



9110-04

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2016-0074]

Privacy Act of 1974; Department of Homeland Security /United States Coast Guard –

031 USCG Law Enforcement (ULE) System of Records

AGENCY: Department of Homeland Security, Privacy Office.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records titled, “Department of Homeland Security/United States Coast Guard-031 USCG Law Enforcement (ULE) System of Records.” This system of records allows the Department of Homeland Security/United States Coast Guard to collect and maintain records related to maritime law enforcement, marine environmental protection, and the determinations supporting enforcement action taken by the United States Coast Guard. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the Federal Register. This newly established system will be included in the Department of Homeland Security’s inventory of record systems.

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

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

ADDRESSES: You may submit comments, identified by docket number DHS-2016-0074 by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

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, please visit <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Marilyn Scott-Perez (202-475-3515), Privacy Officer, Commandant (CG-61), United States Coast Guard, 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 proposes to establish a new DHS system of records titled, “DHS/United States Coast Guard-031 USCG Law Enforcement (ULE) System of Records.”

The collection and maintenance of this information will allow the DHS/USCG to collect and maintain records regarding maritime law enforcement, security, marine safety, and environmental protection activities. USCG Law Enforcement consists of certain records that were formerly covered under the DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE) system of records. These records are being moved under ULE to maintain USCG law enforcement and case-related data in one repository. In addition to the transfer of this law enforcement data out from under MISLE to ULE, this notice also serves to inform that USCG Biometrics at Sea System records, which are collected under the purpose and identified authorities cited herein, are maintained in the Automated Biometric Identification System (IDENT)—the DHS biometric repository maintained by the DHS Office of Biometric Identity Management. Separately and elsewhere in the Federal Register, the remaining portions of the records covered under MISLE will be republished under two new systems of records: the Vessel Identification System and the Merchant Vessel Documentation System. The MISLE SORN will be retired upon the publication of all three new systems of records.

USCG Law Enforcement may contain information on persons who come into contact with USCG through its law enforcement, safety, and environmental protection activities, including vessel and facility owners, operators, crew, employees, passengers, and other persons associated with a USCG law enforcement or environmental protection

activity or having an interest in the subject vessel or facility involved or identified in the respective case file. Consistent with the authority being enforced, ULE collects and maintains in case files both biographic and, as appropriate, references to biometric records obtained from individuals and persons, as well as identifying information relating to ownership, registry, and location of vessels and facilities.

Consistent with DHS's information-sharing mission, information stored in the DHS/USCG-031 USCG Law Enforcement (ULE) 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. In addition, information may be shared 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.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in the Federal Register. This newly established 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. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/USCG-031 USCG Law Enforcement (ULE) 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 of Records

Department of Homeland Security (DHS)/USCG–31

System name:

DHS/USCG-031 USCG Law Enforcement (ULE) System of Records.

Security classification:

Sensitive but Unclassified.

System location:

Records are maintained at the United States Coast Guard (USCG) Headquarters in Washington, D.C., USCG Operations Systems Center (OSC) in Kearneysville, WV, and other field locations. Records collected from the USCG Biometrics at Sea System (BASS) are maintained at the DHS Office of Biometric Identity Management in Washington, D.C. The Marine Information for Safety and Law Enforcement (MISLE) System is the information technology (IT) repository for marine safety, security,

environmental protection, and law enforcement records. The Automated Biometric Identification System (IDENT) is the IT repository for USCG BASS records.

Categories of individuals covered by the system:

Individuals with established relationship(s) or associations to maritime vessels or marine transportation facilities that are the subject of enforcement or compliance activities regulated by the USCG. This may include:

- Vessel owners or operator;
- Charterers;
- Masters;
- Crew members;
- Vessel or boat agents;
- Mortgagees;
- Lien claimants;
- Vessel builders;
- Transportation facility owners, managers, or employees;
- Individuals who own, operate, or represent marine transportation companies; and
- Other individuals come into contact with the USCG as part of an enforcement or compliance activity.

Categories of records in the system:

The following information may appear in case files, reports, investigations, and other documents (either physical or electronic) maintained by USCG relating to an enforcement or compliance activity:

- Name of individual, vessel, or facility;
- Home and work address;
- Home, work, and mobile phone numbers;
- Facility number;
- Involved party identification number;
- Social Security number (SSN);
- Driver license number;
- Alien Registration Number (A-Number);
- Military identification number;
- U.S. Coast Guard license number;
- Foreign seaman's booklet number;
- Resident alien number;
- Merchant mariners license or documentation number;
- Taxpayer Identification Number (TIN);
- Casualty case number;
- Pollution incident case number;
- Date of incident;
- Civil penalty case number;
- Biometric information, which may include:
 - Photographs and digital images,
 - Height,

- Weight,
- Eye color,
- Hair color,
- Fingerprints, and
- Irises.Videos;
- Vessel or boat registration data;
- Port visits;
- Vessel or boat inspection data;
- Vessel or boat documentation data;
- Port Safety boarding;
- Casualties;
- Pollution incidents, civil violations (as applicable), and associated information (data pertaining to people or organizations associated with the subject vessels);
- Information on marine transportation facilities including:
 - Name,
 - Identification number,
 - Location,
 - Commodities handled,
 - Equipment certificates,
 - Approvals,
 - Inspection reports,

- Pollution incidents, and
- Casualties.
- Violations of U.S. laws and data pertaining to people or organizations associated with those facilities;
- For owners, operators, agents, and crew members;
- Statements submitted by USCG personnel relating to boarding;
- Investigations as a result of a pollution and/or casualty incident, as well as any violations of United States law, along with civil penalty actions taken as a result of such violations. Such reports could contain names of passengers on vessels, as well as witnesses to such violations; and
- Narratives, reports, and documents by USCG personnel describing their activities on vessels and within facilities, including incident reports, violations of laws, and international treaties

Authority for maintenance of the system:

14 U.S.C 89a, 93(a) and (c), 632; 16 U.S.C 1431; 33 U.S.C 1223; 33 U.S.C. 1228; 46 U.S.C. 3717; 46 U.S.C. 12119, 12501-502.

Purpose(s):

The purpose of this system is to collect and maintain USCG case records and other reported information relating to the safety, security, law enforcement, environmental, and compliance activities of vessels, facilities, organizations engaged in marine transportation, and related persons.

Routine uses of records maintained in the system, including categories of users and

the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (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 U.S. 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 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 the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) 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, 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.

H. To federal and state safety enforcement agencies, including, but not limited to, the Maritime Administration and National Transportation Safety Board, U.S. Department of Transportation, to access historical data that may assist in safety investigations and improve transportation safety.

I. To federal, state, and local environmental agencies, including, but not limited to, the U.S. Environmental Protection Agency, to access historical data that may improve compliance with U.S. laws relating to environmental protection.

J. To the U.S. Department of Defense and related entities, including, but not limited to, the Military Sealift Command and U.S. Navy, to access data on safety information regarding vessels chartered by those agencies.

K. To the International Maritime Organization or intergovernmental organizations, nongovernmental organizations, or foreign governments in order to conduct joint investigations, operations, and inspections;

L. To federal, state, or local agencies with which the U.S. Coast Guard has a Memorandum of Understanding, Memorandum of Agreement, or Inspection and Certification Agreement pertaining to Marine Safety, Maritime Security, Maritime Law Enforcement, and Marine Environmental Protection activities.

M. 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 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:

DHS/USCG stores records in this system electronically 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.

Retrievability:

Records may be retrieved by name of individual, vessel, or facility, facility number, involved party identification number, SSN, TIN, driver license number, (A-Number), military identification number, U.S. Coast Guard license number, cellular number, foreign seaman's booklet number, resident alien number, merchant mariners license or documentation number, person or organization name, casualty case number, pollution incident case number, date of incident, civil penalty case number, USCG unit entering data, or incident location.

Biometric records associated with case files or reports may be retrieved from IDENT by reference to the applicable Organization/Unit/Subunit designations for the

Biometrics-at-Sea-System.

Safeguards:

DHS/USCG safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. USCG has imposed strict controls 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.

Retention and disposal:

Records are retained in accordance with National Archives and Records Administration (NARA) schedule N1-026-05-15 approved July 7, 2005. Most of the records in this system are retained indefinitely by NARA; however law enforcement boarding activities are retained for three years. A copy of this system has been transferred to the National Archives and Records Administration permanent records collection. Updates of system information are transferred to NARA every 5 years. All system hardware and data is stored at OSC, Kearneysville, WV. Backups are performed daily. Copies of backups are stored at an off-site location.

System Manager and address:

Commandant (CG-633), United States Coast Guard, Mail Stop 7710, Washington, D.C. 20593; Commandant (BSX), United States Coast Guard, Mail Stop 7501, Washington, D.C. 20593; Director, United States Coast Guard, National Vessel Documentation Center, 792 T J Jackson Drive, Falling Waters, WV 25419; IDENT

Program Management Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

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, 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 the Chief Privacy Officer and Commandant (CG-611), United States Coast Guard, whose contact information can be found at <http://www.dhs.gov/foia> under "Contacts." 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 (FOIA) Officer, Department of Homeland Security, Washington, D.C. 20528-0655.

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.

Record access procedures:

See “Notification procedure” above.

Contesting record procedures:

See “Notification procedure” above.

Record source categories:

Records are obtained from USCG boardings, USCG inspections, USCG investigations, USCG documentation offices, and vessel notice of arrival reports in the course of normal routine business. This information is gathered from the owners,

operators, crew members, agents, passengers, witnesses, other government agencies, and USCG personnel. In addition records or record identifiers are ingested from other DHS and Federal systems, including IDENT, Vessel Identification System (VIS), Merchant Vessel Documentation System (MVDS), and the National Crime Information Center (NCIC).

Exemptions claimed for the system:

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3-4), (d), (e)(1-3), (e)(5), (e)(8), and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2) has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f).

When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

Dated: December 1, 2016

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

[FR Doc. 2016-29341 Filed: 12/7/2016 8:45 am; Publication Date: 12/8/2016]