PRIVACY IMPACT ASSESSMENT

Case Management and Reporting System (CMRS)

Revised March 2009

Table of Contents

Section I. Introduction and Overview

I.1   Introduction

This Privacy Impact Assessment (PIA) documents the types of personal information protected under the Privacy Act and the Freedom of Information Act (FOIA) that the Case Management and Reporting System (CMRS) processes and stores. In addition, this document identifies the categories of individuals to whom this information pertains, and the system(s) controls that will be used to protect access to this information. NARA will continue to revise this PIA as appropriate.

I.2   Purpose

This PIA addresses privacy issues raised by the use of CMRS. It will also ensure that the collection and use of name-retrievable information in CMRS is in compliance with applicable laws and regulations governing personal privacy.

I.3   Terms and Definitions
The following is a list of terms used in the PIA document for CMRS.

Terms	Definitions
Beneficiary Identification and Records Locator Subsystem (BIRLS)	System created and maintained by the Department of Veterans Affairs (VA) that provides basic information about a veteran's military service and shows the location of the veteran's claim file.
Case Management and Reporting System (CMRS)	NARA system that allows for the electronic processing of requests relating to military personnel and medical records. CMRS also provides reports concerning quality, quantity, and timeliness of request processing.
CMRS Analytics	A data warehousing and business intelligence repository used by NPRC. Data is transferred daily from the CMRS operational system to the data warehouse for fast retrieval and enhanced reporting capabilities.
CMRS Change Request (CCR)	A CCR is a standardized method of suggesting a change to CMRS, telling why the change is required, and setting the priority of the change.
Case Reference Guide (CRG)	Request processing procedures created by NPRC that are accessible through CMRS.
Civilian Personnel Records (CPR) facility	CPR is one of two sites administered by the NPRC. This facility is responsible for the storage and handling of civilian personnel, medical, and payroll records of separated civilian Federal employees, USPS money orders, Treasury

CPR (continued)	Checks, IRS records, VA records, military and dependent medical records, and local agency administrative records.
Configuration Control Board (CCB)	A group of NPRC officials and contractors who make the final decisions on any proposed changes to CMRS.
Dead File	The paper record from which the electronic Official Personnel File (eOPF) was originally created. It is no longer the official record and so will be stored by the agency or at the NPRC until disposal is authorized.
Defense Personnel Records Image Retrieval System (DPRIS)	A Department of Defense, internet based software application that translates and reformats CMRS information requests into a standardized transaction request format required for processing by PERMS (see definition of PERMS below).
Dependent Medical Record	A record created by a military treatment facility that covers medical treatment for a dependent of a military service member
Electronic Official Personnel File (eOPF)	The official, scanned version of a federal civilian employee's personnel file.
Loan and Transfer	An action whereby NPRC sends a paper or electronic record back to the creating military service department or federal agency after receiving a request from the creating entity or office authorized by that entity to request/receive the actual record
Military Personnel Records (MPR) facility	MPR is one of two sites administered by the NPRC. This facility is responsible for the storage and handling of military personnel and medical records of discharged, deceased and retired members of all branches of the U.S. armed forces. In addition, MPR stores and handles military dependent medical records
Military Personnel Registry System (MPRS)	An index used to locate military personnel records retired to the NPRC. Also used to identify auxiliary records.
National Personnel Records Center (NPRC)	This center is comprised of two separate buildings: the military personnel records (MPR) facility and the civilian personnel records (CPR) facility. The National Archives and Records Administration administers the NPRC.
Official Military Personnel File (OMPF)	A history of a service member's career from entrance to departure by discharge, retirement, resignation, or death.

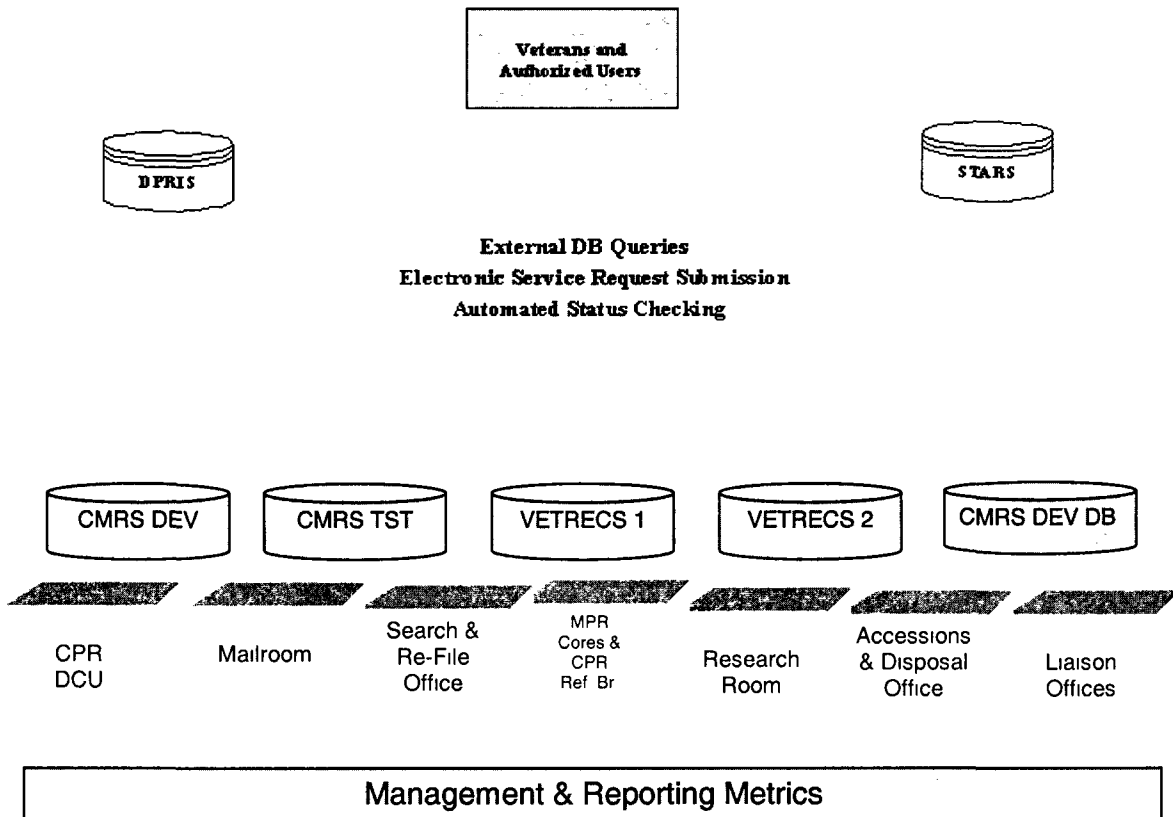| Official Personnel File (OPF)	A history of a civilian employee's federal service from the first enter-on-duty date to the final separation (via resignation, retirement, termination or death) date.
On-line Analytical Processing (OLAP)	Software application that allows for the fast analysis and presentation of multi-dimensional information.
Performance Measurement and Reporting System (PMRS)	NARA's official source for statistical information. PMRS includes all established performance measures related to the Government Performance and Results Act (GPRA) and other useful data.
Personnel Electronic Record Management System (PERMS)	Department of the Army electronic records management system that stores images of documents on both magnetic media and optical platters.
Social Security Number (SSN)	Personal identifier found in many military personnel files and federal civilian personnel files.

I.4   CMRS Overview

The Case Management and Reporting System (CMRS) is an information technology system that provides a seamless electronic information flow and an automated tool set to support the reference service mission at the Military Personnel Records (MPR) facility. In addition, CMRS supports the Loan and Transfer of Official Military Personnel Files (OMPFs) from NPRC holdings to the authorized requesting service department. CMRS also is used to track Official Personnel Files (OPFs) during the conversion process from paper to an electronic format and to display images of the scanned OPF documents on the web application when needed for immediate access. Finally, CPR services search requests created by MPR staff for copies of medical records of military members and dependents that are housed at the Civilian Personnel Records (CPR) facility. The medical record documents are scanned into CMRS and associated with the appropriate search request to make them available to the MPR technician for viewing and printing.

A central component of the CMRS support is an online case and records-tracking database. The database tracks and processes in digital form, both electronic and paper-based records inquiries from receipt through closure. All new cases are received electronically or converted to electronic images in the mailroom upon receipt. CMRS guides the cases through team and caseworker assignment. The system assists in case analysis through simple to use help aids and provides easy access to external reference databases, including digital Official Military Personnel Folders (OMPFs) maintained by the Department of Defense (DOD). CMRS aids in the retrieval and tracking of OMPFs and related medical records and provides automated templates for use in preparation of case-related correspondence. The system is equipped with robust status accounting, work metric measurements, and management reporting capabilities. These features are used to

support both web and telephone-based case status, to process customer billing, to evaluate team performance, and to plan refinements to the business processes associated with reference services.

CMRS includes two web applications. One, eVetRecs, gives veterans and their next of kin the ability to submit service requests via their personal computers and the other, eMilRecs, gives authorized Federal agencies and military departments a secure interface to easily submit service requests, check the service request status, and retrieve the responses via their personal computers. Federal agencies also use eMilRecs to track boxes of OPF folders/documents shipped to CPR for scanning. Figure 1.1 graphically depicts the current CMRS workflow process.

Veterans and
Authorized Users

DPRIS

STARS

External DB Queries
Electronic Service Request Submission
Automated Status Checking

| CMRS DEV | CMRS TST | VETRECS 1 | VETRECS 2 | CMRS DEV DB |

| CPR DCU | Mailroom | Search & Re-File Office | MPR Cores & CPR Ref Br | Research Room | Accessions & Disposal Office | Liaison Offices |

Management & Reporting Metrics

Figure 1.1 Scope of the Case Management and Reporting System

I.5   References

The following sections list the applicable laws, regulations, and NARA documentation that applies to information in CMRS.

Applicable Federal Laws and Regulations	
Computer Security Act of 1987	P.L. 100-235
Government Performance and Results Act of 1993 (GPRA)	P.L. 103-62

E-Government Act of 2002	P.L. 107-347
Freedom of Information Act	5 USC § 552, as amended
Privacy Act of 1974	5 USC § 552a

I.6   NARA Documentation

- CMRS Functional Operations Document, Version 1.0.
- NARA 35, Privacy Act notice for CMRS – See copy at Appendix A.

Section II. Data in the System

II.1   What data is in the system?

CMRS contains two general categories of information about individuals:

- Information about users of the system,
- Information scanned into the system concerning individuals who request access to Official Military Personnel Files (OMPFs) and medical records among the holdings at National Personnel Records Center (NPRC).
- Scanned images of medical records of military members and their dependents, or personnel documents from OPFs (retained in CMRS temporarily).

There are two basic categories of users:

- NARA employees, other federal employees, and employees of government contractors who use the system in the performance of their duties; and
- Any individual (veteran or 3rd party requester) who uses the system to gain information about requests submitted to the NPRC (via eVetRecs).

a.   What information will be collected from the requester or veteran?

All requesters must provide identification data, including name, address, phone number, e-mail address, and signature. The veteran or third party requester must provide information necessary to identify a specific military record. This information includes date and place of birth, branch of service, duration of military service, social security number and/or service number, specific unit(s) of assignment, military rank, and date/place of medical treatment. The requester must submit this information in writing, via mail, fax, commercial delivery service, or in person. Upon receipt at NPRC, the incoming request is scanned by authorized agency staff into CMRS where it is stored by date and the name of the employee who scanned it. This information is retained for 30 days after assignment of the request to a processing technician, or 30 days after the case is closed, whichever comes first. Paper requests are held for this period in case a re-scan is necessary. After 30 days, the paper document is destroyed.

Requester identification data and information that is required to identify a specific military record can also be submitted electronically at **https://VetRecs.archives.gov**. Electronic requests received via the web server go directly into CMRS where they are held until a signature page is received from the requester, by mail, fax, commercial

delivery service, or in person. The signature page is scanned into CMRS and the request is activated for processing. If the signature page is not received within 60 days after the electronic request is made, the request is cancelled. Once the signature page is received it is scanned into the system, where it is stored by date and scanning employee's name. The signature page is kept on file for a period of 30 days after assignment of the request to a processing technician or 30 days after the case is closed, whichever comes first. Signature pages are held for this period in case a re-scan is necessary. The paper signature page is destroyed after 30 days.

b. What information will be collected from third party requesters?

Third party requesters include individuals acting on behalf of the veteran, military dependent, Federal, state, and local government offices/personnel, representatives of the military service branches, and next-of-kin. These requesters provide contact information and information concerning the requested military record.

c. What information will be collected from employees?

NPRC employees and authorized employees of other Federal agencies provide unique login information that will establish the parameters for their use and grant them access to the data necessary to perform their duties. No other identifying information is collected on employees.

d. What information will be collected from other agency users?

Employees of the Department of Veterans Affairs, Social Security Administration, and the military service departments are to provide an assigned login id and a personal password to gain access to CMRS. No other identifying information is collected on other agency users.

II.2 What are the sources of the information in the system?

a. What NARA (NPRC) files and databases are used?

The NPRC Registry files are used to locate records. The Registry files list military personnel and medical files in the NPRC holdings, by name, service number and/or social security number. They include civilian personnel and medical files located at other locations, indexed by social security number, name and date of birth, as well as x-ray files indexed by service number or social security number. There is no direct access within CMRS to information contained in the records identified/located.

The Case Reference Guide (CRG) contains background information on military personnel and medical records and instructions on how to respond to various requests for those records. The CRG also contains instructions on how MPR should request dependent medical records from CPR.

b. What Federal Agencies are providing data for use in the system?

The Department of Veterans Affairs provides access to the Beneficiary Identification and Records Locator Subsystem (BIRLS) to assist NPRC staff in identifying veterans and locating responsive records. Information in BIRLS does not reside in CMRS nor is it accessible through an interface with CMRS. Identifying data obtained from BIRLS, such as veteran's service number or date of birth, may be entered into CMRS to assist staff in processing requests. Access to this data is only available as authorized by the system manager.

Federal civilian human resources offices of various agencies provide employee data such as names and social security numbers when they need to track OPFs sent to CPR for scanning.

c. What State and Local Agencies are providing data for use in the system?

No information in CMRS is provided by state or local agencies, except in instances where requests are received from such agencies. Similar to other requests tracked in CMRS, only contact information is entered into the system.

d. What other third party sources will data be collected from?

CMRS collects contact information and information needed to locate the appropriate military file from third party requesters. Third party sources can be any requester (e.g. friends, potential employers, news agencies, and veteran's organizations) seeking information from military records or dependent medical records on file at the NPRC.

e. What information will be collected from the veteran/employee?

Contact information and request-related information is collected directly from information provided by the veteran or the third party requester. The only information directly collected from employees of NPRC or the military service agencies is their login id and personal password. The system administrator inputs information about employees, such as their unit of assignment, phone numbers, and level of access into the system.

II.3 How will data collected from sources other than NPRC records and the veteran be verified for accuracy?

Data is accepted as accurate if it comes from a government source. If there appears to be a discrepancy in the information supplied by the veteran or information from other sources, NPRC personnel will attempt to verify the data by determining where the information in question originated. Once the origin is determined, the accuracy of the information is compared against NPRC records.

a. How will data be checked for completeness?

Contact information is determined to be complete if the NPRC is able to contact the requester at the address or e-mail provided.

Information on a specific veteran or military dependent is determined to be correct if NPRC staff is able to locate the requested OMPF or medical file.

Information on a specific civilian employee is determined to be correct if the corresponding paper OPF arrives in a shipment for scanning and/or storage.

Data provided by employees is determined to be correct if they are able to access the system.

b. Is the data current? How do you know?

Requesters provide contact information and we assume the data is current if we are able to contact them. Requesters also provide information concerning the requested OMPF or dependent medical record. If NPRC staff can locate the responsive record using the information provided, we assume the information provided is current.

II.4 Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, the data elements in CMRS are described in detail and documented in the CMRS functional operations document. A copy of the document can be provided upon request.

Section III. Access to the data

III.1 Who will have access to the data in the system?
Access to data within CMRS is granted in accordance with the permissions set by the system administrator and outlined in the functional operations document.

a. NPRC employees
NPRC employees responsible for data entry have access to information provided by the requester (e.g., name, address, phone number, e-mail and information concerning the subject of the request). Staff responsible for responding to requests has access to requester information, data used to identify responsive records, information available from the OMPF, and information used to provide responses.

b. Managers
Managers have access to input data concerning requestors as well as access to data concerning the quantity and quality of work performed by NPRC employees working under their supervision.

c. System Administrator

The system administrator has access to login and password data provided by all users. The system administrator also has access to input data concerning requesters, as well as data concerning the performance of individual employees.

d. Developers and System Contractors
Developers, including the employees of the system contractor, OPTIMOS, have access to data about system users.

e. Other agency users
Authorized members of the individual service departments have access to input data and information about the use of their records. This access includes access to incoming requests and replies. Some agency users have permission to view the system to verify services billed to the agency and for quality checks of the work being done in their name. Other agency users follow the same protocols established for NPRC staff.

f. Veterans/3rd party requesters
Requesters only have access to information concerning the status of their request. This access is granted, on line, by utilizing https://VetRecs.archives.gov.

III.2 How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

A full view of information provided by the requester is available to all users; however, individual system users have specific limited permissions, which are set by the system administrator. For NPRC employees, access to data in CMRS is limited by individual job requirements. Individual employees can only access and update requests that are assigned to them. First-line supervisors (Coach) can only access work assigned to their employees. Within their work group a coach may make or change assignments, secure statistical data and run inquiries. The system administrator has access to all data in CMRS and can make changes to system workflows, which impact the way CMRS processes requests and data.

The system administrator documents each user's current access requirements. Levels of access seldom change and most involve opening or closing accounts in the system. All requests for access or changes to access are documented by the system administrator, consistent with existing criteria and policies for access to data in CMRS.

III.3 Will users have access to all data on the system or will the users access be restricted?

Users processing requests for OMPFs and medical records only have access to the information provided by the requester, data used to identify responsive records, and information used to provide responses, such as form letters and paragraphs, case-working instructions, and references. Managers have the same access as those processing requests. They also have access to make or change assignments, secure statistical data, and run inquiries.

The system administrator and support contractors have the ability to make changes to the way the CMRS processes requests and data. No changes, however, are made without the concurrence of the Configuration Control Board (CCB). All changes made to the CMRS are documented on a CMRS Change Request (CCR). All CCRs are reviewed and discussed by the CCB. The CCR's are identified and tracked by the initials of the originator and a sequential number. The CMRS project manager tracks and controls all requests for changes to the CMRS from initiation through approval. The CMRS contractor, Optimos, works with the project manager and performs the required programming once the change is approved.

III.4 What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?

Data can be viewed by all users, but very little can be changed. Data in CMRS is only accessible using an assigned login id and password. Information provided by the requester is accessible in read-only format to all authorized CMRS users. Users can only access and act on those requests that have been assigned to them or in areas in CMRS to which they have been given permission by the system administrator.

The CCB approves the policies governing the operations of CMRS and has oversight of system administrator activities. The CCB is made up of the Director and Assistant Director of the NPRC, the CMRS project manager, the business process reengineering project manager, at least two reference core managers from MPR, a representative from CPR and a representative of the CMRS contractor, Optimos.

III.5 Do other systems share data or have access to data in this system?

CMRS Analytics is the data warehouse and business intelligence repository that stores CMRS request data for quick retrieval, reporting, and analysis by NPRC managers and supervisors. Authorized users gain access to the data in the warehouse through a web interface, controlled by a unique login id and password. No personal data about veterans or requesters is retrievable.

The Performance Measurement and Reporting System (PMRS) exports data fields/elements from CMRS relating to volume, turn-around of requests and request identification numbers, in compliance with the Government Performance and Results Act (GPRA). Only statistics are used in these interfaces. No personal data is transferred.

a. Will other agencies share data or have access to data in this system?

Specific offices/personnel of the individual military services have access to data in CMRS. Electronic access allows for faster turnaround of a high volume of requests. All Federal users gain access to CMRS through a unique login id and password. The level of access given to authorized employees of other agencies allows them to enter requests and receive information/responses to those requests. Other agencies gain access

through terminals physically located at the NPRC or by remote access facilitated by the use of a secure server.

b.   How will the data be used by the agencies? Who is responsible for assuring proper use of the data?

The data will be used by the agencies to make requests for information from the NPRC, to make replies to requests that cannot be processed by NPRC given the subject of the request or to ensure a more efficient response.

The individual service departments are Federal agencies governed by the same restrictions that apply to NPRC usage of name retrievable data. In most instances they retain legal ownership of the OMPFs physically stored at the NPRC and oversight of these records through the provisions of regulations and policy guidance governing the maintenance and use of personal information. All access is governed by password and login, and the system administrator grants access levels based on work responsibilities.

c.   How will the system ensure that agencies only get the information they are entitled to?

Agency users can only access information required to perform their duties. Access is determined by the CCB.

Section IV. Attributes of the Data

IV.1   Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes, the CMRS is designed to manage the workload of the NPRC and provide statistical reports concerning the volume of request received and the performance of individuals and teams.

IV.2   a.   Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

The system will not derive any new data or create previously unavailable data about an individual through aggregation of collected information. The medical documents that are scanned into CMRS as an attachment to a specific request will only remain in the system temporarily. Once the request is satisfied and there is no indication of a need in the near future, the medical documents are deleted.

b.   Will the new data be placed in individual's record?

Although the system will not derive new data or create previously unavailable data about an individual through aggregation, a scanned copy of the request made with attachments and a copy of the response from NPRC will be attached to the appropriate request within

CMRS. The request and responsive material are maintained in accordance with the provisions of the Privacy Act and current records disposition instructions.

   c.   Can the system make determinations about the veteran (or requesters), military dependent or employees that would not be possible without the new data?

No new determinations are made about the veteran, military dependent or third party requester.

New determinations can be made about NPRC employees relating to quality, quantity, and timeliness of work performed.

New determinations can be made about other agency users relating to the quantity of requests made against the CMRS.

   d.   How will the new data be verified for relevance and accuracy?

New data relating to employees is verified by manual reports and feedback. This data concerns quality, quantity and timeliness of work produced. No other personal information is collected.

IV.3   a.   If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

NARA does not plan any consolidation or linkage about system users with other files or systems.

NARA, through NPRC, may offer services to link files or systems for records it stores on behalf of other Federal agencies, when such services are requested by the originating agency and are made in accordance with applicable laws. If this determination is made, the data in CMRS would continue to be password protected and available to authorized personnel as required by limits set by the system administrator.

   b.   If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?

Data input personnel enter information identifying the requester and requested record into CMRS. The request and any attachments are scanned into CMRS. Data input personnel are not authorized to alter any of the data. All users enter a password and login to gain access to the system.

IV.4   How will the data be retrieved? Can it be retrieved by personal identifier?

Data in CMRS can be retrieved by name, social security number, service number, address, phone number, e-mail address, or date of birth. There is no current limit on the query function.

IV.5 What are the potential effects on the due process rights of veterans (requesters) and employees of: consolidation and linkage of files and systems; derivation of data; accelerated information processing and decision making; use of technologies?

As stated above, NARA does not plan any consolidation or linkage of data about system users with other files or systems. NARA may, however link files and/or systems for records it stores on behalf of agencies, upon the request of the agency. Such linkages may prove likely to enhance the exercise of rights by the public, particularly when an individual is requesting records that document his or her rights. For example, NARA (through the NPRC) assists veterans in obtaining benefits to which they are entitled by providing him or her with information from their OMPFs transferred to NARA from the Department or Defense, the Department of Veterans Affairs or the Social Security Administration.

The NPRC receives requests for OMPFs and related medical records at the rate of 3,500 – 4,000 per day via mail, fax, and the Internet. CMRS delivers a seamless flow of information and automated features to enhance and support the reference service mission at NPRC. This accelerated information process allows NARA to meet its performance goals for customer service and allows requestors to receive timely and more accurate responses to their requests.

a. How are the effects to be mitigated?

The primary use of the system is to track requests from veterans (or their representatives), government agencies or next of kin for information from OMPFs and other related records. Generally, the system speeds processing of requests and provides improved opportunities for accuracy. Veterans benefit from the introduction of this system through quicker responses and more accurate information. Data continues to be extracted from its original source, so the system has no impact on the reliability of that data. The reliability of CMRS data is based on the fact that the requester supplies almost all data. Statistical data concerning performance is based on the number of requests received, requests held for additional records or information, and requests completed or referred. CMRS operates within the agency's firewall, and only authorized users have access through the use of login id's and passwords. Identifying information about requesters is protected in accordance with existing privacy laws and the implementing regulations of the service agencies and NARA.

Section V. Maintenance of Administrative Controls

V.1 a. **Explain how the system and its use will ensure equitable treatment of veterans (requesters) and employees.**

Equitable treatment for veterans (requesters) is assured because the workload is easily controlled. This allows all staff to process high priority, time-sensitive requests, and requests that relate to records not held by the NPRC, as well as requests for records that must be reconstructed. Most requests are processed by the date of receipt, without regard to complexity.

Equitable treatment for employees will occur because the workload will be evenly distributed across the entire NPRC workforce, with all staff receiving both routine and complex work assignments.

b. **If the system is operated in more than one site, how will consistent use of the System and data be maintained in all sites?**

Access to CMRS is available to authorized users of other Federal agencies (the individual military service departments, the Department of Veterans Affairs, and offices of the Social Security Administration) that use CMRS to receive and process requests or data from NPRC systems. The NPRC system administrator and CCB authorize and set the parameters of individual CMRS use at remote locations. These controls are consistent with uses established for employees at NPRC. Users at remote locations gain access through a secured server.

c. **Explain any possibility of disparate treatment of individual or groups.**

Treatment of any individual or group depends on the request made and the records available to process that request. No disparate treatment is readily possible.

V.2 a. **What are the retention periods of data in the system?**

The disposition of CMRS data is scheduled under FILES 203, item 1340. Transaction data is retained for five years; data warehouse data for ten years. The electronic CMRS request and response files are kept as records of disclosure pursuant to the provisions of the Privacy Act and Department of Defense regulations until NARA becomes the legal owner of the related OMPF. Paper records associated with CMRS are kept 30 days after assignment of the request to a processing technician, or 30 days after the case is closed, whichever comes first. Scanned military and dependent medical records are "working copies" of the official records made only to facilitate efficient delivery between the two NPRC sites and, thus, are retained in CMRS temporarily. Once the request has been satisfied and it is determined that no need for the records will be required in the near future, the images are deleted from the system.

b. **What are the procedures for eliminating the data at the end of the retention period?**

The IT solution for exporting and storing the disclosure data under item 1340-2b has not been designed; therefore, no transaction data has been disposed of yet. Scanned images of the dependent medical records are deleted from CMRS by an automated routine once the request has been answered and there is no indication of a need for the records in the near future.

c.   While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Data provided by the veteran (requester) is thought to be accurate, relevant, timely, and complete unless official government records or processing guidelines prove that it is not. Protocols are in place to ensure that data relating to users is timely, accurate and complete. This information is reviewed in reports to management and employee performance appraisals.

V.3   a.   Is the system using technologies in ways that the NPRC has not previously employed?

Yes, these include scanning of request documents and attachments into an electronic format, automated workflow processes, web access to submit requests, and electronic referrals to other Federal agencies having custody of the record needed to process the request. In addition, NPRC has added the box-tracking functionality within CMRS for paper OPFs that are being converted to electronic format. Also, a dependent medical record stored at CPR is being scanned into CMRS as a temporary attachment in response to a need for the record by MPR to respond to an inquiry.

b.   How does the use of technology affect veteran (requester)/employee privacy?

Technology enhances the workflow at NPRC and allows more NARA and Federal agency staff the ability to view information that is protected by the provisions of the Privacy Act. However, we do not anticipate the use of CMRS will cause a substantial change in the privacy policy regarding requester information at NPRC. Consistent with the Privacy Act and our internal polices, the NPRC continues to make private information accessible to appropriate employees with a need to know. Employee performance privacy is still protected by the permissions granted to the user by the system administrator.

V.4   a.   Will this system provide the capability to identify, locate, and monitor individuals?

Since personal identifying information is input into the system, it provides the capability to identify and locate individuals who request access to OMPFs and related records on veterans. The work processes of NPRC and the employees of other agencies can be monitored within CMRS.

b.   Will this system provide the capability to identify, locate, and monitor groups of people?

The use of CMRS makes it possible to identify and locate groups with the same name, geographical location, date of birth, or similar branch of military service. The work processes of groups of employees (teams and cores) can be monitored.

c.   What controls will be used to prevent unauthorized monitoring?

Monitoring capabilities are limited only to supervisory and management personnel for production, planning, evaluation, and reporting purposes. Access permissions given to supervisors are controlled by system administrator and the CCB.

V.5   Under which System of Record notice does the system operate?

NARA 35, Case Management and Reporting System (CMRS). Please see attached copy.

APPENDIX A. Privacy Act System Notice for CMRS

NARA 35

System name:

Case Management and Reporting System (CMRS)

System location:

This automated system is located at the National Personnel Records Center (Military Personnel Records) in St. Louis, MO, and the National Archives and Records Administration in College Park, MD. The addresses for these locations are listed in Appendix B following the NARA Notices.

Categories of individuals covered by the system:

Individuals covered by this system include persons who request information from or access to inactive military personnel, medical, and organizational records in the physical custody of the National Personnel Records Center (Military Personnel Records). Also covered are the subjects of these inactive records.

Categories of records in the system:

CMRS files may include: correspondence, including administrative forms used for routine inquiries and replies, between NARA staff and requesters; stored copies of frequently requested documents from individual Official Military Personnel Files (OMPFs); production and response time data used for internal reporting purposes; and databases used to respond to requests. These files may contain some or all of the following information about an individual: Name, address, telephone number, position title, name of employer/institutional affiliation, identification of requested records, Social

Security Number/Service Number, previous military assignments, and other information furnished by the requester.

Authority for maintenance of the system:

44 U.S.C. 2108, 2110, and 2907

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

NARA maintains CMRS files to: Maintain control of records being requested for either internal or external use, establish employee and requester accountability for records, prepare replies to requester's reference questions, record the status of requesters' requests and NARA replies to those requests, and to facilitate the preparation of statistical and other aggregate reports on employee performance and requester satisfaction.

The routine use statements A, C, D, E, F, and G, described in Appendix A following the NARA notices, also apply to this system of records.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Electronic records.

Retrievability:

Information in CMRS files may be retrieved by the name, social security or military service number of the veteran whose record was the subject of the request. By use of a querying capability, information may also be retrieved by use of a system-assigned request number, by name and date of birth of the veteran, and by requester-supplied information, such as name and address, phone number, or email address.

Safeguards:

During business hours, electronic records are accessible to authorized NARA personnel via passwords from terminals located in attended offices. After business hours, buildings have security guards and/or secured doors, and all entrances are monitored by electronic surveillance equipment.

Retention and disposal:

The disposition of the records in the CMRS system is under consideration. Accordingly, the records generated by the system cannot be destroyed until a records schedule is approved by the Archivist. Once the disposition is determined, retention and disposal of the records will be governed in accordance with the applicable disposition instructions in the NARA records schedule contained in FILES 203, the NARA Files Maintenance and Records Disposition Manual. Individuals may request a copy of the disposition instructions from the NARA Privacy Act Officer.

System manager(s) and address:

The system manager, CMRS, is the Director, National Personnel Records Center. The address for this location is listed in Appendix B following the NARA Notices.

Notification procedure:

Individuals interested in inquiring about their records should notify the NARA Privacy Act Officer at the address given in Appendix B.

Record access procedures:

Individuals who wish to gain access to their records should submit their request in writing to the NARA Privacy Act Officer at the address given in Appendix B.

Contesting record procedures:

NARA rules for contesting the contents and appealing initial determinations are found in 36 CFR part 1202.

Record source categories:

Information in the CMRS file is obtained from requesters and from NARA employees who maintain the file.

Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy? Yes

Has a risk assessment been performed for this system? If so, and risks were identified, what controls or procedures were enacted to safeguard the information? A risk assessment has been performed on the CMRS system. A plan of action has been developed and is being executed to address vulnerabilities. Resolutions have included application of the latest Windows, UNIX, JAVA, Veritas and Oracle/Siebel software patches. Unnecessary FTP, Rexec and Telenet patches have been disabled. Passwords have been assigned to the Oracle TNS Listener accounts.

CMRS servers are not configured according to security benchmark guides found in NIST's 800-70 configuration checklist repository. Additionally, the non-public facing CMRS test, development and production servers all reside in a dedicated subnet within NARANet. Both of these risks will be addressed as a part of the CMRS Upgrade effort for which a contract is scheduled to be awarded in FY09.

Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information. NARA conducts vulnerability scans on all network devices, including the CMRS servers, on a monthly basis per a predefined schedule. A quarterly report of open vulnerabilities is compiled and analyzed. In addition, a subset of NIST 800-53 controls are tested for NARA systems on an annual basis.

Identify a point of contact for any additional questions from users regarding the security of the system.
Linda Ferro
NHV – St Louis
Email: linda.ferro@nara.gov
Phone: 314.801.0957

Conclusions and Analysis

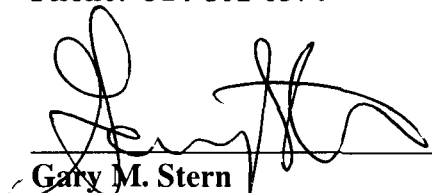**1. Did any pertinent issues arise during the drafting of this Assessment?**
No

2. If so, what changes were made to the system/application to compensate?
N/A

The Following NARA Officials Approved this Document

_____ (Signature) _$f.17.0\Upsilon$_ (Date)

RONALD L. HINDMAN, NRP
Director, National Personnel Records Center (NPRC) and
CMRS System Owner
Room 2075
Phone: 314-801-0574

_____ (Signature) _8/31/09_ (Date)

Gary M. Stern
Senior Agency Official for Privacy
8601 Adelphi Rd,
College Park, MD
Room 3110
301-837-2024

_____ (Signature) _8/21/09_ (Date)

Martha Morphy
Chief Information Officer
8601 Adelphi Rd,
College Park, MD
Room 4400
301-837-1992