DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2011-0078]

Privacy Act of 1974; Department of Homeland Security United States Coast Guard-029 Notice of Arrival and Departure 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 proposes to update and reissue an existing system of records titled, "Department of Homeland Security United States Coast Guard-029 Notice of Arrival and Departure System of Records." This system of records allows the Department of Homeland Security/United States Coast Guard to facilitate the effective and efficient entry and departure of vessels into and from the United States and assist with assigning priorities for conducting maritime safety and security missions in accordance with international and United States regulations. As a result of the biennial review of this system, records have been updated to include cargo within the purpose and record source categories. This updated system will be included in the Department of Homeland Security's inventory of record systems. The Privacy Act exemptions for this system remain unchanged.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This system will be effective

[INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2011-0078 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 703-483-2999.
- Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 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: Marilyn Scott-Perez (202-475-3515) Privacy Officer, United States Coast Guard, 2100 2nd Street SW, Stop 7101, Washington, D.C. 20593. For privacy issues contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. §552a, the Department of Homeland Security (DHS) United States Coast Guard (USCG) proposes to update and

reissue an existing DHS system of records titled, "DHS/USCG-029 Notice of Arrival and Departure (NOAD) System of Records."

USCG collects information related to NOAD for U.S. vessels in commercial service and all foreign vessels bound for or departing from ports or waterways within the United States. This information is maintained within the Ship Arrival Notification System (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), DHS/USCG-013, June 25, 2009, 74 FR 30305 and the Maritime Awareness Global Network (MAGNet) System of Records Notice, DHS/USCG-061, May 15, 2008, 73 FR 28143. Information is retrieved from the SANS by vessel and not by personal identifier; however, USCG uses the information taken from the SANS in other systems to conduct screening and vetting of individuals 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 U.S. 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 (IMO) 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 U.S. 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 the effective and efficient entry and departure of vessels into and from the U.S. and assist the USCG with assigning priorities while conducting maritime safety and security missions in accordance with international and U.S. regulations.

NOAD information 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 which time the data is deleted. Should derogatory information be discovered by USCG either through TECS or USCG's own sources, such information would be communicated either through USCG's MAGNet, the Coast Guard Messaging System (CGMS), or other USCG systems.[1] NOAD data is transmitted to the Intelligence Coordination Center (ICC) and stored in the CoastWatch Pre-Arrival Processing Program (CP3). NOAD data within CP3

[1] See www.dhs.gov/privacy for PIAs for MAGNet and the Law Enforcement Intelligence Database (LEIDB), a system used to analyze USCG message traffic.

is destroyed or deleted when no longer needed for reference, or when ten years old, whichever is later.

As a result of the biennial review of this system, the purpose and the record source categories have been amended to include cargo. Cargo has been collected under previous rulemaking but was never included in the SORN. Disclosure to consumer reporting agencies category has also been added.

Consistent with DHS' information sharing mission, information stored in NOAD may be shared with other DHS components, as well as appropriate federal, state, local, tribal, territorial foreign, or international government agencies. This sharing will only occur after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice. This system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice 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 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 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. The SANS is not a system of records, but NOAD information maintained in the SANS can be removed and used in other systems within USCG. Below is the description of the DHS/United States Coast Guard-029 Notice of Arrival and Departure System of Records.

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

System of Records:

DHS/USCG-029

System name:

DHS/USCG-029 Notice of Arrival and Departure Information (NOAD)

Security classification:

Unclassified.

System location:

NOAD information for USCG is collected within the Ship Arrival Notification System (SANS) located at USCG Operations Systems Center in Kearneysville, WV. NOAD records may be maintained in the 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 crew members who arrive and depart the U.S. by sea and 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 persons in addition to crew who arrive and depart the U.S. by sea.

Categories of records in the system:

- Records on vessels includes: name of vessel; name of registered owner; country of registry; call sign; 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.
- Records on arrival information pertaining to the vessel 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 waterways 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 individual onboard in addition to crew include: full name; date of birth; nationality; identification type (for example: passport, U.S. alien registration card, government-issued picture ID (Canada), government-issued picture ID (U.S.), number, issuing country, issue date, expiration date); U.S. address information; and from where the person embarked (list port or place and country).
- Records related to cargo onboard the vessel 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; and 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.

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 NOAD information to screen individuals and cargo 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. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of a 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, 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.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

NOAD information is stored electronically in the SANS located at USCG Operations Systems Center in Kearneysville, WV. USCG uses an alternative storage facility for the SANS historical logs and system backups. Derivative NOAD system data may be stored on USCG Standard Workstation III computers or USCG 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 the SANS is not retrievable by name or other unique personal identifier. NOAD information is extracted from the SANS by vessel and then retrieved by name, passport number, or other unique personal identifier.

Safeguards:

NOAD data in the SANS 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:

In accordance with NARA Disposition Authority number N1-026-05-11, NOAD information on vessels and individuals maintained in the SANS is destroyed or deleted when no longer needed for reference, or after ten years old, whichever is later. Why does this seem much more general than other retention schedules? Is this consistent with other discussions of retention?

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, Immigration and Customs Enforcement 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 USCG's mission to provide for safety and security of U.S. ports, will be deleted after five years if they do not constitute a permanent record according to NARA.

System Manager and address:

Commandant, USCG-26, United States Coast Guard Headquarters, 2100 2nd Street, SW, Washington, D.C. 20593-0001.

Notification procedure:

The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, DHS/USCG will consider individual requests to determine whether or not information may be released. Thus, 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, 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://www.uscg.mil/foia/ for additional information.

Record access procedures:

Write to 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://www.dhs.gov/foia or at 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, crewmembers, and cargo which 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: October 13, 2011

Mary Ellen Callahan,

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2011-28975 Filed 11/08/2011 at 8:45 am; Publication Date: 11/09/2011]