used for screening and vetting of vessels, vessel crews and passengers. USCG is publishing a system of records notice (SORN) in order to permit the traveling public greater access to individual information and a more comprehensive understanding of how and where information pertaining to them is collected and maintained. Elsewhere in today's Federal Register, DHS has issued a Notice of Proposed Rulemaking to exempt this SORN from certain provisions of the Privacy Act.

DATES: Submit comments on or before January 12, 2009.

ADDRESSES: You may submit comments, identified by docket number DHS-2008-0121 by one of the following methods:

Federal e-Rulemaking Portal: http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=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://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&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://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions please contact: David Roberts (202-475-3521) United States Coast Guard Privacy Officer, United States Coast Guard. 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

United States Coast Guard (USCG) collects information related to Notice of Arrival and Departure (NOAD) for U.S. vessels in commercial service and all foreign vessels that are bound for or departing from ports or places of the United States. This information is maintained within the SANS, as well as other USCG systems used for screening and vetting of vessels, primarily, but not exclusively, through Marine Information for Safety and Law Enforcement (MISLE, DOT/CG 679, April 22, 2002, 67 FR 19612) and the Maritime Awareness Global Network (MAGNet, DHS/USCG-061, May 15, 2008, 73 FR 28143). Information is retrieved from SANS by vessel and not by personal identifier; however, USCG uses the information taken from SANS in other systems to conduct screening and vetting pursuant to its mission for protecting and securing the maritime sector.

The information that is required to be collected and submitted through Electronic Notice of Arrival and Departure (eNOAD) can be found on routine arrival/departure documents that passengers and crewmembers must provide to DHS, when entering or departing the United States. eNOAD information includes complete name, date and place of birth, gender, country of citizenship, travel/mariner document type, number and country of issuance, expiration date, country of residence, status on board the vessel, and United States destination address (except for U.S. Citizens, lawful permanent residents, crew and those in transit).

Additionally, vessel carriers and operators must provide the vessel name, vessel country of registry/flag, International Maritime Organization number or other official number, voyage number, date of arrival/departure, and foreign port where the passengers and crew members began/terminate their sea transportation to the United States.

USCG will collect vessel particulars that are submitted by the vessel owner, agent, master, operator, or person in charge of a vessel in advance of a vessel's arrival or departure from the United States. The information will be used to perform counterterrorism, law enforcement, safety and security queries to identify risks to the vessel or to the United States.

The purpose of the information collection is to assess risk to vessels arriving to or departing from a U.S. port and to identify vessels that may pose a safety or security risk to the United States.

The information collection allows USCG to facilitate effectively and efficiently the entry and departure of vessels into and from the

U.S. and assists the USCG with assigning priorities while conducting maritime safety and security missions in accordance with international and U.S. regulations.

Information in SANS is maintained for a period of no more than ten years or when no longer needed, whichever is longer, from the date of collection at

[[Page 75443]]

which time the data is deleted. The only NOAD information retained based initially on SANS data is information related to those individuals about whom derogatory information is revealed during the screening process. All other crew and passenger information vetted by USCG is immediately deleted. Should derogatory information be discovered by USCG either through TECS or USCG's own sources, such alerts and information would be communicated either through USCG's Maritime Awareness Global Network (MAGNet) system, or through the Coast Guard Messaging System (CGMS).\1\ The SANS data is transmitted to the Intelligence Coordination Center (ICC) and stored in the CoastWatch Pre-Arrival Processing Program (CP3). SANS data within CP3 is destroyed or deleted when no longer needed for reference, or when ten years old, whichever is later.

\1\ See http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.dhs.gov/privacy for PIAs for MAGNet and the
Law Enforcement Intelligence Database (LEIDB), a system used to analyze USCG message traffic.

Elsewhere in today's Federal Register, DHS has issued a Notice of Proposed Rulemaking to exempt this SORN from certain aspects of the Privacy Act.

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 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. SANS is not a system of records, but NOAD information maintained in SANS can be removed and used in other systems within USCG.

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 of their records, and to assist individuals to more easily find such files within the agency. Below is the description of the Asset Management 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 Number: DHS/USCG-029

SYSTEM NAME:

Notice of Arrival and Departure Information (NOAD)

SECURITY CLASSIFICATION:

Unclassified and Classified.

SYSTEM LOCATION:

SANS, the information technology system which receives NOAD information for USCG, is located at USCG Operations Systems Center in Kearneysville, WV. NOAD records may be maintained in SANS, or at computer terminals located at USCG Headquarters, Headquarters units, Area Offices, Sector Offices, Sector sub-unit Offices, and other locations where USCG authorized personnel may be posted to facilitate DHS' mission.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this notice consist of:

A. Crew members who arrive and depart the U.S. by sea, and

B. Individuals associated with a vessel and whose information is submitted as part of a notice of arrival or notice of departure, including but not limited to vessel owners, operators, charterers, reporting parties, 24-hour contacts, company security officers, and

C. Persons in addition to crew who arrive and depart the U.S. by sea.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records on vessels include: Name of vessel; name of registered owner; country of registry; call sign; International Maritime Organization (IMO) number or, if a vessel does not have an IMO number the official number; name of the operator; name of charterer; name of classification society; Maritime Mobile Service Identity (MMSI).

Records on arrival information as it pertains to the voyage includes: Names of last five foreign ports or places visited by the vessel; dates of arrival and departure for last five foreign ports or places visited; for each port or place of the U.S. to be visited, the name of the receiving facility, the port or place; for the port or place of the U.S. the estimated date and time of arrival; for the port or place in the U.S. the estimated date and time of departure; the location (port or place and country) or position (latitude and longitude or waterway and mile marker) of the vessel at the time of reporting; the name and telephone number of a 24-hour point of contact (POC).

Records on departure information as it pertains to the voyage includes: The name of departing port or place of the U.S., the

estimated date and time of departure; next port or place of call (including foreign), the estimated date and time of arrival; the name and telephone number of a 24-hour POC.

Records on crewmembers include: Full name; date of birth; nationality; identification type (for example, Passport, U.S. Alien Registration Card, U.S. Merchant Mariner Document, Foreign Mariner Document, Government Issued Picture ID (Canada), or Government Issued Picture ID (U.S.), number, issuing country, issue date, expiration date); position or duties on the vessel; where the crewmember embarked (list port or place and country); where the crewmember will disembark.

Records for each person onboard in addition to crew: Full name; date of birth; nationality; identification type (for example, passport, U.S. alien registration card, government issued picture ID (Canada), or government issued picture ID (U.S.), number, issuing country, issue date, expiration date); U.S. address information; where the person embarked (list port or place and country); where the person will disembark.

Records on cargo include: A general description of cargo other than Certain Dangerous Cargo (CDC) onboard the vessel (e.g., grain, container, oil, etc.); name of each CDC carried, including United Nations (UN) number, if applicable; amount of each CDC carried.

Records regarding the operational condition of equipment required by 33 CFR part 164: The date of issuance for the company's Document of Compliance certificate; the date of issuance of the vessel's Safety Management Certificate; the name of the Flag Administration, or recognized organization(s) representing the vessel flag administration, that issued those certificates.

[[Page 75444]]

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 14 U.S.C. 632; 33 U.S.C. 1223, 46 U.S.C. 3717; 46 U.S.C. 12501; Federal Records Act of 1950, P.L. 90-620; The Maritime Transportation Act of 2002, P. L. 107-295; The Homeland Security Act of 2002, P. L. 107-296; 33 CFR part 160, 36 CFR chapter XII.

Purpose(s):

The purpose of this system is to maintain Notice of Arrival and Notice of Departure information to screen individuals associated with vessels entering or departing U.S. waterways for maritime safety, maritime security, maritime law enforcement, marine environmental protection, and other related purposes.

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 U.S. Department of Justice (DOJ) (including U.S. 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 (2) any employee of DHS in his/her official capacity, or (3) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent said employee, or (4) the U.S. or any agency

thereof;

B. To a Congressional office, for 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 purposes of performing an 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) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) USCG 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, fraud, or harm to the security or integrity of this system, other systems, or programs (whether maintained by USCG or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons when reasonably necessary to assist in connection with the USCG's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government, when necessary to accomplish an agency function related to this system of records, in compliance with the Privacy Act of 1974, as amended;

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 Federal and foreign government intelligence or counterterrorism agencies or components where USCG 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.

I. 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, property, or other vital interests of a data subject and disclosure is proper and consistent with the official duties of the person making the disclosure;

J. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantined disease or for combating other significant public health threats; appropriate notice will be provided of any identified health threat or

risk;

K. 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, settlement negotiations, response to a subpoena, or in connection with criminal law proceedings;

L. 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 in the proper performance of the official duties of the officer making the disclosure;

M. To an appropriate Federal, state, local, tribal, territorial, 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;

N. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations where USCG is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law.

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

Storage:

SANS data is stored electronically at the National Vessel Movement Center located at USCG Operations Systems Center in Kearneysville, WV. USCG uses an alternative storage facility for SANS historical logs and system backups. Derivative NOAD system data may be stored on CG SWIII computers or CG unit servers located at USCG Headquarters, Headquarters units, Area Offices, Sector Offices, Sector sub-unit Offices, and other locations where USCG authorized personnel may be posted to facilitate DHS' mission.

Retrievability:

NOAD information maintained in SANS is not retrievable by name or other unique personal identifier. NOAD information is extracted from SANS by vessel and then retrieved by name, passport number, or other unique personal identifier.

Safeguards:

Information in this system is safeguarded in accordance with applicable laws, rules, and policies. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include role-based access provisions, restricting access to authorized personnel who have a need-to-know, using locks, and password protection identification features. USCG file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel.

The system manager, in addition, has the capability to maintain system back-ups for the purpose of supporting continuity of operations and the discrete need to isolate and copy specific data access transactions for the purpose of conducting security incident investigations.

All communication links with the USCG datacenter are encrypted. The databases are Certified and Accredited in accordance with the requirements of the Federal Information Security Management Act (FISMA).

Retention and Disposal:

Information on vessels maintained in SANS is destroyed or deleted when no longer needed for reference, or when ten years old, whichever is later. [National Archives and Records Administration (NARA) Request For Records Disposition Authority, Job No. N1-026-05-11]

Outputs, which include ad-hoc reports generated for local and immediate use to provide a variety of interested parties, for example, Captain of the Port and marine safety offices, sea marshals, Customs and Border Patrol (CBP), Immigration and Customs Enforcement (ICE)--with the necessary information to set up security zones, scheduling boarding and inspections activities, actions for non-compliance with regulations, and other activities in support of CG's mission to provide for safety and security of U.S. ports, will be deleted after five years if it is not a permanent record according to NARA.

The only NOAD information retained based initially on SANS data is information related to those individuals about whom derogatory information is revealed during the screening process. All other crew and passenger information vetted by USCG is immediately deleted. Should derogatory information be discovered by USCG either through TECS or USCG's own sources, such alerts and information would be communicated either through USCG's Maritime Awareness Global Network (MAGNet) system, or through the Coast Guard Messaging System (CGMS).\2\ This information will be maintained for the life of the investigation or ten years, which ever is longer. The SANS data is transmitted to the ICC and stored in the CP3. SANS data within CP3 is destroyed or deleted when no longer needed for reference, or when ten years old, whichever is later.

\2\ See http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.dhs.gov/privacy for PIAs for MAGNet and the Law Enforcement Intelligence Database (LEIDB), a system used to analyze USCG message traffic.

SYSTEM MANAGER(S) AND ADDRESS:

Commandant, CG-26, United States Coast Guard Headquarters, 2100 2nd Street, SW., Washington, DC 20593-0001.

NOTIFICATION PROCEDURES:

To determine whether this system contains records relating to you, write to the System Manager identified above. Your written request should include your name and mailing address. You may also provide any additional information that will assist in determining if there is a

record relating to you if applicable, such as your Merchant Mariner License or document number, the name and identifying number (documentation number, state registration number, International Maritime Organization (IMO) number, etc.) of any vessel with which you have been associated and the name and address of any facility (including platforms, deep water ports, marinas, or terminals) with which you have been associated. The request must be signed by the individual, or his/her legal representative, and must be notarized to certify the identity of the requesting individual pursuant to 28 U.S.C. 1746 (unsworn declarations under penalty of perjury). Submit a written request identifying the record system and the category and types of records sought to the Executive Agent. Request can also be submitted via the FOI/Privacy Acts. See http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.uscg.mil/foia/ for additional information.

RECORD ACCESS PROCEDURES:

Write the System Manager at the address given above in accordance with the ``Notification Procedure''. Provide your full name and a description of the information you seek, including the time frame during which the record(s) may have been generated. Individuals requesting access to their own records must comply with DHS's Privacy Act regulation on verification of identity (6 CFR 5.21(d)). Further information may also be found at http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.dhs.gov/foia or at http://frwebgate.access.gpo.gov/cgi-bin/leaving.cgi?from=leavingFR.html&log=linklog&to=http://www.uscg.mil/foia/.

CONTESTING RECORD PROCEDURES:

See ``Notification'' procedures above.

RECORD SOURCE CATEGORIES:

The system contains data received from vessel carriers and operators regarding passengers and crewmembers who arrive in, depart from, transit through the U.S. on a vessel carrier covered by notice of arrival and departure regulations.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

This system, however, may contain records or information recompiled from or created from information contained in other systems of records, which are exempt from certain provisions of the Privacy Act. For these records or information only, in accordance with 5 U.S.C. 552a (j)(2),(k) (1), and (k)(2), DHS will also claim the original exemptions for these records or information from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) through (I), (5), and (8); (f), and (g) of the Privacy Act of 1974, as amended, as necessary and appropriate to protect such information.

Dated: December 2, 2008.

Hugo Teufel III,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. E8-29279 Filed 12-10-08; 8:45 am]

BILLING CODE 4410-10-P