<NO

<PREAMB>

9110-04

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2020-0231]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security, United States Coast Guard.

ACTION: Notice of Modified Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/United States Coast Guard (USCG)-061 Maritime Awareness Global Network (MAGNET) System of Records." The modified system of records is to be reissued and renamed as "DHS/USCG-061 Maritime Analytic Support System (MASS) System of Records." This system of records allows the DHS/USCG to collect and maintain records in a centralized location that relate to the U.S. Coast Guard's missions that are found within the maritime domain. The information covered by this system of records is relevant to the eleven U.S. Coast Guard statutory missions (Port, Waterways, and Coastal Security (PWCS); Drug Interdiction; Aid to Maritime Navigation; Search and Rescue (SAR) Operations; Protection of Living Marine Resources; Ensuring Marine Safety, Defense Readiness; Migrant Interdiction; Marine Environmental Protection; Ice Operations; and Law Enforcement). DHS/USCG is updating this system of records notice to include and update additional data sources, system security and auditing protocols, routine uses, and user interfaces. Additionally, DHS/USCG is concurrently issuing a Notice of Proposed Rulemaking, and subsequent Final Rule, to exempt this system of records from certain provisions of the Privacy Act due to criminal, civil, and administrative enforcement

requirements. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

This modified system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be applicable **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER (DAY/MONTH/YEAR)]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2020-0231 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: Constantina Kozanas, 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 DHS-2020-0231. 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: Kathleen Claffie, (202) 475-3515, HQS-DG-M-CG-61-PII@uscg.mil, Chief, Office of Privacy Management (CG-6P), U.S. Coast Guard, 2703 Martin Luther King, Jr. Ave. SE Stop 7710, Washington, D.C. 20593-7710. For privacy questions, please contact: Constantina Kozanas, (202) 343-1717, Privacy@hq.dhs.gov, 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. sec. 552a, the Department of Homeland Security (DHS) / U.S. Coast Guard (USCG) proposes to modify and reissue a current DHS system of records titled, "DHS/USCG-061 Maritime Awareness Global Network (MAGNET) System of Records." The modified system of records is to be reissued and renamed as "DHS/USCG Maritime Analytic Support System (MASS) System of Records."

The Coast Guard's enterprise modernization to the MAGNet framework prompted the need to reissue this SORN. The updated framework enables the U.S. Coast Guard to:

(1) Improve the system's security protocols by enhancing system access authentication processes.

(2) Enhance data management services by hosting MASS in a cloud environment, allowing USCG to apply new technologies to better tag data for retention, access, and use purposes.

(3) Refresh user interfaces making MASS more user-friendly and intuitive to access and use.

(4) Ingest new data sources on an as-needed basis in the future more easily.

(5) Update routine uses for MASS by either adding or removing previous routine uses. A new routine use (D) is being added to account for disclosures relating to performing audit or oversight operations; new routine uses (E) and (F) are being added to conform to Office of Management and Budget M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (January 3, 2017); a new routine use (I) is being added to account for disclosures related to investigating threats or potential threats to national or international security or assisting in counterterrorism efforts; a new routine use (N) is being added to account for disclosures related to the purpose of testing new technology; and a new routine use (O) is being added to account for disclosures to news media and public with the approval of the Chief Privacy Officer. Previous routine uses (A), (C), (E), and (K)

have been removed as disclosures are authorized under new routine uses (D), (H), (H), and (A), respectively. Finally, USCG is re-lettering several of the routine uses to align with these changes.

These updates better accommodate the accomplishment of the eleven U.S. Coast Guard statutory missions. Those missions require the collection of a wide range of information, including personally identifiable information (PII). The collection and use of PII is required to effectively conduct the responsibilities associated with these mission areas and promote Maritime Domain Awareness (MDA).

MASS provides storage and access to maritime information and provides basic search capabilities either by a person or by vessel. Person searches may be retrieved by passport or merchant mariner license number. Vessel searches may be retrieved by vessel name, hull identification, or registration number. MASS enhances current capabilities by adding data sources, media storage, access capabilities, and infrastructure to provide rapid, near real-time data to the USCG and other authorized organizations. MASS users leverage the ability to share, correlate, and provide classified and unclassified data across agency lines to provide MDA critical to homeland and national security and safety.

MASS receives data from several systems both within and outside of DHS through electronic transfers of information. These electronic transfers include the use of Secure File Transfer Protocol (SFTP), system-to-system communications via specially written Internet Protocol socket-based data streaming, database-to-database replication of data, electronic transfer of database transactional backup files, and delivery of formatted data via electronic mail.

Consistent with DHS's information sharing mission, information stored in MASS 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, 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.

Additionally, DHS/USCG is updating rulemaking associated with this system of records to exempt certain provisions of the Privacy Act due to criminal, civil, and administrative enforcement requirements. Furthermore, this notice includes non-substantive changes to simplify the formatting and text of the previously published 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. Similarly, the Judicial Redress Act (JRA) provides covered persons the statutory right 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 Maritime Awareness Support System (MASS) System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this revised 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)-061 Maritime Analytic Support System (MASS)

SECURITY CLASSIFICATION: Unclassified, Classified.

SYSTEM LOCATION: Records may be maintained at all locations at which the USCG operates or at which Coast Guard operations are supported including: U.S. Coast Guard Headquarters and field offices as listed on the USCG website. System information may be duplicated at other locations where the USCG has been granted direct access for support of Coast Guard missions for purposes of system back up, emergencies, preparedness, and/or continuity of operations. The main system is currently located at U.S. Coast Guard Intelligence Coordination Center, Department of Homeland Security, National Maritime Intelligence Center, Washington, D.C. 20395.

SYSTEM MANAGER(S): Commandant, Coast Guard Intelligence (CG-2), U.S. Coast Guard Headquarters, 2701 Martin Luther King, Jr. Avenue SE, Washington, D.C. 20032.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Maritime information is critical to accomplish the eleven Coast Guard statutory missions mentioned above. The collection of the pertinent information in support of these missions have been authorized by: 14 United States Code (U.S.C.) secs. 1, 2, 81, 88, 89, 91, 93, 94, 141, 143, 634; 19 U.S.C. 1401; 33 U.S.C. secs. 1221, 1223, 1321; 46 U.S.C. 2306, 3306, 3717, 12501; 46 U.S.C. 3306; 50 U.S.C. 191; 33 U.S.C. 1223; the Magnuson-Stevens Fisheries Conservation and Management Act, 16 U.S.C. 1801; the Lacey Act, 16 U.S.C. secs. 3371-78; the Endangered Species Act, 16 U.S.C. secs. 1531-44; the National Marine Sanctuaries Act, 16 U.S.C. secs. 1431-45; The Espionage Act of 1917; 33 U.S.C. 1221, The Ports and Waterways Safety Act (PWSA); The Maritime Transportation Security Act of 2002 (MTSA), Pub L. No. 107-295; The Homeland Security Act of 2002, Pub L. No. 107-296; National Presidential Security Directive 41 (NPSD); and 33 Code of Federal Regulations (CFR) Part 160.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to enhance the U.S. Coast Guard's capabilities by developing a total picture of the maritime environment and

the people, places, and things that affect it. The enhancements of this picture effectively promote the successful execution of the Coast Guard's statutory missions of Port, Waterways, and Coastal Security (PWCS); Drug Interdiction; Aid to Maritime Navigation; Search and Rescue (SAR) Operations; Protection of Living Marine Resources; Ensuring Marine Safety; Defense Readiness; Migrant Interdiction; Marine Environmental Protection; Ice Operations; and Law Enforcement.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Individuals associated with vessels, facilities, companies, organizations, and ports involved in the maritime sector.

2. Individuals identified through observation by and interaction with Coast Guard personnel during Coast Guard operations that include boarding of vessels, conducting aircraft over-flights, and through Field Intelligence Support team (FIST) sightings and reports.

3. Individuals identified during Coast Guard enforcement actions as violating, suspected of violating, or witnessing the violations of U.S. laws, international laws, or treaties.

4. Individuals associated with vessels or other individuals that are known, suspected, or alleged to be involved in contraband trafficking, illegal migrant activity (smuggling, trafficking, and otherwise), or terrorist activity.

5. Any other individual not listed above who operates in, or affects, the maritime domain.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. Information related to individuals associated with vessels, companies, organizations, and ports involved in the maritime sector includes:

- Name;
- Nationality;

- Address;
- Telephone number;
- Taxpayer or other identification number;
- Date of birth;
- Relationship to vessels and facilities;
- The individuals' relationship to other individuals, companies, government agencies, and organizations in MASS;
- Individuals involved with pollution incidents, and violations of laws and international treaties; and casualties to include publicly available information; and
- Information gathered from publicly available social media.

2. Field Intelligence Reports, Requests for Information, Intelligence Information Reports, Situation Reports, Operational Status Reports, and Operations Reports on:

A. Individuals who are associated with vessels involved in contraband trafficking, illegal migrant activity (e.g., smuggling, trafficking), or any other unlawful act within the maritime sector, and with other individuals who are known, suspected, or alleged to be involved in contraband trafficking, illegal migrant activity (e.g., smuggling, trafficking), terrorist activities, or any other unlawful act within the maritime sector.

B. Individuals, companies, vessels, or entities associated with the maritime industry (e.g., vessel owners, vessel operators, vessel characteristics, crewmen, passengers, facility owners, facility managers, facility employees, or any other individuals affiliated with the maritime community) to include publicly available information (including social media sources).

C. Commodities handled, equipment, location, certificates, approvals, inspection data, pollution incidents, casualties, and violations of all laws and international treaties.

RECORD SOURCE CATEGORIES: Information contained in MASS is gathered from a variety of sources both internal and external to the Coast Guard. Source information

may come from sensors, inspections, boardings, investigations, documentation offices, vessel notice of arrival reports, owners, operators, crew members, agents, passengers, witnesses, employees, U.S. Coast Guard personnel, law enforcement notices, commercial sources, as well as other federal, state, local, and international agencies that are related to the maritime sector and/or national security sector. In addition, MASS maintains information from open source data (i.e., publicly available information) including social media sources.

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 the U.S. Attorneys Offices, or other federal agencies 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 only 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 (GSA) pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization 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 there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach, there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the federal government, or national security; 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 breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the 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.

G. 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.

H. 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.

I. To an appropriate federal, state, territorial, tribal, local, international, or foreign government intelligence entity, counterterrorism agency, or other appropriate authority charged with investigating threats or potential threats to national or international security or assisting in counterterrorism efforts, when a record, either on its face or in conjunction with other information, identifies a threat or potential threat to national or international security, or DHS reasonably believes the information may be useful in countering a threat or potential treat, which includes terrorist and espionage activities, and disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure.

J. To an appropriate federal, state, or local agency entity, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

K. To appropriate federal, state, local, tribal, foreign governmental agencies, multilateral governmental organizations, and non-governmental or private organizations for the purpose of protecting the vital interests of a data subject or their persons, including to assist such agencies or organizations in preventing exposure to or transmission of a

communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk.

L. To the International Maritime Organization (IMO), intergovernmental organizations, nongovernmental organizations, or foreign governments in order to conduct investigations, operations, and inspections pursuant to its authority.

M. To an organization or individual in either the public or private sector, either foreign or domestic, when 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 or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

N. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data for purposes of testing new technology.

O. 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 a database. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/USCG may retrieve records by name (individual, company, government agency or organization), boat

registration number, documented vessel name/number, tax payer or other identification number, address, and telephone number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Dynamic information on vessel position(s) and movement(s) will be readily retrievable for three (3) years and then archived. Seven (7) years after being archived the records will be deleted from the system. The other information discussed in the Categories of Records section will be readily retrievable for five (5) years and then archived. Ten (10) years after being archived the records will be deleted from the system. This information is stored for this length of time to ensure the analytic process is properly informed and to show patterns or history to analysts in the course of their duty. The requirements supporting the collection and storage of data are reviewed regularly.

Audit records, maintained to document access to information relating to specific individuals, will be readily retrievable for 90 days and then moved to long term storage. After five (5) years the records will be deleted from the system. Access to audit records will only be granted to authorized personnel.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL 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.

RECORD ACCESS PROCEDURES: 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 and intelligence system. However, DHS/USCG will consider individual requests to determine whether information may be

released. 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 U.S. Coast Guard FOIA Office (CG-611), whose contact information can be found at http://www.dhs.gov/foia under "Contacts Information." If an individual believes more than one DHS 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 the individual may be available under the Freedom of Information Act (FOIA).

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual 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, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes 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 an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second individual certifying his/her agreement for the first individual to access his/her records.

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

CONTESTING RECORD PROCEDURES: Because this system contains classified and sensitive but unclassified information related to intelligence, counterterrorism, homeland security, and law enforcement programs, records in this system have been exempted from notification, access, and amendment to the extent permitted by subsections (j)(2) and (k)(1) and (2) of the Privacy Act. A request to amend non-exempt records in this system may be made by writing to the System Manager, identified above, in conformance with 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS.

NOTIFICATION PROCEDURES: See "Record Access Procedures."

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

HISTORY: 73 FR 28143 (May 15, 2008); 73 FR 56924 (Final Rule) (Sept. 30, 2008).

Constantina Kozanas,
Chief Privacy Officer,
Department of Homeland Security.
<FRDOC> [FR Doc. 2020–25540 Filed 11–20–20; 8:45 am]
<BILCOD> BILLING CODE 4410–10–P

[FR Doc. 2020-25540 Filed: 11/20/2020 8:45 am; Publication Date: 11/23/2020]