Privacy Impact Assessment (PIA)

Name of Project: Case Management and Reporting System (CMRS)

Project's Unique ID: 638P

Legal Authority(ies):	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 U.S.C. § 552. as amended) Privacy Act of 1974 (5 U.S.C. § 552a) Clinger-Cohen Act of 1996 Office of Management and Budget (OMB) No. A-130 Health Insurance Portability and Accountability Act of 1996 (HIPAA) Federal Information System Management Act of 2002 (FISMA) Authority for Maintenance of the System: 44 U.S.C. 2108, 2110, and 2907**.**

Purpose of this System/Application:

CMRS uses Oracle 12c DBMS, Oracle Business Intelligence Enterprise Edition version 12.1.x, Oracle Siebel Business Applications version 8.1.x for Service Base, Sales Option, Reports, eService for Customers, Service Analytics, and Answers running on an Oracle (Solaris 10) operating system to provide 20th-century military veterans, their families, and Federal agencies the ability to request access to vital personnel service records and medical case files. These requests are processed through NARA's online record request portals: www.vetrecs.archives.gov (for the public) and www.milrecs.archives.gov (for Federal agencies). These requests are processed at NARA's National Personnel Records Center (NPRC) in St. Louis, Missouri.

This Privacy Impact Assessment (PIA) documents the types of personal information that the Case Management and Reporting System (CMRS) possesses and stores. CMRS is one application on the Integrated Siebel Platform, which has its own Privacy Impact Assessment. In addition, this document identities 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.

Section 1: Information to be Collected

1. Describe the information (data elements and fields) available in the system in the following categories:

Employees		Unique login in formation 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.
External Users		The requester or veteran name, address, phone number, e-mail address and

		signature; any information necessary to identify a specific military record. This includes date and place of birth, branch of service, duration of military service, social security number and/or service number, specific units of assignment, military rank, and date/place of medical treatment.
Audit trail information (including employee log-in information)		The CMRS System Administrator reviews and analyzes the event logs on a weekly basis for unusual patterns of activity as defined in the NARA Information System Security Officer (ISSO) Guide, v1.3 such as: 1. Users accessing system after normal business hours 2. Users performing authorized functions they do not normally perform 3. Unusual or increased activity by privileged users 4. Unexpected or unexplained changes to system security settings 5. Failed logon or resource access attempts 6. System reboots at unusual times or increases in the number of system reboots
Other (describe)		This category includes two distinct subsets of users: third party requestors and other agency users. - All third party requestors, including 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 contact information and information concerning the requested record available in the system. - Other agency users, including employees of the Department of Veterans Affairs, the Social Security Administration. These parties are required to provide an assigned login ID and personal password to gain access to CMRS. No other identifying information is collected.
Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?		
NARA operational records		NPRC registries, including the military personal registry, the civilian personnel registry, and the medical records registry, are used to locate the physical location of records maintained by NARA. The registries identify military personnel and medical files in the NPRC holdings by name, service number, and/or social security number and include civilian personnel and medical files located at the NPRC Annex in Valmeyer, IL, which are indexed by social security number. The Case Reference Guide (CRG) contains 'how to' information on military personnel and medical records. It provides instructions on how to locate records and the appropriate way to research and respond to various requests for those records. The CRG also contains instructions on how dependent and other medical records can be ordered from Valmeyer. 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, requested records' identification numbers, Social Security

		number/service number, previous military assignments, and other information furnished by the requester. CMRS files may also include the name and social security number of the subject of the Federal civilian employee personnel file.
External users		Third party sources, including any requester (e.g., friends, potential employers, news agencies, and veterans' organizations) seeking information from military records or dependent medical records on file at the NPRC/CMRS, will collect contact information and information needed to locate the appropriate military file.
Employees		The only information directly collected from employees of NPRC or the military service agencies is their login id and personal password.
Other Federal agencies (list agency)		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 respective records; BIRLS information does not reside in CMRS and is not accessible through an interface with CMRS. Data obtained from BIRLS (such as a veteran's service number or date of birth) may be entered into CMRS to assist staff in accessing requests. The 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 NPRC for scanning.
State and local agencies (list agency)		No state or local agencies provide information; this may only occur when requests are received from such agencies (and even then, only contact information is entered into the system).
Other third party source		None

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
Yes, CMRS is designed to manage the workload of the NPRC and provide statistical reports concerning the volume of requests received and the performance of individuals and teams.

2. Is there another source for the data? Explain how that source is or is not used?
CMRS is the source for data required to satisfy workload tracking and management oversight. The data is not available from other sources.

Section 3: Intended Use of this Information

1. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?
Yes, statistical and analytical data will be derived from the compiled data. This data is limited to user access and transactional values collected in CMRS. The data will be maintained completely within the CMRS database.

The documents that are scanned into CMRS as an attachment to a specific request will be kept for the entire lifecycle of CMRS.

2. Will the new data be placed in the individual's record?
Yes, CMRS will be used to accumulate performance data on NPRC employees. The performance data will be used to assist managers to complete performance ratings on employees and helps control workflow. Printouts of the data will be retained and associated with the performance rating.

For fulfilled requests, a scanned copy of the request made with attachments and a copy of the response letter from the NPRC will be attached to the appropriate request within CMRS. Correspondence is maintained in accordance with the Privacy Act and current records disposition instructions. Digitized records are maintained for access purposes, to diminish the number of times paper records must be touched.

3. Can the system make determinations about employees/the public that would not be possible without the new data?
Yes, new determinations are made about the veteran, military dependent or third party requester based on the information available in NPRC holdings. This may include entitlement to medals or other benefits.

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.

4. 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.

5. If the 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 were made, the data in CMRS would continue to be protected and available to authorized personnel as required by limits set by the system administrator.

6. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
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, although annotations can be made on by NARA staff on the related TIF files. All users enter a password and log in to gain access to the system.

7. Generally, how will the data be retrieved by the user?
Name, social security number, service number, address, phone number, e-mail address or date of birth of the veteran can retrieve data in CMRS. 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 e-mail address. There is no current limit on the query function.

8. Is the data retrievable by a personal identifier such as a name, SSN or other unique identifier? If yes, explain and list the identifiers that will be used to retrieve information on an individual.
Refer to question 7 directly above.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
The data elements in CMRS are described in detail and documented in the CMRS functional operations document.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.
Treatment of any individual or group depends on the request made and the records available to process that request.

11. Will this system be used to identify, locate, and monitor individuals? If yes, describe the business purpose for the capability and the controls established explain.
Since personal identifying information of requesters 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 system also includes information about veterans as well. The work processes of NPRC and the employees of other agencies can be monitored within CMRS. The audit logs are reviewed on a weekly basis.

12. What kinds of information are collected as a function of the monitoring of individuals?
CMRS is the source for data required to track the quantity and quality of work completed by NPRC employees. Supervisory staff and management for production, planning, evaluation and reporting purposes utilize this data.

13. 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. The system administrator and the Configuration Control Board (CCB) control access permissions given to supervisors.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
eVETRECS, the public facing CMRS web interface does not use persistent cookies or other tools to track individual web visitors.

Section 4: Sharing of Collected Information

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?
NPRC Employees: NPRC employees responsible for data entry have access to information provided by the requester. Staff responsible for responding to requests has access to the requester information, data used to identify responsive records, information available from the OMPF and information used to provide responses.

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.

System Administrator: System administrator has access to login data of all users. Passwords within

CMRS are encrypted and are not accessible to system administrators, although the administrator staff can change passwords when they are forgotten or lost by users. The system administrator also has access to input data concerning requestors as well as data concerning the performance of individual employees.

Developers and System Contractors: Developers, including the employees of the current system support contractor have access to data about system users.

Other Agency Users: Authorized employees of the military 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.

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

2. How is access to the data by a user determined and by whom? Are criteria, procedures, controls, and responsibilities regarding access documented? If so, where are they documented (e.g., concept of operations document, etc.). Are safeguards in place to terminate access to the data by the user?

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:

(1) 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.

(2) First-line supervisors (coaches) 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.

(3) The system administrator has access to all data in CMRS and can make changes to system workflows, which affect 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.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

(1) 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.

(2) Managers have the same access as those processing requests. They also have access to make or change assignments, secure statistical data, and run inquiries.

(3) The system administrator and support contractors have the ability to make changes to the way the CMRS processes requests and data. No changes are made without the concurrence of the 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 CCRs are identified and tracked by the initials of the originator and a sequential number. The CCB Secretariat tracks all requests for changes to the CMRS while the CMRS project manager tracks and them through the approval, development, testing and deployment phases. The CMRS contractor works with the project manager and performs the required programming once the change is approved.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those who have been granted access (please list processes and training materials)? How will these controls be monitored and verified?

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 requestor 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.

a. CMRS CCB Members will include representation from the following offices/organizations. Note that as CMRS expands to support other functional areas, membership will be adjusted accordingly.

b. CMRS Advisory Members will include representation from the following organizations. Again, note that as CMRS expands to support other functional areas, membership will be adjusted accordingly. Advisory members will be invited to participate at the call of the CCB Chairperson.

The CMRS implements accounts management strictly based on Need-to-Know and also reviews users' logs on a weekly basis. Furthermore, the IT Security PII Awareness and Training details appropriate use and handling of PII data.

5. Are contractors involved with the design and development of the system and will they be

involved with the maintenance of the system? **If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**
Yes - Contractors are involved with the design and development of the system and will be involved with the maintenance of the system. All contracts include Privacy Act clauses and mandates to comply with other regulatory guidelines.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared. If no, continue to question 7.
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 requestors 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.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?
Yes, CMRS Analytics is addressed under CMRS certifications and PIAs, while PMRS is addressed separately.

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?
The NARA CIO and personnel acting in the roles of Project Managers and System Owners are responsible for protecting privacy rights of the public and employees affected by the interface.

9. Will other agencies share data or have access to the data in this system (Federal, State, Local, or Other)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.
Specific offices/personnel of the individual military services have access to data in CMRS. The Personnel Information Exchange Services of the VA pulls data from the CMRS repository through secured channels (VPN) for their use in the system. 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 web interface and circuits.

Section 5: Opportunities for Individuals to Decline Providing Information

1. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?
Not applicable.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Not applicable.

Section 6: Security of Collected Information

1. How will data be verified for accuracy, timeliness, and completeness? What steps or procedures are taken to ensure the data is current? Name the document that outlines these procedures (e.g., data models, etc.).
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.

Completeness - Contact information is determined to be complete if the NPRC is able to contact the requestor 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.

Current - Requestors provide contact information and we assume the data is current if we are able to contact them. Requestors 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. The "CMRS functional operations document" outlines these procedures.

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

N/A

3. What are the retention periods of data in this system?

The disposition of CMRS data is scheduled under FILES 203, item I 340. 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 records are retained in CMRS.

4. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented? Cite the disposition instructions for records that have an approved records disposition in accordance with, FILES 203. If the records are unscheduled, that cannot be destroyed or purged until the schedule is approved.

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.

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, describe.

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, records may be scanned into CMRS in response to a request. NARA is deploying in-stacking scanning via handheld, mobile devices to accomplish this scanning.

6. How does the use of this technology affect public/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. Consistent with the Privacy Act and our internal policies, the NPRC continues to make private information accessible to appropriate employees with a need to know. Employee performance privacy is protected by the permissions granted to the user by the system administrator.

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

8. 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.

9. 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. A quarterly report of open vulnerabilities is compiled and analyzed. In addition, a subset of NIST 800-53 rev4 controls are tested for NARA systems on an annual basis.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
Questions regarding the security of this system can be addressed to Edward Graham, IT Project Manager, Edward.Graham@nara.gov, 301-837-3732.

Section 7: Is this a system of records covered by the Privacy Act?

1. Under which Privacy Act systems of records notice does the system operate. Provide number and name.
NARA 35. Privacy Act Notice for Case Management and Reporting System (CMRS)

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.
No updates to the SORN are needed.

Conclusions and Analysis

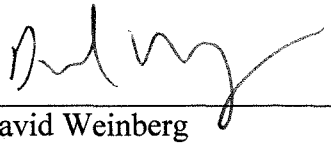
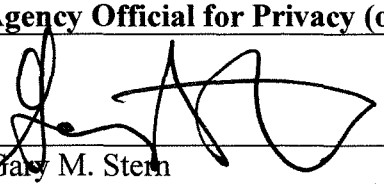
1. Did any pertinent issues arise during the drafting of this Assessment?
No

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

See Attached Approval Page

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

IT Security Manager
Privacy Act Officer

The Following Officials Have Approved this PIA	
System Manager (Project Manager)	
 (Signature)	8/7/18 (Date)
Name: David Weinberg	
Title: Director, Federal Records Center Program	
Contact information: 301-837-3115	
Senior Agency Official for Privacy (or designee)	
 (Signature)	8/1/18 (Date)
Name: Gary M. Stern	
Title: General Counsel	
Contact information: 301-837-1750	
Chief Information Officer (or designee)	
 (Signature)	8/13/18 (Date)
Name: Swarnali Haldar	
Title: Chief Information Officer	
Contact information: 301-837-1583	