



## DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2020-0232]

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security  
United States Coast Guard-061 Maritime Analytic Support System (MASS) System of  
Records.

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

**ACTION:** Notice of proposed rulemaking.

**SUMMARY:** The Department of Homeland Security is giving concurrent notice of a modified and reissued system of records pursuant to the Privacy Act of 1974 for the “Department of Homeland Security/United States Coast Guard-061 Maritime Analytic Support System (MASS) System of Records” and this proposed rulemaking. In this proposed rulemaking, the Department and the United States Coast Guard propose to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

**DATES:** Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

**ADDRESSES:** You may submit comments, identified by docket number DHS-2020-0232, 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.

*Instructions:* All submissions received must include the agency name and docket number for this notice. 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, Chief, Office of Privacy Management (CG-6P), United States Coast Guard, 2703 Martin Luther King, Jr. Ave. SE Stop 7710, Washington, D.C. 20593-7710. For privacy issues, please contact: Constantina Kozanas, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

**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 modify and reissue the 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, as explained in the revised system of records notice reissued concurrently with this proposed rule.

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 collects information from numerous data sources in order for the Coast Guard to successfully execute its eleven statutory missions. 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

DHS is issuing this Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act.

## 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 the 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 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.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/USCG-061 Maritime Analytic Support System (MASS) System of Records. Some information in DHS/USCG-061 Maritime Analytic Support System (MASS) System of

Records relates to official DHS national security, law enforcement, and intelligence activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS's ability to obtain information from third parties and other sources; to protect the privacy of third parties; and to safeguard classified information. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case-by-case basis.

A notice of system of records for DHS/USCG-061 Maritime Analytic Support System (MASS) System of Records is also publishing elsewhere in this issue of the Federal Register.

#### **List of Subjects in 6 CFR Part 5**

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend chapter I of title 6, Code of Federal Regulations, as follows:

#### **PART 5--DISCLOSURE OF RECORDS AND INFORMATION**

1. The authority citation for Part 5 continues to read as follows:

**Authority:** 6 U.S.C. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301.

2. In Appendix C to Part 5, revise paragraph 8 to read as follows:

#### **Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act**

\* \* \* \* \*

8. The Department of Homeland Security (DHS)/United States Coast Guard

(USCG)-061 Maritime Analytic Support System (MASS) System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/USCG-061 Maritime Analytic Support System (MASS) System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. The DHS/USCG-061 Maritime Analytic Support System (MASS) System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies.

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) and (4); (d); (e)(1) through (3), (e)(4)(G) through (I), (e)(5) and (8); (f); and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 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) through (I), and (f).

Where a record received from another system has been 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.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

- (a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that

investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. When an investigation has been completed, information on disclosures made may continue to be exempted if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In

the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

- (d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.
- (e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.
- (f) From subsections (e)(4)(G) through (I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.
- (g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

\*\*\*\*\*

Constantina Kozanas,  
Chief Privacy Officer,  
Department of Homeland Security

[FR Doc. 2020-25541 Filed: 11/20/2020 8:45 am; Publication Date: 11/23/2020]