Privacy Impact Assessment
for the

Marine Information for Safety and Law Enforcement (MISLE) System

September 3, 2009

Contact Point
Mr. Gary Chappell
MISLE Project Officer
U.S. Coast Guard
CG-635
(202) 372-1293

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Coast Guard Marine Information for Safety and Law Enforcement (MISLE) system is a steady-state system designed to capture information required to support the Coast Guard's marine safety, security, environmental protection and law enforcement programs. Supporting these programs require the collection of personally identifiable information about individuals associated with vessels as well as investigatory information. The Coast Guard has conducted this privacy impact assessment because MISLE collects and uses personally identifiable information.

Introduction

In 2002, the MISLE system integrated the functions of several existing stand-alone systems into a single system to improve the Coast Guard's ability to track its interactions with vessels, facilities, waterways, people, and organizations. MISLE integrated the Marine Safety Information System (MSIS), the Law Enforcement Information System (LEIS), and the Search and Rescue Management Information System (SARMIS) into one system. MISLE continues and expands upon the ability of those systems to document and create histories of Coast Guard actions related to vessels, facilities, people, organizations, and Coast Guard units.

MISLE is the Coast Guard's primary operations business support system. Coast Guard personnel use MISLE to schedule and record operational activities such as vessel boardings, facility inspections, marine casualty investigations, pollution response actions, law enforcement actions, and search and rescue operations. Coast Guard personnel enter data on response actions in real time as the incident unfolds. Coast Guard personnel enter most data on boardings, inspections, and investigations into MISLE after completion of the action. MISLE is also used to record and generate official documents such as Certificates of Inspection and Certificates of Documentation for vessels. MISLE uses historical data on vessels, facilities, people, organizations, and waterways to identify risks and target operational activities accordingly. In addition, Coast Guard unit and program managers use MISLE data to evaluate the effectiveness of operations and the use of Coast Guard resources.

MISLE is only available to authorized Coast Guard personnel via the Coast Guard intranet. However, the Coast Guard provides extracted information from MISLE to federal and state agencies to meet their mission requirements and some information on vessels, facilities, and organizations is provided to the public. Data provided to meet mission requirements for other agencies include: vessel inspection and casualty data to the Military Sealift Command to enhance safety, vessel and facility casualty data to the Department of Labor and State safety agencies to enhance safety and recreational vessel registration data to State titling and registration personnel to prevent fraud and deter boat theft.

Coast Guard personnel directly enter information into MISLE based on their knowledge of the activity, vessel, facility, person, or organization. Some information is entered into MISLE automatically through connections with other information systems, including: incident notifications received from the National Response Center, security plans received from Homeport[1], U.S. mariner information received

[1] Homeport is a publicly accessible, secure Internet portal that supports diverse Coast Guard needs for critical information sharing and service delivery to the maritime industry, partner agencies and Coast Guard users.

from the Merchant Mariner Licensing and Documentation System (MMLD), Coast Guard resource information received from the Abstract of Operations System (AOPS) and vessel arrival information received from the Ship Arrival Notification System (SANS). MISLE also collects information derived from submissions by the public (reports or forms), or from documents reviewed or collected by Coast Guard personnel (certificates or licenses). Reports received from the public include reports of marine casualties, notices of arrival, reports of pollution incidents and reports of distress.

Section 1.0 Information Collected and Maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

1.1 What information is to be collected?

MISLE collects information on vessels, facilities, Coast Guard activities, information on individuals and organizations, and adjudication information.

Vessel Information

MISLE collects information on vessels and their characteristics, including: vessel identification data, (Name, Type, Identification number, Call Sign, etc.), registration data (country or state of registration, authorized uses, etc.) documents (Certificate of Registry, Safety Certificates, Security Plans, etc.), and dimensions (length, width, tonnage, etc.). MISLE also retains a history of Coast Guard contacts with vessels, (maritime safety and security boardings, casualties, pollution incidents, and violations of laws and international treaties, etc.) and information on relationships with individuals, companies, and organizations associated with those vessels such as owners, operators, agents, and crew members.

Facility Information

MISLE collects information on maritime facility characteristics, including: name, type, identification number, location, commodities handled and contact information. MISLE also retains a history of Coast Guard contacts with those facilities (inspections, pollution incidents, casualties, and violations of laws and international treaties) and information on relationships with individuals, companies, organizations, vessels and waterways associated with those facilities.

Coast Guard Activities

MISLE includes records of activities performed by Coast Guard personnel involving vessels, facilities, persons, and organizations. These activities include: vessel sightings, boardings, examinations and inspections (safety and security inspections); documentation of vessels; facility inspections and examinations; inspections of freight containers; notifications of vessel arrivals and incidents; responses to incidents (Search and Rescue, Pollution, etc.); investigations of marine casualties and pollution incidents;

Homeport has a separate PIA.

controls placed on vessels, facilities, persons and organizations; enforcement actions (civil penalties, warnings, license revocations, etc); and security assessments. In addition, the names of Coast Guard personnel performing the activity are included in some activity records.

Information on Individuals and Organizations

MISLE collects information on individuals, companies, government agencies, and other organizations associated with vessels, maritime facilities (including platforms, bridges, deep water ports, marinas, terminals, and factories), waterways and Coast Guard activities. This information includes: name, nationality, address, telephone number, and taxpayer or other identification number (for example: Social Security number, drivers license number, Passport Number, Military ID, VISA Number, etc.); date of birth. MISLE also retains a history of Coast Guard contacts with those individuals and organizations (pollution incidents, casualties, violations of laws or international treaties, etc.) and their relationship to vessels, facilities and other individuals, companies, government agencies and organizations. MISLE retains records of access to and entries into the system made by Coast Guard personnel as part of its security protocol. Otherwise, information on Coast Guard personnel is not captured unless they are the subject of an activity or event (such as SAR), usually during off duty hours.

Adjudication Information

MISLE stores some information in its docket module from TurboCourt. TurboCourt is a commercial service that provides on-line form filling assistance and electronic filing for individuals and attorneys for court filings for a large number of courts in almost thirty states. The Coast Guard adjudicates proceedings related to the suspension and revocation of Merchant Mariner Credentials. The Docketing Module in MISLE is the electronic document repository for all documents used by the Administrative Law Judge (ALJ) program in Coast Guard cases. This information includes the name, mailing address, email address, and phone numbers of respondents, attorneys, and witnesses.

1.2 From whom is information collected?

Vessel Information

Coast Guard personnel obtains information on vessels through one of the following means: documents submitted by an individual or organization associated with the vessel for use in a business process (vessel registration, application for inspection, arrival notice, security plan, etc.), documents viewed by Coast Guard personnel while on the vessel (boardings, inspections, investigations, etc.), direct communication with an individual or organization associated with the vessel (boardings, inspections, investigations, etc.), or search of other databases (Lloyds Register, State boat registration databases, Maritime Mobile Service Identity (MMSI) database, and EQUASIS.

The Lloyds Register database is a propriety commercial database of vessels and vessel owners licensed from Lloyds Register – Fairplay, LTD. State boat registration databases are maintained by each state for recreational boats that primarily operate in that state. The Federal Communications Commission (FCC) and several maritime organizations authorized by the FCC assign MMSI numbers. MMSI numbers issued to vessels along with information on the vessel and vessel operator are reported to the Coast Guard and maintained in a database within MISLE. EQUASIS is a database maintained by the European Commission

for the reporting of Port State control actions on vessels. Information on state registered vessels is collected from State Boating Registration systems and consolidated in the Vessel Identification System (VIS) portion of MISLE.

Facility Information

Coast Guard personnel obtain information on facilities through one of the following means: documents submitted by an individual or organization associated with the facility for use in a business process (International Convention for the Prevention of Pollution from Ships marine pollution MARPOL certification, operations manual, security plan.), documents viewed by Coast Guard personnel while on the facility (inspections, spot checks, investigations.), direct communication with an individual or organization associated with the facility (inspections, spot checks, investigations), or search of other databases (United States Army Corps of Engineers (USACE) Port Series, Minerals Management Service Platform database.).

Information on Individuals and Organizations

Coast Guard personnel obtain information on individuals and organizations through one of the following means: documents submitted by an individual or organization for use in a business process (vessel registration, arrival notice, security plan, response plan, etc.), documents viewed by Coast Guard personnel while on a vessel or facility (boardings, inspections, investigations, etc.), direct communication with an individual or organization (boardings, inspections, investigations, etc.), or search of other databases (Merchant Mariner Licensing and Documentation System, Direct Access, etc.). Ownership information on State registered vessels is collected from State Boating Registration systems and consolidated in the Vessel Identification System (VIS) portion of MISLE.

1.3 How is the information being collected?

Coast Guard personnel enter most information directly into MISLE based on their knowledge of the activity, vessel, facility, person or organization. Some information is entered into MISLE automatically through connections with other information systems, including: incident notifications received from the National Response Center, security plans received from Homeport, U.S. mariner information received from the Merchant Mariner Licensing and Documentation System (MMLD), Coast Guard resource information received from the Abstract of Operations System (AOPS) and vessel arrival information received from the Ship Arrival Notification System (SANS). Information on State registered vessels and their owners is downloaded from State Boat Registration Systems monthly and consolidated in the VIS portion of MISLE. The remaining information is derived from submissions by the public, such as reports/forms, or from documents reviewed or collected by Coast Guard personnel, such as certificates or licenses. Reports received from the public include reports of marine casualties, notices of arrival, reports of pollution incidents and reports of distress.

1.4 Why is the information being collected?

The Coast Guard collects this information to support its marine safety, security, environmental protection, and law enforcement programs. The information enables the Coast Guard to identify safety and security risks so that it can more effectively target those vessels, facilities, persons and organizations that present the greatest risks (such as risk of a vessel collision resulting in pollution or injury, risk of security

breaches resulting in injury or property damage, or risk of introduction of contraband or illegal aliens into the U.S.), thereby protecting the maritime transportation system and its users. It also allows the Coast Guard to evaluate the effectiveness of its operations. For instance, tracking trends in vessel collisions and groundings allows the Coast Guard to determine the effectiveness of its prevention activities including the allocation of Coast Guard resources and tracking how resources for those prevention activities.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

Under 46 U.S.C. § 3717, the Coast Guard was directed to establish a Marine Safety Information System to collect information on commercial vessels operating in U.S. waters. Under 46 U.S.C. § 12501 the Coast Guard was directed to establish a Vessel Identification System to make available information on the ownership of documented and state registered vessels. Under 14 U.S.C. Chapter 5 the Coast Guard is assigned a variety of duties, including aids to navigation, saving life and property and law enforcement. Under 33 U.S.C. § 1223, the Coast Guard was assigned wide authority to set vessel operating requirements, including requiring pre-arrival messages.

1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.

The primary risks identified with data collection are as follows: collecting inaccurate information, inappropriate release during transmission, and inappropriate release by system users. These risks were minimized through training and system design. Coast Guard personnel who collect and enter most information into MISLE receive training in identifying the accuracy and completeness of information prior to collecting information. MISLE is only available on the Coast Guard intranet and user access controls are in place to restrict the ability to enter and retrieve data to authorized personnel. Coast Guard personnel receive annual Privacy Act training so that they understand the conditions by which information may be disclosed from the system. Most disclosure of information from MISLE to persons and organizations outside the Coast Guard are performed by a highly trained staff at Coast Guard Headquarters under strict oversight.

Section 2.0 Uses of the System and the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

MISLE uses this information to support daily Coast Guard marine safety, security, environmental protection, and law enforcement operations and is analyzed to support planning and resource management. The following descriptions detail how MISLE uses information:

Notifications identify new incidents for action by field units. Notifications are communications to the Coast Guard, from external or internal sources, regarding events that will initiate Coast Guard actions.

Examples include: radio calls from boaters in distress, phone reports of pollution incidents, and written reports of marine casualties.

Activities document actions taken and information collected during those actions. Activities in MISLE include: vessel boarding, vessel inspection, facility inspection, investigation, transfer monitor, operational control, and enforcement.

Investigations document incident causes and help identify needed changes to regulations and policies. For example, information collected during investigations of vessel groundings and collisions will be analyzed to see if there are common causes, geographic trends and causal factors that can be addressed through waterway improvements or regulation. Waterway improvements would include changes to aids to navigation or dredging of channels. Regulations might require new or improved equipment (such as radar for collision avoidance), training or oversight (inspections or certifications).

Enforcement activities document actions taken against vessels, facilities, persons and organizations for violations of a law, regulation or treaty. Enforcement actions include: civil penalties, criminal prosecution and suspension or revocation actions against mariner licenses. The information collected in MISLE is used to build a case file used by prosecutors, hearing officers and judges to render a decision and impose sanctions. Criminal prosecution cases are usually transferred to the Department of Justice for prosecution.

Information is also used to produce some certificates, such as Certificates of Documentation and Certificates of Inspection. A certificate of documentation is a document issued by a country to prove that a vessel is registered with that country and entitled to fly its flag. Certificates of Documentation for U.S. flag vessels can only be generated by MISLE based on data elements entered during the vessel documentation process. Certificates of Inspection required for certain U.S. flag commercial vessels can only be generated by MISLE based on data entered into that system as a result of inspections.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

Yes. Analysis within MISLE is limited to a few reports and search lists. For instance users can search for investigations of vessel groundings within a certain area of responsibility or with a specified date range. Reports allow units to identify such things as outstanding deficiencies and operational controls issued by the unit. An outstanding deficiency is a deficiency that has been detected by the Coast Guard that has not been confirmed as being corrected. An operational control is a condition that is placed by the Coast Guard on a vessel or facility that limits its ability to operate. Operational controls on vessels include: limiting transit to daylight only, detention in port, prohibition on entry into port, and prohibiting cargo transfers. Operational controls on facilities include: prohibiting or limiting cargo operations, prohibiting docking by vessels and restricting personnel access to facility. Operational controls are issued under a variety of legal authorities, including: Captain of the Port Order, Admin Order (CERCLA), international convention (SOLAS, MARPOL) and withholding of Customs clearance.

More extensive analysis of MISLE data, such as trend analysis, is performed through the Coast Guard Business Intelligence (CGBI) system and Enterprise Geographic Information System (EGIS).

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Coast Guard personnel entering the information and their respective chain-of-command verify information for accuracy. Coast Guard analysts perform data checks at the headquarters location. For instance, using CGBI analysts will identify data that does not fit specified formats (e.g., Social Security number must have 9 digits) or using EGIS analysts will plot activity locations and identify locations that plot outside the unit area of responsibility for further investigation. The accuracy of data received from outside databases is the responsibility of the database owner. MISLE data from other databases is automatically corrected as data is updated in the system from which the data is received.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Coast Guard has identified information required in order to effectively conduct operations. The information collected is used solely to meet U.S. Coast Guard statutory requirements. Technical security and access measures are in place to ensure that users have approved access and are using information in an appropriate manner. These are discussed in Sections 7 and 8 of this PIA. The accuracy of data received from outside databases is the responsibility of the database owner. MISLE data provided from other information systems is automatically corrected as data is corrected in the system from which the data is received. MISLE data directly entered by Coast Guard personnel is corrected when errors are identified and verified during data entry reviews or after requests for correction are received in accordance with section 7.2.

Risks associated with this process include: mishandling or improper release of information by Coast Guard personnel and entering erroneous information into the system. These risks are mitigated through a combination of training, procedures and policies. Coast Guard personnel with access to MISLE are verified as requiring access for their job before being assigned an account. Those personnel are required to receive training on the proper handling of PII and other sensitive information contained in the system. Logs are maintained to track user access to the system. Social Security numbers are collected to uniquely identify individuals so that they are only provided their own record. Social Security numbers are needed to uniquely identify an individual in MISLE due to the large number of names in the system, to interface with other information systems such as financial and law enforcement databases that rely on Social Security number to uniquely identify an individual and to meet legal requirements. Legal requirements include 46 USC 12103 which requires an individual to provide their Social Security number in order to document a vessel and 31 USC 7701 which requires the collection of Social Security numbers for individuals that are assessed fines or fees. Procedures require an investigation before any requested changes are made to the system to verify the authenticity of the information to be entered.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the data in the system?

Information collected by MISLE is stored for a minimum of three years after the record is created, after which the information will be retained, archived, or destroyed in accordance with Coast Guard Commandant Instruction M5212.12A, Information and Life Cycle Management Manual, approved by the National Archives and Records Administration (NARA). Some records are permanent and are maintained indefinitely by NARA.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes. See NARA schedule N1-026-05-15.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Information within MISLE is retained to support adjudication decisions, law enforcement uses, and protection of maritime security. To support these functions, the Coast Guard has an approved retention schedule in place. Additionally, via the approved disposition and retention schedule, NARA has directed that the information be retained for as short as 3 years or as long as permanent depending on the type of information. Retention is based on a combination business need (i.e., how long do we need this information for our business process) and long term usefulness. In discussions with NARA, all data elements were made permanent because of potential long term usefulness and ability to provide in ASCII format while the retention of attachments, which can be in a variety of electronic formats, were limited by business process needs.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared?

MISLE provides data to the Maritime Awareness Global Network (MAGNet) system, Enterprise Geographic Information System (EGIS), Enterprise Data Warehouse (EDW), Coast Guard Core Accounting System (CAS), and Coast Guard Maritime Information Exchange (CGMIX). MAGNet is a secure system for classified information, up to the Secret level, that operates under the Maritime Awareness Global Network

Systems of Records Notice (DHS/USCG-061, May 15, 2008, 73 FR 28143). MAGNet managers and users are responsible for protecting the information on individuals provided to that system. EGIS and EDW are internal Coast Guard systems. CAS is a secure financial information system. Information is provided to the public through data extracts to CGMIX, however, all PII is removed from those extracts prior to posting of the information.

4.2 For each organization, what information is shared and for what purpose?

MISLE shares data with MAGNET in order to provide consolidated Maritime Domain Awareness (MDA) information for the Coast Guard and to other law enforcement and intelligence agencies responsible for marine safety, maritime security, maritime law enforcement, and marine environmental protection. Such uses include maintaining suspect lists, enforcing U.S. and international laws dealing with items such as counter narcotics, illegal migrant activity, fisheries, boating safety, and the prevention and detection of terrorist activities.

Information is provided to EGIS and EDW for internal analysis and use. Such analysis would include trend analysis, tabulations and geographic analysis. Information is provided to CAS to initiate and track financial transactions that result from MISLE activities such as civil penalty collections and user fee payments. Non-sensitive information is provided to the public (including Federal, state, local and foreign agencies) through CGMIX to facilitate information sharing and improve public access to Coast Guard data.

4.3 How is the information transmitted or disclosed?

MISLE data is transferred as batch database copies over internal Coast Guard networks.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Privacy risks as a result of sharing data with MAGNET, EGIS, EDW, CAS, and CGMIX include: risk of system users releasing information to the public and risk of disclosure during the transfer of information between systems. Analysis indicates these risks are low. MAGNet is a classified intelligence information system. All users have at least a secret clearance and are trained and monitored to minimize the risk of releasing system information to unauthorized personnel. Because data is transferred to MAGNet over internal Coast Guard networks, the risk of disclosure during transfer is low. EGIS, EDW and CAS are internal Coast Guard systems. Data is transferred over internal networks, thereby reducing the risk of unintended disclosure. Systems containing sensitive data include user log in and password protection to ensure only users with a job requirement can access the data. No PII is included on CGMIX so there is no risk of intended disclosure for that system. Only data elements that do not contain PII are exported to CGMIX, for example fields that require selection from a pick list that does not include PII. Information included from a free from text field, such as an investigation brief, is reviewed by trained personnel prior to release.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared, what information is shared and for what purpose?

MISLE Records may be shared with the following:

The Department of Defense, specifically the Military Sealift Command and the US Navy receive vessel inspection and security information for the purpose of improving the safety of military sealift vessels and coordinating maritime rescue and/or security efforts.

The Department of Labor and state level counterparts receive information about personnel casualties on vessels or at facilities to create national and state level statistics on deaths and injuries.

The National Transportation Safety Board and state level counterparts receive information about safety investigations and inspections in order to carry out their statutory duties of overseeing transportation safety, but specific to this instance, maritime transportation safety.

The International Maritime Organization, non-governmental organizations, foreign governments and similar organizations receive information in order to conduct joint investigations, operations, and inspections of facilities and vessels and ensure compliance with international treaties.

State numbering and titling officials receive information on vessels and their owners to prevent duplicate registrations, identify vessel ownership and track changes in vessel ownership and registration.

The following MISLE records may be shared with the public to provide information on vessels, facilities, and organizations:

Port State Information Exchange (PSIX) web site: Vessel Name, Identification number, flag, call sign, type, dimensions, tonnage, Coast Guard issued document status, and summary of Coast Guard contacts (i.e. boardings, inspections, investigations, etc.).

Coast Guard Maritime Information Exchange (CGMIX): List of Coast Guard Approved Equipment, List of Coast Guard Accepted Laboratories, List of Coast Guard Approved Liferaft Servicing Facilities, List of MARPOL reception facilities.

CGMIX: Incident Investigation Reports for vessel and personnel casualties (sanitized to remove personal information and any other sensitive information).

Marine Casualty and Pollution Database: database of information on marine casualties and pollution incidents with sensitive information removed. Provided on CD ROM and distributed by NTIS.

Merchant Vessels of the United States: information on documented vessels and their owners required to be published by 46 USC 12119. Provided on CD ROM and distributed by NTIS.

5.2 How is the information transmitted or disclosed?

Information is transmitted by a variety of means depending on the nature of the data and recipient. Some data is transferred via other information systems, including MAGNet, Homeport (the Coast Guard's Internet portal), VIS (vessel registration data) and CGMIX (non sensitive data provided to the public, all PII removed). MISLE information is transferred to those systems electronically via secure internal networks. Other means of transferring data include extracts on CD-ROM, email attachments and paper printouts. When sensitive information is transmitted via CD-ROM, the information is encrypted and the disk is marked to indicate handling requirements (for example: For Official Use Only). When sensitive information is transmitted via paper documents, they are marked to indicate handling requirements (for example: stamped For Official Use Only) and delivered by a method approved for that type of material (courier, certified mail, etc.).

5.3 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

A Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) is established with any external organization with whom sensitive information (including PII) is shared. The agreements identify the information to be shared, requirements for protecting the information and restrictions on further transmission of the information.

5.4 How is the shared information secured by the recipient?

Recipients are required to secure the data in accordance with the handling requirements, mentioned in 5.3, set by law, regulation, and policy. The requirements for securing data may be included in an MOU or MOA with the recipient.

5.5 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

At a minimum, users from other agencies must be trained on the specified handling requirements set by law, regulation or policy. Additional requirements may be established by the system or agency distributing the information.

5.6 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The primary risks identified with data sharing are as follows: releasing the wrong information, release during transmission, and release by recipient. These risks were minimized by: only releasing the information required by the recipient and removing sensitive information when possible; providing training to Coast Guard personnel to recognize sensitive information and know how to handle it; limiting

personnel authorized to share data; establishing a review process for data that is shared; using secure networks, encryption or secure delivery methods to protect information during transfer; marking media and documents to identify the type of information they contain; establishing MOUs/MOAs with recipients that specify their responsibilities including handling requirements.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

Yes. Notice is provided via this PIA and the Marine Information for Safety and Law Enforcement Records System SORN (DHS/CG-013). In addition, each form and web site that collects information from individuals (for example: investigation statement forms and the Homeport portal which collects security plans) contains a Privacy Act notice indicating the use of the information and provides the option to not submit that information. Where information transferred to MISLE from another system, the other system is responsible for providing the Privacy Act notice to the individual.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. Privacy Act notices are provided and individuals are given the opportunity to decline to provide personal information if they do not consent to the intended uses, however failure to provide personal information may result in the individual not receiving a service, such as documentation of a vessel.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No. Individuals are notified of intended uses by the Privacy Act Notice provided when information is collected. Examples include: investigation statement forms, forms requesting documentation of a vessel, forms requesting inspection of a vessel and submission of security plans through the Homeport portal. In some cases the individual has the right to not provide information if they do not consent to the intended uses.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Privacy risks identified were: individuals not receiving a Privacy Act notice and inability to understand their consent rights. These risks were mitigated by printing Privacy Act notices on forms to ensure they are available to the individual at the time of collection, and providing Privacy Act training to Coast Guard personnel so they can explain the consent right.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

The individual should submit a written request for the information that includes their name, mailing address, Social Security number, and if applicable, their merchant mariner license or document number, to the System Manager at the following address: Department of Homeland Security, United States Coast Guard, Commandant (CG-385), 2100 2ND Street, SW, Washington, DC 20593-0001. Social Security numbers are needed to uniquely identify an individual's records in MISLE the large number of names in the system, a name may not be associated in the system with their current address, and there may be more than one person with the same name at an address. Individuals should also include the name and identifying number (documentation number, state registration number, International Maritime Organization (IMO) number, etc.) of any vessel with which you have been associated and the name and address of any facility (including platforms, bridges, deep water ports, marinas, terminals, and factories) with which they have been associated. They or their legal representative must sign the request. These procedures are published in the MISLE Privacy Act Systems of Record Notice.

FOIA requests may be sent to Donald Taylor, Freedom of Information Act Request, 245 Murray Drive, Bldg 410, Washington, DC 20593.

7.2 What are the procedures for correcting erroneous information?

The individual should submit a written request that identifies the erroneous information, how they know the information is erroneous, and (if available) the correct information to the System Manager at the following address: Department of Homeland Security, United States Coast Guard, Commandant (CG-61), 2100 2nd Street SW, Washington D.C. 20593-0001. They should also include any available documentation supporting their claim that the information is erroneous.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals were notified through publication of the Systems of Record Notice in the *Federal Register*. They may also be notified by Coast Guard personnel during information collection or on request.

7.4 If no redress is provided, are alternatives available?

Individuals have the right to appeal a decision to not correct information contained in MISLE. Appeals follow the Coast Guard chain of command. A decision by the Commandant of the Coast Guard will be considered the final agency action.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

Access, correction and redress rights required by the Privacy Act have been provided for MISLE data. Because of the sensitive nature of the system, it is not practical to provide individuals direct access to their records in the system. Therefore we rely on individual requests and have Coast Guard personnel extract their records from the system for review. Based on the individual's review of their records we allow redress and correction of erroneous information in MISLE.

Risks associated with this process include: mishandling or improper release of information by Coast Guard personnel and entering erroneous information into the system. These risks are mitigated through a combination of training, procedures and policies. Coast Guard personnel with access to MISLE are verified as requiring access for their job before being assigned an account. Those personnel are required to receive training on the proper handling of PII and other sensitive information contained in the system. Logs are maintained to track user access to the system. Social Security numbers are collected to uniquely identify individuals so that they are only provided their own record. Procedures require an investigation before any requested changes are made to the system to verify the authenticity of the information to be entered.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

Authorized and vetted users, managers, systems administrators, and developers all have access. Users are authorized through the MISLE account creation process. During that process a user requests an account, their need for access is investigated and verified by the command to which they are assigned, then

a MISLE account is created and a password is assigned. Access levels are driven by need to know, eligibility, and suitability.

8.2 Will contractors to DHS have access to the system?

Yes. The Privacy Act, 5 U.S.C § 552a (m) (1) states that contractors maintaining a system of record on behalf of a Government agency shall be considered employees of that agency.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Privileges are determined both by user role and the unit to which the user is assigned. User privileges cannot exceed the privileges assigned to the unit.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The MISLE Login and Unit Management User Guide establishes the policy used by approvers to ensure only those persons who should have access to the system are approved.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Applications for access are reviewed and approved or disapproved by Coast Guard personnel at the unit to which the user is assigned. Applications are submitted electronically and include: user name, email address, assigned unit. Assigned unit personnel determine the appropriate role for the user. All approvals are logged for audit purposes.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Audits are conducted annually to validate access. Users who do not access the system for 90 days are automatically deactivated. The system logs data access for review, audit, and/or disciplinary action.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All Coast Guard Personnel accessing MISLE are required to have periodic training in the use of Sensitive but Unclassified information in addition to basic system operation instruction. CG general mandated Privacy Awareness training is required annually and provided to Coast Guard personnel who access the system.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Final C&A with Authority to Operate was signed on August 17, 2009 and expires August 17, 2012.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Access is restricted to specific users based on their profile and job requirements so that they only will have access to such information that they are allowed to access. All access is logged for security purposes.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Was the system built from the ground up or purchased and installed?

MISLE was built using a combination of commercial off-the-shelf software and government design software.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

MISLE Servers are built to DHS and USCG guidelines. A FIPS-199 analysis was completed in February 2006 and a full authority to operate was granted in August 2006. This system completed a FIPS-199 analysis to ensure the categorization of the system is accurately and appropriately labeled and secured. Security and privacy requirements were derived based on the sensitivity category of the system, which is considered to be HIGH sensitivity. The high baseline requirements reflect that stringent controls are necessary for protecting the confidentiality, integrity, and availability of the data in this system. The system is designed to support the high baseline requirements and protects the integrity and privacy of personal information.

9.3 What design choices were made to enhance privacy?

User accounts, access restrictions, and encryption of data transmissions were built in to ensure data integrity, privacy, and security.

Responsible Officials

Project Manager, Commandant (CG-635)
U.S. Coast Guard
2100 2nd Street SW, Washington, DC
20593-0001

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security