Privacy Impact Assessment
for the

Maritime Analytic Support System (MASS)

DHS/USCG/PIA-005(a)

April 24, 2020

Contact Point
LCDR Gerrod Glauner
U.S. Coast Guard
(202) 372-2795

Reviewing Official
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) United States Coast Guard (USCG) has developed the Maritime Analytic Support System (MASS) as a platform with the means to access records that are part of the MASS System of Records (previously called the Maritime Awareness Global Network (MAGNet) System of Records). The system employs a combination of system software, database management software, and custom written software to support the execution of the eleven USCG statutory missions. The USCG is updating and replacing the original MAGNet Privacy Impact Assessment (PIA) to establish MASS as the update to the MAGNet framework, and to describe the system's use of personally identifiable information (PII) from members of the public.

Overview

MASS was developed to establish Maritime Domain Awareness (MDA). MDA is the review and collection of as much information as possible about the maritime world, and provides storage, access, and basic search capabilities of maritime information. MASS establishes a full awareness of the entities (people, places, things) and their activities within the maritime industry. MASS collects the information described above, and through algorithms or link analysis, connects that information to provide a more robust picture in order to allow the successful execution of the eleven statutory USCG missions: Ports, 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.

MASS enhances current capabilities by adding additional data sources, media storage, access capabilities, and infrastructure to provide rapid, near real-time data to the Coast Guard and other authorized organizations in accordance with the routine uses in the forthcoming MASS System of Records Notice (SORN).[1] USCG and MASS users leverage the ability to share, correlate, and provide classified and unclassified data across the Coast Guard to provide MDA critical to homeland national security and safety.

MASS receives data from 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.

The Office of Coast Guard Intelligence (CG-2) uses MASS to provide awareness to the field, as well as strategic planners, by aggregating data from existing sources internal and external

[1] The MAGnet SORN, "DHS/USCG-061 Maritime Awareness Global Network (MAGNet)" is being updated to more clearly provide notice of what and how information is being used in MASS. That SORN will be renamed "DHS/USCG-061 Maritime Analytic Support System (MASS)."

to the Coast Guard. MASS correlates and provides the medium to display information such as ship registry, current ship position, crew background, passenger lists, port history, cargo, known criminal vessels, and suspect lists. CG-2 serves as MASS's executive agent and shares appropriate aggregated data on a need to know basis with other law enforcement and intelligence agencies.

MASS provides output to the Common Operating Picture (COP). The COP is an integrated or "common" view of the vessels operating in water that are important to the U.S. Government, including geographic positions of the vessels, as well as characteristics of the vessels. The COP is integrated (or "shared") amongst authorized users and is commonly used within the USCG and the Department of Defense (DoD) to monitor areas of operation. The output destined for the COP may be submitted to the Common Intelligence Picture (CIP) for review prior to the data being transferred to the COP. Additionally, users are able to run queries about specific vessels or vessel movement from workstations and retrieve additional information from the MASS database. MASS is able to accept data from the realms of geospatial and imagery, and then process this data into the MASS database. This allows MASS to accumulate position reports from the COP.

MASS provides access to the database via Coast Guard workstations located throughout the world; the system is accessible on multiple networks at different classification levels. It is expected that the workstations are properly equipped to access the appropriate networks with current Internet-style applications or browser technology. Users at workstations are able to query the system online using either pre-stored parameterized queries or queries built ad hoc by the users. Results of database searches are returned online to the users for viewing and/or processing at their workstations. Prior to gaining account access, users must complete the System Authorization Access Request (SAAR) form, which also requires that individual to provide justification for access. Once the form is completed and signed, it is routed to the user's supervisor (or System Security Office for access to the classified data). Once approved, the user is then authorized to access only that data for which he or she has been approved; access controls are then implemented through the user's Common Access Card (CAC).

Due to the age of the MAGNet system and legacy processes, a review was conducted to modernize it. The Coast Guard Intelligence Enterprise approved the requested update to the MAGNet framework, prompting the need to refresh the existing PIA.[2] The updated framework enables the Coast Guard to improve the system's security protocols, data management services, user interfaces, routine uses for sharing information, and ingest new data sources on an as needed basis.

The Coast Guard's eleven missions require the collection of a wide range of information, which includes the collection of PII. The collection and use of PII within MASS generates inherent privacy risks. The fundamental privacy risks identified within MASS include the potential over-collection of information, the disclosure of PII to unauthorized recipients, and the inaccuracies of

[2] The original MAGNet PIA (DHS/USCG/PIA-005 USCG Maritime Awareness Global Network (MAGNet)) will be retired upon publication of this PIA. Retired PIAs are available at https://www.dhs.gov/privacy.

publicly available data found in the open source domain. This PIA identifies techniques and methods used to mitigate these privacy risks and discusses them below.

Section 1.0 Authority and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

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.) §§ 1, 2, 81, 88, 89, 91, 93, 94, 141, 143, 634; 19 U.S.C. § 1401; 33 U.S.C. §§ 1221 et seq 1223, 1321; 46 U.S.C. §§ 2306, 3306, 3717, 12501; 46 U.S.C. Subtitle VII, § 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. §§ 3371-3378; the Endangered Species Act, 16 U.S.C. §§ 1531-1544; the National Marine Sanctuaries Act, 16 U.S.C. §§ 1431-1445; The Espionage Act; The Ports and Waterways Safety Act (PWSA); The Maritime Transportation Security Act of 2002 (MTSA), Pub L. 107-295; The Homeland Security Act of 2002, Pub L. 107-296; National Presidential Security Directive 41 (NPSD); and 33 Code of Federal Regulations Part 160.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The MAGnet SORN, "DHS/USCG-061 Maritime Awareness Global Network (MAGNet)"[3] is being updated to more clearly provide notice of what and how information is being used in MASS. That SORN will be renamed "DHS/USCG-061 Maritime Analytic Support System (MASS)."

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The Authority to Operate (ATO) for MASS will be granted upon completion of this PIA.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The MAGNet Records Management disposition schedule is registered under N1-026-08-1 with the National Archives and Records Administration (NARA). The MASS Records Management Disposition schedule (SF-115) was drafted and submitted to NARA for review and

[3] DHS/USCG-061 Maritime Awareness Global Network (MAGNET), 73 FR 28143 (May 15, 2008).

approval. MASS will follow the MAGNet disposition schedule until approval of the MASS SF-115 is received from NARA.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

MASS does not interact directly with individuals to collect information and only operates as an electronic database; therefore, the PRA does not apply.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

MASS's data and records are a compilation of many systems and sources. MASS collects records of information, as described below, on ports, port facilities, maritime vessels, and vessel characteristics.

- Vessel characteristics can include performance data, vessel identification data, registration data, movements, reported locations, activity, and associate information. Associate information can include data pertaining to people or organizations associated with vessels, owners, passengers, and crew members.
- Reports submitted by Coast Guard crew members relating to boarding, over-flights, or other means of surveillance, as well as any violations of the U.S. laws or treaties, along with enforcement actions taken during boarding. Such reports and activities could contain electronic documents, biometric, photographic, and video data, as well as names of passengers on vessels, owners, crew members, and agents.
- Records containing information on vessels and associates that are known, suspected, or alleged to be involved in contraband trafficking, illegal migrant activity (e.g., smuggling, trafficking), or terrorist activity.
- Records containing information on facilities and their characteristics, including location, commodities handled, equipment, certificates, approvals, inspection data, pollution incidents, casualties, and violations of all laws and international treaties, if applicable, and information pertaining to individuals, companies, and organizations associated with those facilities such as owners, operators, managers, and employees.
- Records containing information on individuals (to include PII), companies, government agencies, and other organizations associated with vessels, facilities

(including platforms, bridges, marinas, terminals, and factories), and/or Coast Guard activities including nationality, address, telephone number, and Social Security number (SSN), taxpayer identification number or other identification number;[4] date of birth; relationship to vessels and facilities; their relationship to other individuals, companies, government agencies, and organizations in MASS; pollution incidents; casualties; and violations of all laws and international treaties.

2.2 What are the sources of the information and how is the information collected for the project?

MASS electronically collects information from other systems operated by government entities. MASS collects information from these systems because of their relevance in supporting the execution of the eleven Coast Guard missions. It is the intention of the Coast Guard to include additional sources of information that have not yet been identified and to allow users of the system to store textual remarks about the data. At present, MASS receives data from the following systems:[5]

U.S. Coast Guard's Ship Arrival Notification System (SANS)

U.S. Coast Guard's Marine Information for Safety for Law Enforcement (MISLE)

U.S. Coast Guard's Nationwide Automated Identification System (NAIS)

U.S. Coast Guard's Common Operating Picture (COP)

U.S. Coast Guard's Common Assessment and Reporting Tool (CART)

U.S. Coast Guard's Satellite Automated Identification System (SAIS)

U.S. Coast Guard, Coast Guard Messaging System CGMS / Navy Command and Control Office Information Exchange (C2OIX) Messages

U.S. Navy's Sea Watch System

U.S. Navy's Merchant Ships Characteristics (MSC) System

U.S. Customs and Border Protection's Daily Hazardous Cargo Reports

U.S. Department of Transportation's Maritime Safety and Security Information System (MSSIS)

[4] MASS receives vessel information and associated entities of personnel from the Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) system. Social Security numbers (SSN) are used as unique identifiers in MISLE for personnel associated with Vessels. MASS also receives and processes Notice of Arrival and Departure (NOAD) information from the USCG Ship Arrival Notification System (SANS). Although SSNs are not required or requested, it is sometimes submitted as part of the NOAD.

[5] A list of all systems providing data to MASS and their applicable SORNs are found in Appendix A. This Appendix will be updated as new data is ingested.

Long Range Identification Tracking system (LRIT)

Department of Motor Vehicles: State of California

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

MASS contains and uses open source information from numerous sources, including publicly available social media. This information is collected to resolve open USCG cases, to identify gaps or discrepancies in collected information, and to provide the most current information for Coast Guard missions. The variety of the data being collected and used is dictated by mission requirements.

2.4 Discuss how accuracy of the data is ensured

The MASS system does not check the data for accuracy itself. Accuracy of the data is solely based on the quality of MASS data sources. Because the MASS system and its supporting personnel do not interact directly with individuals to collect PII, there is no opportunity for MASS to verify accuracy with the individuals. However, once source systems are updated with new or updated information, MASS receives those updates based on the source system's schedule.

2.5 Privacy Impact Analysis: Related to Characterization of the information.

The Coast Guard requires the collection of data associated with maritime safety and security operations. MASS is capable of complex data processing and handling, and the USCG uses this information to establish MDA and to assist in the execution of its eleven statutory missions.

Privacy Risk: There is a risk of inaccurate data within the system.

Mitigation: This risk is partially mitigated. All of the MASS information is not specifically collected from individuals therefore MASS depends on input from the collecting sources. MASS users are trained to identify and verify the veracity of the information being used. If users determine the data is incorrect, MASS users manually notify the source system of that information. This risk is further mitigated through information updates from the source systems. As sources update and correct erroneous information, MASS will subsequently update to match the source based on the refresh rate of the source system.

Privacy Risk: There is a risk for the potential of collecting more information than is necessary for Coast Guard to complete its mission.

Mitigation: This risk is partially mitigated. As described above, information is limited to that information that would be relevant to the maritime sector and specific USCG cases. This helps to mitigate any risks associated with the collection of a large amount of information. MASS is

designed to provide a total awareness for maritime officers and officials. Fulfillment of this goal requires a large amount of information.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

MASS gives users the ability to share, correlate, and provide classified and unclassified data across the Coast Guard to provide MDA critical to homeland and national security and safety. MASS collects as much information (people, places, and things) as possible in the maritime community relating to USCG's eleven statutory missions. This awareness is in accordance with these missions and crucial in ensuring homeland and national security and safety.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

MASS enables its users the ability to conduct simple or complex searches or queries. Searches will query the MASS database for information that is pertinent to the user's specific search term(s) and role-based access and will return only the data based on that search criteria.

MASS will also recommend values that hold the same criteria searched for, even if there are minor spelling inconsistencies in the data. Additionally, users can request alerts on specific database information. For example, upon data ingest, if new information is found then the capability will let the user know that new information is available for his or her specific query. MASS does not provide "data mining" capability[6] as a specific search is required to return information.

MASS by design does not conduct automated analytics but is used in conjunction with authorized and approved link analysis or query-based tools. The Coast Guard designates and implements tools on an "as needed" basis to improve capabilities, information security, and functionality. These specific tools are meant to assist the users in analysis, case management, data visualization, and document production on a secure platform.

3.3 Are there other components with assigned roles and responsibilities within the system?

The information collected by and maintained in MASS may be shared across all government components, agencies, and departments that are responsible for ensuring homeland and national security and safety. This information includes any information listed in the Section 2.1 of this PIA. Any entity that has established a need for maritime information is considered;

[6] Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3.

however, records containing PII will only be shared with organizations that possess appropriate authority.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of PII being used by or disclosed to unauthorized recipients.

Mitigation: This risk is mitigated. Access controls are implemented within the system and the database to ensure PII is only available to those who have an appropriate need to know.[7] Specifically, Coast Guard security and auditing systems were installed and configured to maintain access control within the database. Coast Guard security systems are used to protect PII by automatically filtering data by user access level. Audit logs are used to record all users and queries that access PII. For example, MASS uses auditing tools to record queries run against U.S. persons. Finally, all users of the system must sign a user agreement to protect the data and are not granted access until the signed form is provided.

Memoranda of Agreement (MOA) are established with all of the agencies that provide data to the MASS system. As noted in Section 8.0, the user groups and access controls employed in MASS help mitigate the risk of misuse.

Privacy Risk: There is a risk of inaccurate commercial or publicly available data being used by MASS users to make decisions.

Mitigation: This risk is mitigated by several factors. First, open source information is used to resolve gaps or discrepancies in existing MASS data; all searches of commercial data are predicated on existing data and interests. Commercial or publicly available data is not the sole source of information on which users will take action. Second, all open source data accessed by MASS users is stored separately and tagged as open source information. This is done to preserve the integrity of USCG information.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

MASS's data and records are a compilation from many sources and USCG is reliant on those source agencies to provide notice. MASS and its supporting personnel do not interact directly with individuals to collect PII. However, USCG provides notice through the publication of this PIA and the forthcoming MASS SORN.

[7] For example, individuals without a need to know would not have access to another user's case.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals may address consent issues with the source systems that collect information, but MASS itself does not provide a mechanism for consent to use. MASS is confined to the uses described in this PIA and the relevant SORN.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that USCG does not provide sufficient notice of collection of this information.

Mitigation: This risk is partially mitigated. MASS's data and records are a compilation from many sources. MASS and its supporting personnel do not interact directly with individuals to collect PII, so USCG cannot directly provide notice. However, notice is provided through the publication of this PIA and the forthcoming MASS SORN.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

MASS will follow the MAGNet disposition schedule until approval of the MASS disposition schedule is received from NARA. The proposed MASS disposition schedule is as follows:

- Dynamic information on vessel position(s) and movement(s) will be readily retrievable for three (3) years and then moved to long term storage. After seven (7) years the records will be deleted from the system. The other information as laid out in Section 2.1 will be readily retrievable for five (5) years and then moved to long term storage. After ten (10) years 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. Records will be kept accessible online for three (3) years, then archived offline within MASS to support ongoing investigations or law enforcement activities.
- 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 authorize personnel.

5.2 Privacy Impact Analysis: Related to Retention

Information is needed for the period specified to continuously analyze data. Maintaining this data as directed allows for trend analyses. The periods described above align not only with MASS's mission requirements, but also the policy that information retention should be kept to the minimum necessary in order to fulfill mission duties.

Privacy Risk: There is a risk that information in MASS is maintained longer then required or necessary.

Mitigation: This risk is mitigated. Records within MASS, as well as associated access records, have date time stamps associated with the records. As the records reach their maturity based upon storage procedures and requirements, the records will be automatically deleted. These deletions will be retained up to two months based upon archive and backup procedures in case of system issues or errors and will then be automatically permanently deleted.

MASS will follow the MAGNet disposition schedule until approval of the MASS disposition schedule is finalized. MASS's technical capability will allow for a seamless transition moving to the MASS disposition schedule once it is formally approved by NARA.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

All or a portion of the records or information may be disclosed through authorized channels and liaisons to national and international governing bodies, agencies, and departments. Disclosure of information outside of DHS is only authorized once the receiving party has established a need to know that coincides with DHS, Intelligence Community, and DoD related missions, investigations, and interests of national security. All sharing will be documented as required by the Privacy Act of 1974, as amended. Information sharing during routine information management inspections conducted by NARA or other federal government agencies is also part of normal agency operations. The forthcoming MASS SORN will contain specific descriptions of normal agency operations. The MASS SORN will also identify reasons for the sharing of information and who may access it.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

External sharing noted in 6.1 is a summary of what will be cited in the forthcoming MASS SORN. The MASS SORN will establish specific routine uses for data sharing, including with whom and with what entities it can be shared. The SORN accurately depicts how the information will be used by external entities. As noted above, all sharing is either required by law or coincides

with DHS, Intelligence Community, and DoD related missions, investigations, and otherwise in the interests of national security.

6.3 Does the project place limitations on re-dissemination?

Before information can be shared with external DHS entities, a Memorandum of Understanding (MOU), an Information Sharing Agreement (ISA), and/or a Memorandum of Agreement (MOA) must be established. Specific limitations on the re-dissemination are established on case-by-case basis with each outside entity. MOUs, ISAs, and MOAs will be dictated by a need to know and mission requirements and are reviewed by the USCG Privacy Office.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

All disclosures to the public outside of the DHS are made via a Freedom of Information Act or Privacy Act request. All other disclosures of records are made in accordance with each specific MOU, ISA, or MOA. All ad hoc requests for information are forwarded to the source system's owner for response. These records are maintained in accordance with the records management disposition schedule established with NARA.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of unauthorized re-dissemination of information from MASS.

Mitigation: This risk is mitigated by establishing specific MOUs, ISAs, and MOAs with entities outside of DHS. These agreements and understandings outline the legal actions and repercussions to be taken in the event the outside entity fails to adhere to the agreement or understanding. The use of the Privacy Act request reinforces that information is protected under the Privacy Act.

Section 7.0 Redress

7.1 What are the procedures which allow individuals to access their own information?

An individual may seek access to his or her records by filing a Privacy Act or Freedom of Information Act (FOIA) request. Only U.S. citizens, lawful permanent residents, and covered persons from a covered country under the Judicial Redress Act (JRA) may file a Privacy Act request. Individuals not covered by the Privacy Act or JRA still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. If an individual would like to file a Privacy Act or FOIA request to view his or her record, he or she may mail the request to the following address:

Commandant (CG-6P)
Attn: FOIA/PA Officer
U.S. Coast Guard
2703 Martin Luther King, Jr. Ave. SE
Washington, D.C. 20593-7710
(202) 372-8413
eFOIA@uscg.mil

All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing an individual access to these records could inform the target of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another agency.

However, USCG evaluates requests for access and redress on a case-by-case basis. During the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective law enforcement, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals seeking to correct records contained in MASS, or seeking to contest their content, may submit a request in writing to the Coast Guard via mail, facsimile, or email:

Commandant (CG-6P)
Attn: FOIA/PA Officer
U.S. Coast Guard
2703 Martin Luther King, Jr. Ave. SE
Washington, D.C. 20593-7710
(202) 372-8413
eFOIA@uscg.mil

All or some of the requested information may be exempt from correction pursuant to the Privacy Act to prevent harm to law enforcement investigations or interests. Providing individual access to these records could inform the target of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another agency. Access to these records could also permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, or avoid detection or apprehension. However, USCG evaluates requests for correction and redress on a case-by-case basis. During the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced may be unclear or the relevance of the information may not be immediately apparent. In the interest of effective law enforcement, it is appropriate to retain all possibly relevant information that may aid in establishing patterns of unlawful activity.

7.3 How does the project notify individuals about the procedures for correcting their information?

The forthcoming MASS SORN and this PIA provide notice of the procedures. As noted above, USCG will review any information request on a case-by-case basis.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be able to correct or access their information.

Mitigation: This risk is partially mitigated. MASS is not a primary collector of information and is a sensitive but unclassified (SBU) to Top Secret system. As noted in Section 2.2, MASS regularly updates information received from information sources. This ensures that MASS has the most accurate information available to its users. This means that the source systems noted above, and not MASS, are in the best position to correct erroneous or outdated information. Information changes in the source systems will affect change in MASS.

MASS is also exempted from certain provisions of the Privacy Act regarding access and redress. Nonetheless, USCG will examine each separate request on a case-by-case basis, and, after conferring with the appropriate component or agency, may waive applicable exemptions in appropriate circumstances, or when it would not appear to interfere with or adversely affect the law enforcement or national security purposes of the systems from which the information is recompiled or in which it is contained.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

The Coast Guard established the use of security and auditing solutions that are installed and configured to maintain access controls within the database. Coast Guard designated security and auditing solutions are used to control access, viewing, and search functionality to sensitive information. Coast Guard security and auditing solutions also control read-write access to the database, and track queries run against sensitive data, including who has made changes to this data.

Access to the data within MASS is restricted through the use of multi-factor authentication and an established need to know. A username and password can only be obtained once the user has completed training specific to safeguarding information.

Additionally, the Coast Guard Privacy Office (CG-6P) will conduct a USCG Privacy Evaluation (CGPE) within one year of publication of this PIA. Coast Guard Privacy will share the results of the CGPE with the DHS Privacy Office.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

MASS does not provide training specific to the use of this system. The Coast Guard provides general training for Coast Guard personnel users which consist of USCG Federal Cyber Awareness Training and DHS: Protecting Personal Information, among other law enforcement and intelligence specific training. To receive access the user must complete the specific annual training requirements in order to receive and maintain access to the system.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

A "new user" request form is used by prospective users to request access to the system. Prospective users can be categorized as any and all individuals with a need to know, appropriate access levels, and are in support of the eleven Coast Guard missions. The "new user" request form is made available through the approval of the user's supervisor. The "new user" request form is a PDF that must be filled out by any interested party requiring access to MASS. Once the party fills out the request, the form is submitted by the user's supervisor to CGFixIT.[8] There is a two-person review of the information contained on the form, first by the person's management and then by staff at CGFixIT prior to granting access to MASS. CGFixIT will contact the individual to verify the information on the request and create a user account according to the needs of the individual. Only personnel with a need to know and who have the appropriate background checks, security clearances, and have completed the annual privacy training will be granted access.

The roles and rules used within the MASS system were verified during system testing prior to each release of the system. The assignment of the roles is verified by the MASS staff prior to granting access to MASS. Accounts are reviewed on a regular basis to ensure users are re-vetted and are active users. USCG analysts and officers leaving duty where MASS access is required have their accounts immediately deactivated. This deactivation occurs through the CGFixIT process once the user transfers or departs from their Unit or the USCG. In addition, MASS user accounts are locked automatically after 30 days of inactivity, and deactivated 45 days after no activity.

[8] CGFixIT is USCG's enterprise service desk ticketing system that allows end users to request IT services, such as account provisioning.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Before information can be shared with external DHS entities, an MOU, ISA, or MOA must be established. MOUs, ISAs, and MOAs will be dictated by a need to know and mission requirements and are reviewed by the USCG Privacy Office and all other appropriate stakeholders.

Responsible Officials

Mr. Eric Downes
Deputy Chief Information Officer (CIO) for Intel (CG-26)
U.S. Coast Guard

Kathleen L. Claffie
Chief, Office of Privacy Management (CG-6P)
U.S. Coast Guard

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security

Appendix A: Systems from which MASS Receives Data

SYSTEM	PIA	SORN
USCG Ship Arrival Notification System (SANS)	DHS/USCG/PIA-006(b) Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System (AIS) (April 28, 2015), available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-update-uscg-noad-ais-04-28-2015.pdf	DHS/USCG-029 Notice of Arrival and Departure System of Records (July 17, 2017), 82 FR 32715, available at: https://www.federalregister.gov/documents/2017/07/17/2017-14841/privacy-act-of-1974-system-of-records
USCG Marine Information for Safety for Law Enforcement (MISLE)	DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE) (September 3, 2009), available at: https://www.dhs.gov/sites/default/files/publications/privacy_pia_008_uscg_misle_2009.pdf	DHS/USCG-013 Marine Information for Safety and Law Enforcement (MISLE) System of Records (June 25, 2009), 74 FR 30305, available at: https://www.govinfo.gov/content/pkg/FR-2009-06-25/html/E9-14906.htm
USCG Nationwide Automated Identification System (NAIS)	Not a privacy sensitive system	Not a privacy sensitive system
USCG Common Operating Picture (COP)	Not a privacy sensitive system	Not a privacy sensitive system
USCG Common Assessment and Reporting Tool (CART)	DHS/USCG/PIA-022 Coast Guard Maritime Information eXchange (July 30, 2015), available at: https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscg-cgmix-july2015.pdf	DHS/USCG-031 USCG Law Enforcement (ULE) System of Records (December 8, 2016), 81 FR 88697, available at: https://www.regulations.gov/document?D=DHS-2016-0074-0001
USCG Satellite	Not a privacy sensitive system	Not a privacy sensitive system

Automated Identification System (SAIS)		
USCG, Coast Guard Messaging System CGMS / Navy Command and Control Office Information Exchange (C2OIX) Messages	DHS/USCG/PIA-004 USCG Law Enforcement Information Data Base (LEIDB)/Pathfinder (March 31, 2008), available at: https://www.dhs.gov/sites/default/files/publications/privacy_pia_004-uscg-leidbpathfinder-2008.pdf	DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder System of Records (September 30, 2008), 73 FR 56930, available at: https://www.govinfo.gov/content/pkg/FR-2008-09-30/html/E8-22612.htm
U.S. Navy's Sea Watch System	Not a privacy sensitive system	Not a privacy sensitive system
U.S. Navy's Merchant Ships Characteristics (MSC) System	Not a privacy sensitive system	Not a privacy sensitive system
U.S. Customs and Border Protection's Daily Hazardous Cargo Reports	DHS/CBP/PIA-006 Automated Targeting System (ATS) (January 13, 2017), available at: https://www.dhs.gov/publication/automated-targeting-system-ats-update	DHS/CBP-006 Automated Targeting System (ATS) System of Record (May 22, 2012), 77 FR 30297, available at: https://www.govinfo.gov/content/pkg/FR-2012-05-22/html/2012-12396.htm
U.S. Department of Transportation's Maritime Safety and Security Information System (MSSIS)	Not a privacy sensitive system	Not a privacy sensitive system
Long Range Identification Tracking system (LRIT)	Not a privacy sensitive system	Not a privacy sensitive system
Department of Motor Vehicles:	N/A	N/A

State of California		