Privacy Impact Assessment
for the

Merchant Mariner Licensing and Documentation System

DHS/USCG/PIA-015

March 1, 2011

Contact Point
Gary Chappell
MMLD Project Officer
U.S. Coast Guard
CG-633
(202) 372-1293

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

Abstract

The United States Coast Guard (USCG) owns and operates the Merchant Mariner Licensing and Documentation (MMLD) System. The USCG uses MMLD to manage the issuance of credentials to Merchant Mariners and process merchant mariner applications; to produce merchant mariner credentials; to track the who of merchant mariner credentials issued by the Coast Guard; to track the status of merchant mariners with respect to service, training, credentials, and qualifications, related to the operation of commercial vessels; to qualify merchant mariners for benefits and services administered by other agencies; and to perform merchant mariner call-ups related to national security. The records include the credential, background check, and medical status on each U.S. Mariner and World War II Merchant Mariner Veteran. USCG has conducted this privacy impact assessment (PIA) because MMLD collects and uses personally identifiable information (PII).

Introduction

The United States Coast Guard (USCG) is responsible for issuing merchant mariner credentials (MMCs) to merchant mariners in accordance with 46 U.S.C. Part E. Merchant mariners are vessel employees that operate U.S. registered vessels. Any U.S. citizen may apply for a mariner license and any legal U.S. resident may apply for a merchant mariner document. Applicants for merchant mariner credentials are screened by the USCG to ensure they do not present a safety or security risk, they are medically qualified to serve, and they have the training and experience to serve in the position for which they are applying.

The purpose of the Merchant Mariner Licensing and Documentation system is to automate the various credentialing processes, including maintaining records of U.S. merchant mariners. The records include the credentials for each U.S. mariner and World War II Merchant Mariner Veteran's Status information (DD214 program).

The mission of the MMLD is to support the Mariner Credentialing Program (MCP) in ensuring that merchant mariners are qualified in an efficient manner to perform their duties for the purpose of:

- promoting the safety of life and property at sea;
- promoting public safety;
- protecting the marine environment; and
- promoting homeland security

Merchant Mariner Credentials (MMCs) are issued to:

- Deck officers;
- Engineers;
- Pilots;

- Radio Officers on merchant vessels;
- Operators of un-inspected towing and passenger vessels;
- Staff Officers, including pursers, medical doctors, and nurses,
- Crew members for qualified ratings, such as able seamen and qualified members of the engine department; and
- Entry-level ratings, such as ordinary seaman, wiper, and steward.

Applications are received at regional exam centers located across the United States. If a position requires applicants to pass an exam, the exam would be administered at a regional exam center. Each mariner application is reviewed in three capacities: medical, security, and professional.

Medical

The medical review ensures that the mariner is fit to perform the duties for which he is applying. Certain positions require applicants to pass a physical examination and meet certain standards of physical performance. For example, a deck officer needs visual acuity and color perception sufficient to identify aids to navigation in order to operate a vessel, so those attributes would be checked during a physical exam. Applicants may seek a waiver for any medical restrictions on a profession. The medical review is conducted by a team of doctors and medical personnel employed by the U.S. Coast Guard at the National Maritime Center (NMC). The only information entered into MMLD by the medical reviewers is the determination of medical fitness and any medical limitations that will be applied to the credential. Medical information that is not entered into MMLD is maintained as paper files first at NMC and later at NARA.

Security

Each mariner application is sent to the USCG's National Maritime Center (NMC) for processing. Biographic information is collected during the application process, including photographs submitted with the application and fingerprints collected when the mariner applies for a Transportation Worker Identification Card (TWIC) and provided to the NMC by the Transportation Security Administration (TSA). At the National Maritime Center the applicant's biographic information is used to screen against terrorist watch lists and other law enforcement databases. TSA sends fingerprints to the Federal Bureau of Investigation (FBI) for a related law enforcement check in National Crime Information Center (NCIC) and provides the results to NMC.

NMC does not share the results or analysis of the security screening. This information is maintained in MMLD.[1] NMC will only share with USCG a determination of "approved" or "denied".

Professional

The professional review of the application ensures that the applicant has met the required professional certifications to perform a job. For example, an applicant to be a medical officer aboard a

[1] Please see the Merchant Seaman Records System of Records Notice (June 25, 2009,74 FR 30308 at www.dhs.gov/privacy for additional information)

vessel must be an accredited doctor and provide documentation proving that fact. Such professional certifications are validated by personnel at the NMC.

It is important to note that MMLD only collects and stores the medical, security, and professional evaluation information required to process the specific credential requested. MMLD may not have the same information on all mariners because each credential has different requirements. MMLD is a processing system designed to facilitate transfer of applications to the experts (medical, security, professional) responsible for making final suitability determinations.

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 collected, used, disseminated, or maintained in the system?

The information that is collected, used, disseminated and maintained in MMLD consists of the following:

- Full name (including maiden name, if applicable);
- MMLD identification number;
- Medical limitations;
- Mailing address;
- Date and place of birth;
- Phone number(s), include home and work;
- Email Address;
- Next of kin's Name, mailing address, phone number and email address;
- Country of citizenship;
- Social Security number;
- Physical Characteristics (including color of eyes, hair, weight and height);
- Type of credential for which the individual is applying or was issued;
- Credential issue and expiration date;
- Shipping articles (including Information on ships and documented lengths of sea duty);
- Seaman's sea service records;
- Seaman's biometrics including photographs and fingerprint records;
- Safety records (findings and working notes of latest Safety and Suitability evaluations are maintained in MMLD);
- Current state of application, including granted or denied with place and date of issuance;
- Information related to narcotics, driving while under the influence, and conviction records; and
- Character references, including full names, addresses, and telephone numbers.

1.2 What are the sources of the information in the system?

Information is primarily collected from the mariner applying for the credentials. Additional information is provided by shipping companies, schools, and physicians. Information is also obtained from various commercial, federal and state databases to include but not limited to; commercial data providers, such as Accurint,[2] states' Department of Motor Vehicles, Marine Information for Safety and Law Enforcement (MISLE), and NCIC.

Although MMLD obtains information from Accurint it is important to note that the actual results are not retained in MMLD. Accurint results are used to verify the accuracy of MMLD information. If Accurint indicates the information is incorrect, further investigation is conducted and the information is corrected in MMLD, if appropriate.

1.3 Why is the information being collected, used, disseminated, or maintained?

MMLD is the system of record for administering the Mariner Credentialing Program (MCP) to certify domestic and international qualifications for the issuance of Merchant Mariner Credentials (MMCs) to professional U.S. mariners. The information is required to verify that the mariner applicant has the requisite general knowledge and skill to hold the credential issued and is of sound health as required by 46 U.S.C. § 4701, is a U.S. citizen as required by 46 U.S.C. § 4702 and 46 U.S.C. § 7304, and does not present a threat to vessel safety or security. Mailing addresses, email addresses, and phone numbers are collected to contact the mariner concerning licensing issues and for the purpose of call-ups related to national security. Date of birth and SSN are required to check the National Driver Register (NDR) per 46 U.S.C. § 7302.

1.4 How is the information collected?

Information is collected from the mariner applying for the credential on the application form number CG-719B (OMB control number 1625-0040), through supporting documents submitted with, following the evaluation of, the application. Supporting documents may include sea service records, course completion records, and medical records. In addition to information collected directly from the individual, the USCG may collect the following:

- Shipping articles and sea service records provided by shipping companies;
- Medical Review Officer (MRO) provide drug test results, and
- Medical records collected from physicians.

Information is obtained directly from the following databases: MISLE, NCIC, and National Driver Register. MISLE provides information on disciplinary actions. NCIC provides information on any criminal convictions. The National Driver Register provides information on convictions for driving while impaired by alcohol or drugs.

[2] Accurint is a commercial person locating and research database available to government and commercial customers.

1.5 How will the information be checked for accuracy?

Information submitted by mariners is verified by examiners during the application process by comparison with supporting documentation and information from other databases, including Accurint, MISLE, NCIC, and the National Driver Register. Information may also be compared against past applications and other data sources.

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

Pursuant to 46 U.S.C. § 7101, the USCG issues credentials to U.S. mariners. It also requires verification that the applicant has the requisite general knowledge and skill to hold the credential issued and is of sound health. Pursuant to 46 U.S.C. § 7102, the USCG limits issuance of credentials to operate documented vessels to U.S. citizens. Pursuant to 46 U.S.C. § 7302, the USCG issues documents to U.S. mariners only. It also allows a check of the National Driver Register, testing for the use of dangerous drugs, and a check of criminal history. Pursuant to 46 U.S.C. § 7304, the USCG requires proof of citizenship before notation of that fact on merchant mariner documents. Pursuat to 46 U.S.C. § 7319, the USCG maintains records on each merchant mariner's document issued, including the name and address of the seaman to whom issued and the next of kin of the seaman. Pursuant to 46 U.S.C. § 7502, the USCG to maintains computerized records on the issuances, denials, suspensions, and revocations of licenses, certificates of registry, merchant mariners' documents, and endorsements on those licenses, certificates, and documents. Public Law 93-579 § 7 and 31 U.S.C. § 7701 requires the USCG to obtain a social security number when an individual applies for a credential. These record keeping requirements are met by MMLD system.

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

Privacy Risks: Privacy risks include collecting more information from mariners than is needed to process credential applications.

Mitigation: Personnel tasked with processing credential applications are trained to collect and retain only supporting documents containing information pertinent to the credential. All information not needed to process the application is returned to the mariner.

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.

The information is used to administer the MMLD Program and to certify domestic and international qualifications for the issuance of credentials to professional U.S. mariners. Information in MMLD tracks

the status of merchant mariner credential applications from submission to credential issuance or denial. It also tracks credential expiration to verify whether a credential is valid. This information in turn is used to monitor processes, identify process improvements and make other program management decisions. Specifically, management uses MMLD data to determine areas for process improvements and to identify the need for other changes to the credential program in addition to supporting the process for evaluating applications and issuing credentials. For example, the number of requests from mariners about the status of the credential applications led management to develop the on-line mariner credential application status functionality in Homeport. MMLD information is also used to: determine whether a mariner has the citizenship, service, training, licenses, and qualifications necessary to qualify for a credential; determine whether a mariner is in sound health; determine whether a mariner presents a threat to vessel safety; determine if a mariner qualifies for benefits and services administered by other agencies; and to perform merchant mariner call-ups related to national security.

Information is checked during credential renewal every five years and more frequently if there is a change in the credential type. TSA conducts regular checks against the Terrorist Screening Database (TSDB) and other law enforcement databases as part of the issuance of a TWIC, which is required for issuance of a credential. Other checks are also performed by the Coast Guard such as against the National Driver Register.

2.2 What types of tools are used to analyze data and what type of data may be produced?

USCG uses MMLD to create reports and extracts to analyze MMLD data for management decisions and data quality control. Extracts are provided daily from MMLD to the Coast Guard Business Intelligence (CGBI) system which uses software for data analysis. Data analysis primarily involves reports of the number and type of credentials issued.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

USCG uses commercial data aggregators, such as Accurint in order to verify the accuracy of addresses and other information provided on an application. MMLD does not maintain data from commercial or publicly available data sources. If an analyst identifies inconsistent information between the commercial data provider and the applicant, NMC will research the discrepancy by contacting the applicant or someone (employer, spouse) who can verify the accuracy of the information.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

Privacy Risks: Accuracy of data contained in Accurint commercial database; possible error committed during the verification process used to ensure the accuracy of application information.

Mitigation: Data is progressively audited and verified. If application data is inconsistent with Accurint data, NMC will contact the applicant to resolve the discrepancy.

Section 3.0 Retention

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

3.1 What information is retained?

MMLD retains all information it collects. For a complete list of this information, please see Section 1.1.

3.2 How long is information retained?

Paper records related to issuance of Merchant Mariner Licenses and Documents are held on site for one year past the last activity with the file. After that time they are then transferred to the regional Federal Records Center in Suitland, MD where they are stored for up to 60 years after last discharge or evidence of death is reviewed, depending on record. See COMDTINST M5212.12A, Section II, Chapter 16, SSIC 16720 and 16721 for details. Electronic records related to issuance of Merchant Mariner Licenses and Documents will be retained in the system for 60 years pending NARA approval of the SF 115, Request for Disposition Authority.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. SF 115, Request for Disposition Authority signed by Records Officer and registered by NARA September 24, 2008. Disposition Pending.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risks: As with the retention of documents for any length of time, there lies the risk of unauthorized access or loss of documents/information.

Mitigation: By retaining documentation on site for only one year, MMLD minimizes the possibility of loss or unauthorized access, as much as possible.

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, what information is shared and for what purpose?

Information may be shared with Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), or Customs and Border Patrol (CBP) on request when required for their agency mission.

Information is shared with USCG personnel responsible for examining applications and issuing licenses and documents. It may also be shared with USCG personnel responsible for conducting marine safety investigations.

ICE, USCIS, or CBP may require MMLD data for their respective missions such as: name, address, date of birth, and Social Security number to identify individual; or information on place of birth or citizenship. Such information would be required if NMC detects a violation of laws enforced by the agency during the review of the application or related background checks.

4.2 How is the information transmitted or disclosed?

Information is shared with USCG personnel using the MMLD and MISLE information systems to registered users of those systems. If requested by ICE, CIS, or CBP, information would be transmitted either as an encrypted electronic file or hand carried paper document.

4.4 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risks: Sharing information within DHS could unintentionally result in access by unauthorized personnel.

Mitigation: Internal Information sharing with other DHS components, although necessary to perform missions, does pose a risk. The risk is mitigated as best as possible through security procedures. When sharing information internally, it is done only with authorized components and users.

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 are the information shared, what information is shared and for what purpose?

Information from the MMLD is shared with the United States Naval Reserve (USNR). Information shared includes: Credential type;issue and expiration dates;mariner number; and Issue date of Merchant Mariner Documentation. The particular information shared is only on existing Navy Reserve Officers who are in the Navy's Merchant Marine Reserve (MMR) program and have previously agreed to share this

information with the USNR. This information is intended to improve the mission readiness levels and to reduce the amount of paper reporting required by their Navy officers.

Some MMLD information is shared with the Maritime Administration (MARAD) for use in the Mariner Outreach System and national security mariner recalls.[3] Information shared includes: Mariner name, address, phone number, last 4 digits of SSN, date of birth, sea service record information, and credentials issued. MARAD presently requires the last 4 of the SSN to differentiate between mariners with the same first and last names. Presently, the MMLD number is not used because it is an internal number to MMLD that the data recipient (MARAD) is unaware of, and hence could not use.

As part of the mariner security and suitability evaluation some information is shared with the National Driver Register. Personal information shared with the National Driver Register consists of: Last Name; First Name; Middle Name; Suffix; SSN; and Date of Birth. These data elements are used to query the Registry and return data on suspended or revoked state driver's licenses or convictions of serious traffic violations such as driving while impaired by alcohol or drugs.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The USCG has a Memorandum of Understanding (MOU) with MARAD regarding the sharing of MMLD data. The agreement identifies the information to be shared, requirements for protecting the information and restrictions on further transmission of the information. The USCG has a Memorandum of Agreement (MOA) with the United States Naval Reserve regarding the sharing of MMLD data. The agreement identifies the information to be shared, requirements for protecting the information, and the restrictions on further transmission of the information.

Information is shared with the FBI and NCIC pursuant to the Merchant Seamen's Records System of Records Notice (DHS/USCG-030, June 25, 2009, 74 FR 30308). In addition, the USCG has a Memorandum of Agreement (MOA) with the FBI and the NCIC regarding the sharing of MMLD data.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information for the Naval Reserve is transmitted as an encrypted electronic file via e-mail.

[3] One mission of MARAD is to be able to recruit mariners for service on National Defense Reserve Fleet vessels to support the military in times of national emergency. On method to do this is to contact mariners (recall) for service on these vessels in times of emergency. The Marine Outreach System is a MARAD web-based application that allows mariners to update their contact information to facilitate recalls. The system also makes some information from MMLD available to mariners as a reward for their participation in the system.

Information for MARAD is transmitted as an electronic file either by a secure Internet site in the Homeport Internet portal for which users must be registered. A National Highway Traffic Safety Administration secure site is used to submit requests for National Driver Register checks and to retrieve the results.

Recipients are required to secure sensitive data in accordance with the handling requirements set by law, regulation and policy. No requirements are established for securing non-sensitive information.

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

Privacy Risks: The primary risks identified with data sharing are as follows: releasing the wrong sensitive information to a recipient; failing to properly encrypt or secure information during transmission; and unauthorized release of information by recipient.

Mitigation: These risks were minimized by: only releasing the information required by the recipient and removing sensitive information when possible; providing training to USCG 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?

Yes. A System of Records Notice was published in the Federal Register (DHS/USCG 030) for MMLD notifying the public of the information collected in that system. This PIA and the Merchant Seamen's Records System of Records Notice (DHS/USCG-030, June 25, 2009, 74 FR 30308) also provide notice.

Each form and website that collects information from individuals contains a Privacy Act notice indicating the use of the information and providing the option to not submit that information. An example of such notice is as follows:

Privacy Act Statement

In accordance with 5 U.S.C. §552a(e)(3), the following information is provided to you when supplying personal information to the Maritime Administration.

1. Authority which authorized the solicitation of the information: 46 App. USC 1295b and 1295g.

2. Principal purpose(s) for which information is intended to be used: The information is used to evaluate each applicant for an appointment to the U.S. Merchant Marine Academy.

3. The routine uses which may be made of the information: As background information on applicants for the selection process. To contact the applicant, the social security number is a basic identifier.

4. Whether or not disclosure of such information is mandatory or voluntary (required by law or optional) and the effects on the individual, if any, of not providing all or any part of the requested information: Disclosure of the information is voluntary, but the applicant will not be considered further if all information is not provided.

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.

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?

Consent is granted by signing the form providing the information collected from the individual. Examples include: Application for a Merchant Mariner Document, License or Certificate of Registry (CG-719B), Merchant Mariner Physical Examination Report (CG-719K), DOT/USCG Periodic Drug Testing Report (CG-719P), Small Vessel Sea Service Form (CG-719S), and Request Pertaining to Military Records (SF-180).

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risks: Individuals may not receive a Privacy Act notice and/or understand their right to consent.

Mitigation: These risks are mitigated by including a Privacy Act notice in a prominent place on all forms and web sites to ensure they are available and visible to the individual at the time of collection. The Privacy Act notice is written so it is easy to understand and includes the right to refuse to provide the information. Also, Privacy Act Training is provided to USCG personnel annually so they can explain the consent right. Furthermore, the system of records notice and this PIA provide extensive detail about the merchant mariner application process, information collected and how it will be used.

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-611), 2100 2nd Street, SW, Washington, DC 20593-7101. SSNs are needed to uniquely identify an individual's records in MMLD because of the large number of names in the system (their 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) and for the required Safety and Suitability checks. They should also include the name and identifying number (documentation number, state registration number, International Maritime Organization (IMO) number, etc.) of any vessel with which they have been associated. They or their legal representative must sign the request. These procedures are published in the MMLD Privacy Act Systems of Record Notice. The Secretary of Homeland Security has exempted this system from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2).

FOIA requests may be sent to Commandant (CG-611), United States Coast Guard, 2100 2nd Street SW, Washington D.C. 20593-7101, Attn: FOIA.

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-611), 2100 2nd Street SW, Washington D.C. 20593-7101. 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 USCG personnel during information collection or on request.

7.4 If no redress is provided, what alternatives are available to the individual?

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

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: Risks associated with this process include: mishandling or improper release of information by Coast Guard personnel and entering erroneous information into the system.

Mitigation: These risks are mitigated through a combination of training, procedures and policies. USCG personnel with access to MMLD 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. SSNs 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 What procedures are in place to determine which users may access the system and are they documented?

Authorized and vetted users, managers, systems administrators, and developers all have access. Users are authorized through the MMLD account creation process. During that process a user requests an account, their need for access is investigated and verified, then a MMLD account is created and a password is assigned. Access levels are driven by need to know, eligibility, and suitability.

The MMLD User Guide establishes the policy used by approvers to ensure only those persons who should have access to the system are approved.

8.2 Will Department contractors have access to the system?

Yes. Contract employees at the National Maritime Center and Regional Examination Centers require access to MMLD in the course of their duties. Contract employees at the Operations Systems Center maintain the MMLD system. 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 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All Coast Guard Personnel accessing MMLD are required to have periodic training in the use of Sensitive But Unclassified (SBU) information in addition to basic system operation instruction. Annual Privacy Act training is provided to USCG personnel who will access the system.

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.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. Final C&A with Authority to Operate was signed on February 20, 2011 and is scheduled to expire February 19, 2014.

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

Audits are conducted annually to validate access. Users must maintain a current valid USCG email address. Users who do not access the system for 60 days are automatically deactivated. The system logs data access for review, audit, and/or disciplinary action.

Requests for access are reviewed and approved or disapproved by USCG personnel that manage the MMLD system. Requests are submitted electronically and include: user name, email address, assigned unit. Users are assigned the appropriate role based on their job requirements. All approvals are logged for audit purposes.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risks: Privacy risks include potential release of personal information if unauthorized personnel access information in the MMLD database, potential release of personal information by authorized MMLD users and potential release of personal information by third parties provided access to that information

Mitigation: These risks have been mitigated through security procedures and checks. MMLD has implemented security controls appropriate for a sensitive but unclassified information system in accordance with FISMA. MMLD is only accessible via the USCG Intranet to prevent access by personnel from outside the USCG. Requests for data from organizations outside the USCG are highly scrutinized. Any information transferred to users outsite the USCG is transmitted in encrypted format to prevent accidental release. Standards for handling data by users outside the USCG are established by Memorandum of

Agreement, including a clause that prohibits transfer to other persons or organizations. Access is restricted to specific users based on their profile and job requirements so that users 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?

MMLD was built using a combination of commercial off-the-shelf software and custom designed software.

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

MMLD Servers are built to DHS and USCG guidelines. A FIPS-199 analysis was completed in 2004 and a full authority to operate was granted in December 2004. 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.

Conclusion

MMLD account and access security was evaluated in order to ensure controlled and powerful software functionality, as such; the system has various user access levels to mitigate privacy risks. USCG Security Officials follow the same policy and guidelines for approving accounts and determining access groups. The USCG has designed a system that will ensure that only those individuals with an appropriate need to know have access to the information deemed PII sensitive.

Responsible Officials

Project Manager, Commandant (CG-633)
U. S. Coast Guard
2100 2nd Street SW, STOP 7124
Washington, DC 20593-7124

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security