9110-04

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2016-0045]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of modified Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security is modifying and reissuing a current Department of Homeland Security 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 notice was previously re-issued in the Federal Register on November 27, 2015. The Department is providing a further update based on comments received in response to the November 2015 update.

This system of records allows the United States Coast Guard (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 complying with maritime safety and security regulations. As part of the Department's ongoing effort to promote transparency regarding its collection of information, the Coast Guard is updating its November 2015 system of records notice to explain its changes to the routine uses. Additional updates to this notice were explained in the November 2015 update. Further, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. The Coast Guard has re-issued this systems of records notice in its entirety for clarity and transparency.

The Coast Guard also issued a Notice of Proposed Rulemaking (NPRM) to clarify the exemptions for this system at 80 FR 74018 (Nov. 27, 2015). Concurrently with this modified system of records notice, the Coast Guard has issued a Final Rule. Responses from the Coast Guard to comments to the NPRM for this system may be found in the Final Rule elsewhere in this issue of the Federal Register.

This modified system will be included in the Department of Homeland Security's inventory of record systems.

DATES: No further comments are being accepted. This modified system will be effective the date of this Federal Register notice.

ADDRESSES: No further comments are being accepted. This modified system will be effective the date of this Federal Register notice.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Marilyn Scott-Perez, (202) 475-3515, Privacy Officer, Commandant (CG-61), United States Coast Guard, 2703 Martin Luther King Jr. Ave, SE, Mail Stop 7710, Washington, D.C. 20593. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

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) is modifying and reissuing a current DHS system of records titled, "DHS/USCG-029 Notice of Arrival and Departure (NOAD) System of Records."

The collection and maintenance of this information assists DHS/USCG in meeting its statutory obligation to assign priorities while conducting maritime safety and security missions in accordance with international and U.S. regulations. DHS/USCG is modifying this system of records notice to update the routine uses in response to comments received in the November 2015 update of this records notice in the Federal Register and updated OMB Circular A-108.

This system of records notice was previously re-issued in the Federal Register on November 27, 2015 at 80 FR 74116. The Department is providing a further update based on comments received in response to this update.

First, in general, the commenter noted that the proposed routine uses exceed the scope of DHS's authority because these routine uses would permit the sharing of information outside maritime security and screening, which was the purpose for which it was originally gathered. DHS does not concur. It is within DHS's authority to share information legally obtained, and compatible with the purposes for which it was collected, with other law enforcement agencies and components. DHS has a mandate to protect the United States from law enforcement threats, and, as a result, is mandated to share such information with other Federal Government agencies. DHS is working to ensure information regarding threats is shared across the Government to reduce or disrupt threats and prosecute criminals.

Second, the commenter was specifically concerned with routine uses G, H, I, J, and M which permit DHS to disclose records to foreign entities, which are not subject to Privacy Act, consequently putting private information of American citizens at risk. The SORN has been modified to address some of the commenter's concerns. DHS's

partnerships with foreign governments and entities are critical to its ability to successfully apprehend criminals. DHS's refusal or inability to share information regarding suspected criminals would undermine its mutually beneficial relationships with these foreign governments and could impede DHS's efforts to gain information it needs for its efforts to fight crime targeted at the United States. However, to limit the scope of sharing with foreign partners, DHS will consider a foreign entity's ability to safeguard personally identifiable information (PII), and its commitment to and history of safeguarding such information, when determining whether to share records containing PII. In addition, with respect to Routine Use M, DHS will use fictitious data whenever possible when testing new technology, to further reduce risk of PII exposure.

Third, the commenter also stated that Routine Use N, which permits disclosure of information to the news media and public in three narrow instances, is too broad. DHS does not concur. As a Department that regularly interacts with the public and relies heavily on public trust, DHS must be able to preserve its integrity and correct the record when necessary. Prior to disclosing information pursuant to this routine use, the DHS Chief Privacy Officer and the DHS Office of the General Counsel conduct an analysis to minimize the effect of the disclosure and ensure that the disclosure sheds light on Government operations and would not constitute a clearly unwarranted invasion of personal privacy.

Consistent with DHS's information sharing mission, information stored in this system of records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions and missions. In addition, DHS/USCG

may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

The Coast Guard is issuing a Final Rule to clarify the exemptions for this system concurrently with this notice. This modified 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 Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, and similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/USCG-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 and to Congress.

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS)/United States Coast Guard (USCG)-029 Notice of Arrival and Departure.

SECURITY CLASSIFICATION: Unclassified. The data may be retained on classified networks but this does not change the nature and character of the data until it is combined with classified information.

SYSTEM LOCATION: The United States Coast Guard (USCG) maintains records in the operational system at the USCG Operations Systems Center, Kearneysville, West Virginia (WV), and in disaster recovery backup systems in other USCG field locations. USCG maintains records associated with this function in the Ship Arrival Notification System (SANS) operational information technology (IT) system.

DHS replicates records from the operational IT system and maintains them in other IT systems connected on the DHS unclassified and classified networks.

SYSTEM MANAGER(S): Commandant (CG-26), United States Coast Guard, 2703 Martin Luther King Jr. Ave., SE, Mail Stop 7301, Washington, D.C. 20593-0001.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The Secretary of the Department of Homeland Security has delegated to the Coast Guard authority from the Ports and Waterways Safety Act (33 U.S.C. 1221 et seq.). See specifically 33 U.S.C. 1223(a)(5), 1225, and 1231; 46 U.S.C. 3717; 46 U.S.C. 12501; the Maritime Transportation Act of 2002, Pub. L. 107-295; the Homeland Security Act of 2002, Pub. L. 107-296; 33 CFR part 160; and 36 CFR chapter XII.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to maintain NOAD information to improve navigation safety, enhance the Coast Guard's ability to identify and track vessels, and heighten the Coast Guard's overall situational and maritime

domain awareness (MDA), which will enhance mariners' navigation safety and the Coast Guard's ability to address threats to maritime transportation security.

DHS maintains a replica of some or all of the NOAD data in operational IT systems residing on unclassified and classified DHS networks to allow for analysis and vetting consistent with the above stated purposes and this published notice.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Crew members who arrive or depart the United States by sea; and other individuals or organizations associated with a vessel and whose information is submitted as part of a notice of arrival or notice of departure, such as vessel owners, operators, charterers, reporting parties, 24-hour contacts, company security officers, and passengers who arrive and depart the United States 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; and name of classification society.

Records on arrival information pertaining to the voyage include: Names of last five foreign ports or places the vessel visited; dates of arrival and departure for last five foreign ports or places it visited; for each port or place in the United States the vessel will visit, the name of the receiving facility; for the port or place in the United States the estimated date and time of arrival; for the port or place in the United States 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; and the

name and telephone number of a 24-hour point of contact (POC). This individual may be a crew or non-crew member.

Records on departure information pertaining to the voyage include: The name of the departing port or waterway of the United States; the estimated date and time of departure; next port or place of call (including foreign); the estimated date and time of arrival at the next port or place of call; and the name and telephone number of a 24-hour POC.

Records about crewmembers includes: Full name; date of birth; nationality; identification type (e.g., passport, U.S. Alien Registration Card, U.S. Merchant Mariner Document, foreign mariner document, government-issued picture identification (ID) (Canada) or (United States)); identification issue and expiration dates; position or duties on the vessel; location where the crewmember embarked (list port or place and country); and location where the crewmember will disembark.

Records about "other individuals associated with a vessel and whose information is submitted as part of a notice of arrival or notice of departure" (e.g., passenger information) includes: Full name; date of birth; nationality; identification type (e.g., passport, U.S. Alien Registration Card, government-issued picture ID); identification number, issuing country, issue date, expiration date; U.S. address information; and location where the individual 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); 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 include: The date of issuance for the company's document of compliance certificate; the date of issuance of the vessel's safety management certificate; and the name of the flag administration, or recognized organization(s) representing the vessel flag administration that issued those certificates.

RECORD SOURCE CATEGORIES: USCG obtains NOAD records from vessel carriers and operators regarding passengers, crewmembers, and cargo that arrive in, depart from, or transit through the United States on a vessel carrier covered by notice of arrival and departure regulations.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 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. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or 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 or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

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 (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization 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 determines that information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection to assist another federal recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach; or

2. DHS suspects or has confirmed that there has been a breach of this system of records; and (a) DHS has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, harm to DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (b) 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 breach or to 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, when 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. Prior to releasing information to a foreign entity, DHS will consider the foreign entity's ability to safeguard personally identifiable information, and its commitment to and history of safeguarding such information.

H. To federal and foreign government intelligence or counterterrorism agencies or components if USCG becomes aware of an indication of a threat or potential threat to national or international security, or if 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. Prior to releasing information to a foreign entity, DHS will

consider the foreign entity's ability to safeguard personally identifiable information, and its commitment to and history of safeguarding such information.

I. To an organization or individual in either the public or private sector, foreign or domestic, if 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. Prior to releasing information to a foreign entity, DHS will consider the foreign entity's ability to safeguard personally identifiable information, and its commitment to and history of safeguarding such information.

J. To appropriate federal, state, local, tribal, territorial, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, USCG will provide appropriate notice of any identified health threat or risk 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. Prior to releasing information to a foreign entity, DHS will consider the foreign entity's ability to safeguard personally identifiable information, and its commitment to and history of safeguarding such information.

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, 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 appropriate federal, state, local, tribal, territorial, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, if DHS 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, provided disclosure is appropriate in the proper performance of the official duties of the person making the disclosure. When testing new systems, fictitious data will be utilized whenever possible to reduce the risk of unwarranted disclosure. Prior to releasing information to a foreign entity, DHS will consider the foreign entity's ability to safeguard personally identifiable information, and its commitment to and history of safeguarding such information.

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, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/USCG stores records in this system electronically in the operational IT system, as well as on other IT

systems residing on the unclassified and classified networks or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

USCG stores NOAD information electronically in the Ship Arrival Notice System (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 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's mission.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: USCG retrieves records from the SANS by vessel. Information from the retrieved records may then be extracted by name, passport number, or other unique personal identifier. NOAD information maintained in the SANS operational IT system is not directly retrievable by name or other unique personal identifier.

NOAD data that is replicated on the unclassified and classified DHS networks to allow for analysis and vetting consistent with the above stated purposes and this published notice may be retrieved by all core and extended biographic fields (e.g., full name; date of birth; nationality).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: 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, whichever is later.

Outputs, which include ad-hoc reports generated for local and immediate use to provide a variety of interested parties with necessary information, are deleted after five years if they do not constitute a permanent record according to NARA. For example, in accordance with this schedule, USCG shares outputs with the Captains of the Port and marine safety offices, sea marshals, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement if they require such information to set up security zones, schedule boarding and inspections activities, take 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. Records replicated to IT systems residing on the unclassified and classified networks will also follow the same retention schedule.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: USCG safeguards NOAD data 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. In addition, the system manager 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).

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and those of the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/USCG will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Headquarters or USCG's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When seeking records about yourself from this system of records or any other Departmental system of records, your request must conform with the Privacy Act regulations set forth in 6 CFR part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, you should:

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered Judicial Redress Act records, see "access procedures" above.

NOTIFICATION PROCEDURES: See "Record Access procedure."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: No exemption shall be asserted with respect to information maintained in the system that is collected from a person if that person, or his or her agent, seeks access to or amendment of such information.

The Privacy Act, however, requires DHS to maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement or intelligence agency has sought particular records may affect ongoing law enforcement activities. The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2),

exempted this system from the following provisions of the Privacy Act: Sections (c)(3), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information. Further, DHS has exempted section (c)(3) of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(k)(2) as is necessary and appropriate to protect this information.

HISTORY: 73 FR 75442; 76 FR 69749; 79 FR 64812; 80 FR 74116.

Dated: July 10, 2017.

Jonathan R. Cantor,
Acting Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2017-14841 Filed: 7/14/2017 8:45 am; Publication Date: 7/17/2017]