Privacy Impact Assessment
for the

CASE MATTER MANAGEMENT TRACKING SYSTEM

September 25, 2009

Contact Point
Mr. Donald A. Pedersen
Commandant (CG-0948)
(202) 372-3818

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

Abstract

The United States Coast Guard (USCG) developed the Case Matter Management Tracking System (CMMT) to enable attorneys, support personnel and their supervisors to effectively manage their workload. CMMT includes features to track deadlines, record all parties concerned with a matter, log important events, and record work hours. The database includes "Description" and "Case Notes" sections to record narrative information, and a "Find Case" feature to quickly locate cases related to a specific incident, field of law, or other search criteria. USCG has conducted this Privacy Impact Assessment because CMMT maintains and uses personally identifiable information (PII).

Overview

The Office of Chief Counsel in the USCG is responsible for legal services. These services include advice and legal work in practice areas such as military justice, defensive and affirmative claims, legislation, procurement, legal assistance, regulations, law enforcement, as well as other types of legal assistance. The personnel using CMMT are referred to as the Legal Program in this document.

The Case Matter Management Tracking System (CMMT) was developed so attorneys, support personnel and their supervisors can effectively manage their workload. CMMT was designed to be used by approximately 300 personnel located in the Office of Chief Counsel, Coast Guard Headquarters, two Maintenance and Logistics Command legal divisions, ten District legal offices, several base legal offices, the office of Physical Disability Evaluations, and their clients. CMMT serves as a repository for all key information relating to cases and matters across all legal practice areas. CMMT is managed by the Legal Policy and Program Management (CG-0948).

CMMT functionalities for all legal practice areas include: a database to track pertinent information for all involved parties and entities (e.g., witnesses, counsel, judges, courts, experts, plaintiffs, defendants.); docketing and reminder capabilities; financial estimates and reporting for USCG-0948[1]; and integration with document management systems and/or rudimentary document assembly functionality.

Structure

CMMT contains six tabs through which users may enter or search information: Entity, Matter, Military Justice, Physical Disability, Regulations, and Claims/Litigation. Entity pertains to people and/or units within USCG. Matter refers to matters for legal assistance and general matters. Military Justice refers to issues concerning military justice such as courts martial. Physical Disability Evaluations System refers to issues concerning applications for disability benefits.[2] Claims and litigation refers to any claims for or against USCG.

Each of these tabs are a different way to view the same information. For example, a search of an entity may turn up a matter, a military justice proceeding, or a regulation, because an individual or attorney may be associated with those three matters. All users who search may see that a matter exists with a certain case number or party name; however, only individuals authorized to view files my view the file.

[1] USCG-0948 is required to estimate claim values against the USCG
[2] This module is used by other USCG divisions. It is used to process and track applications for physical disability benefits.

Legal Program personnel can access CMMT in one of two ways, a web application or as an installed application. The majority of the users use the installed application since it is faster and friendlier for bulk data entry. Reservists and users who do not have access to the Coast Guard Data Network mainly use the web application. There are a few regular CMMT users who prefer the web interface as well.

In addition, managers within the Legal Program use CMMT to compile workload information to assist with planning, budgeting and resource allocation. For local office/division managers, reports are available through a set of custom queries and reports, and an ad hoc report generator to assist in any data calls required. CMMT also records data for management analysis at Coast Guard Headquarters.

Typical Transaction

As an example of a typical transaction would be as follows:

1. A client will come into a USCG legal office requesting help in creating a will.[3] The client will be directed to fill out an intake form which will contain information necessary in entering the matter into CMMT and to give the attorney the information necessary to assist the client.
2. Either the attorney or a member of the clerical staff will use the information on the intake sheet to first verify that their will be no conflict of interest between the client and any previous clients the office has seen.
3. Assuming no conflict is found, the initial client and case data are entered into CMMT. The information entered will include the client, type of matter, when it was received, and who the responsible attorney will be. Additionally, they may enter other people involved with the matter such as a spouse, the data entry clerk, time entries for the data entry and attorney time, documents created, and matter notes.
4. After the attorney has seen the client and completed the work, the attorney or office clerical worker will return to CMMT and enter a closed date to close the matter. Additionally, they may add more time entries and notes.

CMMT is a permission-based application: a database for tracking matter information, a query tool for searching, and a simple report tool for printing and exporting data. CMMT is organized similarly to an office shared drive with varying degrees of permissions and access (read, write, create, edit, etc). Permissions to access content within CMMT are workgroup based. This means that although every USCG attorney has the CMMT application on his or her desktop, the content is only available to attorneys in the same workgroup. For example, attorneys in the seventh district, while they have CMMT, can not see information entered into CMMT by an attorney located in CG-0943.

[3] USCG attorneys often assist USCG personnel with personal legal matters such as drafting of wills, in addition to duties related directly to the mission of the USCG.

Section 1.0 Characterization of the Information

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

1.1 What information is collected, used, disseminated, or maintained in the system?

CMMT collects information on ongoing and historical legal matters. The information collected will include the type of case, status, dates, notes, calendared events and parties involved. For any individuals in the database (attorneys, clients, family members etc.), personal information including, name, rank, employee ID, type (member, dependant, civilian employee, etc.) and unit are recorded. Data is collected in a database providing a platform for consistent communication between legal staff and collaboration on key aspects of the case. The data is disseminated via a query and reporting tool to legal staff needing to provide workload statistics.

CMMT stores the complete employee roster for USCG to assist the attorneys in finding their clients names. If a spouse is at issue or a party the user is required to enter that person's name manually.

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

CMMT users enter matter based on information provided by clients. Clients can be individuals or commands seeking legal assistance. As a matter progresses, legal staff will add information such as status, concerned parties, notes, calendar events, timekeeping, and docketing as the matter progresses to completion.

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

Periodically, the legal program is required to answer data calls from outside entities on work completed or in progress with USCG. CMMT allows managers within the Legal Program who need workload information to assist with planning, budgeting and resource allocation functions to quickly provide that data. For local office/division managers, reports are available through a menu of "Custom" reports and an AD HOC report generator. CMMT also records data for management analysis at Coast Guard Headquarters.

1.4 How is the information collected?

The legal office receives information from a client pertaining to a specific legal matter. Local legal staff determines if the information received should be entered into CMMT and if further information is required from the client. As the matter progresses, entries are updated by the legal staff as needed.

1.5 How will the information be checked for accuracy?

The local legal staff creating the matters in CMMT will validate that the client requesting legal services is entitled to those services.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

10 USC § 1044(a) gives USCG the authority to provide legal assistance to employees and dependants of USCG, including for personal matters.

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

There is a risk associated with the over-collection of USCG employee information. Because CMMT duplicates the complete employee list of for USCG so that attorney's can easily open and amend ongoing case files associated with USCG employees. All USCG personnel names are present in CMMT but not all USCG personnel have ongoing legal matters. Although a risk is present, the risk is mitigated by the fact that information collected and used within CMMT is strictly limited to the information necessary to fulfill legal responsibilities to the USCG and USCG personnel. Any access risk is mitigated by the access protocols which allow only for attorneys within a certain region to access that region's cases. This means that even though attorneys can see a roster of USCG employees, they may only take action on or review employees cases relevant to their region.

Section 2.0 Uses of 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.

Managers within the Legal Program need workload information to assist with planning, budgeting, data calls from other departments, and resource allocation functions. For local office/division managers, reports are available through a menu of "Custom" Reports and an report generator. CMMT also records data for management analysis at Coast Guard Headquarters. CMMT is also used at different levels of USCG to track caseload volume and traffic.

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

CMMT has built in query and reporting tools. This tool allows all users to run queries that will analyze the current workload in any configuration needed. The data produced will be in a printed or electronic report. Data can also be exported electronically to other applications such as Microsoft Excel or

Microsoft Word. In addition, CG-0948 has procured a third party reporting tool to assist in building libraries of standard and advanced reports.

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

CMMT does not use commercial or publicly available data.

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

The use of the information is limited to Database information among the Legal Program. CMMT is not accessible by the general public. All information is used only in regard to legal matters undertaken with USCG attorneys, or the analysis of USCG attorney workloads and resources.

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?

All data elements referenced in 1.1 are retained in case files for future use. Case files are usually not held within CMMT. Physical case files are still the primary source for case information. At times an attorney may insert case file information into a CMMT entry, but that is not the common practice. The design of CMMT does not allow for uploading of case files and other documents.

3.2 How long is information retained?

Records are retained for two years after the completion of the services and then destroyed. However, physical case files will be maintained indefinitely if a future legal dispute or inquiry about the matters addressed in the file is reasonably foreseeable.

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

The schedule has been approved by USCG Records Management and USCG legal counsel. NARA has not formally approved the schedule.

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

The information is maintained for a limited period of time after the matter is closed as long as future legal dispute is not reasonably foreseeable to reduce the misuse of information.

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 organization(s) is the information shared, what information is shared and for what purpose?

CMMT is used by approximately 300 personnel located in the Office of Chief Counsel, Coast Guard Headquarters, two Maintenance and Logistics Command legal divisions, ten District legal offices, several base legal offices, the office of Physical Disability Evaluations, and their clients. If organizations outside of the legal program request statistical information for data calls from CMMT, the information is first sanitized of any personal identifiable information (PII).

4.2 How is the information transmitted or disclosed?

Information within CMMT is transmitted electronically, however only a very limited amount of information is transmittable. For example, a case number will be assigned to an attorney via CMMT. Case files and their contents are stored in paper files (see Question 3.1).

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

To counter the risk that data may be released without proper authorization, CMMT system administrators and the users of CMMT must sign and acknowledge a set of rules of behavior governing their activities. Users must also acknowledge that they have been trained and understand the security aspects of this information system. These individuals are also required to undergo periodic security awareness training that includes protection for privacy data under their control.

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 organization(s) is the information shared, what information is shared, and for what purpose?

Information is not shared with external organizations on a regular basis. Any information shared is in the form of statistical data. If legal workload statistics are needed, sanitized information is shared with external organizations. Coast Guard legal will verify the information is releasable to other organizations. The information shared would be statistical data such as the number of matters by type, such as, the number of claims generated by a natural disaster. These data calls and responses would not contain PII.

There may be circumstances where USCG is asked to provide documents from CMMT to an external organization. When a request comes in, the documents that are requested will have to be examined on a case by case basis by examining any of the applicable laws, regulations, privileges, and USCG policy. This would be a rare occurrence and the request would most likely come from either Department of Justice (DoJ) or Department of Defense (DoD) which are involved in the same or similar matter.

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.

PII is not shared outside of the Legal Program. CMMT is covered by the Legal Assistance Case Files SORN, DHS/USCG-015, 73 FR 75455 (December 11, 2008). Physical Disability Evaluation System is covered by the Physical Disability Evaluation System Files System of Records USCG-010 (December 19, 2008) 73 FR 77768, Military Personnel id covered by Military Pay and Personnel DHS/USCG-014 (December 19, 2008) 73 FR 77743, and Military Personnel Health Records DHS/USCG-011 (December 19, 2008) 73 FR 77773, and Military Justice is covered by United States Coast Guard Courts Martial Case Files DHS/USCG-008, (October 31, 2008) 73 FR 64961.

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

Information shared with DoJ or DoD will be shared via hard copy or electronic communication encrypted (email) if necessary. All PII will be safeguarded according to DHS protocols.

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

All users to CMMT must sign rules of behavior agreements, which clearly define the access rights and any consequences of inappropriate use of the system, and the information contained in the system.

The SORNs for CMMT cover any potential sharing of information that may be necessary for litigation and information.

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?

Notice to the individual is provided through this PIA, and by a posted privacy policy is displayed on login for all users. The SORNs covering this system are DHS/USCG-015 Legal Assistance Case Files, 73 FR 75455 (December 11, 2008), Physical Disability Evaluation System Files System of Records USCG-010 (December 19, 2008) 73 FR 77768, Military Pay and Personnel DHS/USCG-014 (December 19, 2008) 73 FR 77743, Military Personnel Health Records DHS/USCG-011 (December 19, 2008) 73 FR 77773, and Courts Martial Case Files DHS/USCG-008, (October 31, 2008) 73 FR 64961. The privacy policy is also included to the client on the initial correspondence from the Legal Program.

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

No. If an individual is seeking assistance from the Legal Program, they must provide personal information.

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

No. The PII information gathered by the legal staff is needed to assist the individual in their legal needs. The PII information is not used outside of the Legal Program.

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.

The risk of insufficient notice as it relates to sharing of information was identified and is mitigated through the published SORNs and this PIA that cover the functionality of the validated user. CMMT data released to external organizations is sanitized of all PII.

Section 7.0 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 that allow individuals to gain access to their information?

FOIA and Privacy Act requests may be submitted in writing via mail or overnight carrier to:

Commandant (CG-611)
2100 2nd Street, SW
Washington, DC 20593-0001
Attn: FOIA

7.2 What are the procedures for correcting inaccurate or erroneous information?

Registered users may correct any entry they made by replacing the data into the CMMT Database.

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

Individuals are notified of the procedures for correcting as stated above in section 7.2.

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

Redress is provided.

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

The access and procedural rights for Privacy Act data is stipulated in paragraph 7.1 above. Also, technical tools are provided to allow users to change information. Because of the ample measures in place, the risks associated with inaccurate information and user access are minimal.

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?

CMMT is used by approximately 300 personnel located in the Office of Chief Counsel, Coast Guard Headquarters, two Maintenance and Logistics Command legal divisions, ten District legal offices, several base legal offices, the office of Physical Disability Evaluations, and their clients. This database is used by approximately 300 personnel located in the Judge Advocate General's base offices.

User access is validated by the CMMT Administrator who telephones and/or e-mails the POC to verify the legitimacy of the user's request. The Administrator also verifies the legitimacy of the sponsoring organization requesting legal assistance.

8.2 Will Department contractors have access to the system?

Contractors will have limited access to the system for the limited purposes of the maintenance and operation of the system, which includes ensuring data integrity, correct application functionality and availability.

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

To counter the risk that the Data may be released without proper authorization, CMMT system administrators and users of CMMT must sign and acknowledge a set of rules of behavior governing their activities, and acknowledging that they have been trained and understand the security aspects of this information system. These individuals are also required to undergo periodic security awareness training that includes protection for privacy data under their control.

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

The data is secured in accordance with FISMA requirements. CMMT is up to date with all FISMA requirements and has an Authority to Operate (ATO) dated through April 18, 2010.

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

Weekly auditing of the system login logs are performed by the systems administrator. USCG employees and/or contractors that are involved in auditing and technical maintenance of CMMT are designated by the role they perform and their access to the application is audited in compliance with DHS MD 4300A.

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?

The CMMT processes and stores "For Official Use Only" and "Privacy Act-protected information," including attorney work product, privileged attorney-client information, and information that may be procurement sensitive or proprietary. According to COMDTINST M5500.13A, paragraph 1.B.9 (b), the information processed by, and stored in, the CMMT is Sensitive (Level II).

Passwords for the registered users are secured in an encrypted database table. Additionally, standard password access controls are placed on user accounts. User accounts are audited weekly to ensure inactive, idle accounts are disabled.

To counter the risk that the Data may be released without proper authorization, CMMT system administrators and users of CMMT must sign and acknowledge a set of rules of behavior governing their activities, and acknowledging that they have been trained and understand the security aspects of this information system.

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 What type of project is the program or system?

The Case Matter Management Tracking System was developed so that attorneys, support personnel and their supervisors can effectively manage their workload. CMMT includes features to track deadlines, record all parties concerned with a case, log important events and to record work hours. The database includes "Case Description" and "Case Notes" sections to record narrative information, and a "Find Case" feature to quickly locate cases related to a specific incident, field of law, or other search criteria.

9.2 What stage of development is the system in and what project development lifecycle was used?

CMMT is fully deployed to all USCG legal offices. The database is now in the maintenance phase. Enhancements, upgrades and bug fixes are applied as needed.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Data integrity, privacy and security were considered early on in the analysis and incorporated into the formally established system requirements. These requirements were traced through the development and verified/validated in the system test phase. Data integrity checks are routinely performed to validate the security measures are working.

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix A Privacy Policy

PRIVACY ACT OF 1974 DISCLOSURE AUTHORITY: Title 10, USC, Section 3013.

PRINCIPAL PURPOSE: The purpose of this form is to assist the attorney in preparing legal documents for the client, and to prepare statistical reports on legal assistance services provided during the year. The information on this form is protected by the attorney-client privilege and may be released only in accordance with law or with approval of the client.

ROUTINE USES; Information on this form will be used to provide legal advice: to prepare legal correspondence and documents for the client and to prepare statistical reports.

DISCLOSURE: Voluntary. However, nondisclosure may preclude the legal assistance desired by the client.