NARA

Privacy Impact Assessment
for the

Case Management and Reporting System

Points of Contact and Signatures

ISSO/IT Security POC	**PIA Author** (if different from POC)
Name: Kwame Boakye Gyan Office: IS Phone: (240) 476-7424 Bldg./Room Number: A2 2300 Email: kwame.boakyegyan@nara.gov	Name: Mary Wills Office: AFN Phone: (937) 658-8369 Bldg./Room Number: 360 Email: mary.wills@nara.gov
Chief Information Officer Name: Swarnali Haldar Office: I Phone: (301) 837-1583 Bldg./Room Number: A2 4415 Email: swarnali.haldar@nara.gov Signature and date signed: SWARNALI HALDAR Digitally signed by SWARNALI HALDAR Date: 2022.04.15 07:47:10 -04'00'	**System Owner** Name: Scott Levins Office: AFN Phone: (314) 801-0587 Bldg./Room Number: NPRC Email: scott.levins@nara.gov Signature and date signed: SCOTT LEVINS Digitally signed by SCOTT LEVINS Date: 2022.04.11 10:41:24 -05'00'

Senior Agency Official for Privacy
Gary M. Stern
General Counsel
(301) 837-3026

Garym.Stern@nara.gov

Signature and date signed: GARY STERN
Digitally signed by GARY STERN
Date: 2022.04.08 08:57:09 -04'00'

Case Management and Reporting System

[This PIA should be completed in accordance with the NARA 1609. The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: This section is an overview; the questions below elicit more detail.)

CMRS allows NARA's National Personnel Records Center (NPRC) to provide our nation's veterans, their families, and Federal agencies the ability to request access to vital personnel service records and medical treatment files. These requests are received through the CMRS online record request portals: vetrecs.archives.gov (for the public) and milrecs.archives.gov (for Federal agencies). Requests are also received through traditional postal and FAX means, and all are processed at NPRC in St. Louis, Missouri.

The Case Management and Reporting System (CMRS) uses Oracle 12c RDBMS, Oracle Business Intelligence Enterprise Edition (OBIEE) version 11.1.x, Oracle Siebel Business Applications version IP 15 Patchset 18 for Service Base, Reports, eService for Customers, Service Analytics, running on an Oracle (Solaris 11) operating system to provide request management and reporting.

This Privacy Impact Assessment (PIA) documents the types of personal information that the 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 used to protect access to this information. NARA will continue to revise this PIA as appropriate.

Case Management and Reporting System

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The Case Management and Reporting System (CMRS) manages customer requests for military personnel, medical, and organizational records stored at or serviced by the National Personnel Records Center - Military Personnel Records (NPRC-MPR) in St. Louis, Missouri.
CMRS is used to:
· Maintain data regarding each request including information related to the requester and veteran;
· Locate the appropriate folder for the veteran in question through queries on several NPRC registries and the Veterans Administration (VA) Beneficiary Identification Records Locator Subsystem (BIRLS) registry.
· Create record orders for non-registry record collections;
· Identify duplicate requests and groups them for assignment to the same staff member;
· Manage efficient retrieval, tracking, and refiling of records through the use of barcodes;
· Produce any needed correspondence with the customer (response letter, forms, or other documents);
· Facilitates document shipment to the customer (mailing shipping report.)
In addition:
. CMRS is used to manage and equalize staff workload;
· Requests are assigned to staff members on resource availability and existing caseload.
. VA Scanned Records Intake and Processing - This functionality leverages records scanned and made available by the VA.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

	Authority	Citation/Reference
☑	Statute	See Page 15
☐	Executive Order	
☑	Federal Regulation	See Page 15
☐	Agreement, memorandum of understanding, or other documented arrangement	
☐	Other (summarize and provide copy of relevant portion)	

Case Management and Reporting System

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "Other" any other types of information.

	(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. NARA Employees, Contractors, and Detailees; B. External users or Individuals Outside of NARA (such as other Federal agencies); C. Members of the public	(4) Comments
	Example: Personal email address	✓	*B and C*	*Website will collect email addresses of individuals outside NARA*
1	**Name**	☑	A,B and C	System will collect name of all system users and requesters
2	**Date of birth or age**	☑	C	System will collect the date of birth of veteran
3	**Place of birth**	☑	C	System will collect the place of birth of veteran
4	**Gender**	☐		
5	**Race, ethnicity or citizenship**	☐		
6	**Religion**	☐		
7	**Social Security Number (full, last 4 digits or otherwise truncated)**	☑	C	System will collect the SSN of the veteran
8	**Tax Identification Number (TIN)**	☐		
9	**Driver's license**	☐		
10	**Alien registration number**	☐		
11	**Passport number**	☐		

Case Management and Reporting System

	(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. NARA Employees, Contractors, and Detailees; B. External users or Individuals Outside of NARA (such as other Federal agencies); C. Members of the public	(4) Comments
1	**Mother's maiden name**	☐		
2	**Vehicle identifiers**	☐		
3	**Personal mailing address**	☑	B and C	System will collect mailing address of agency users and public requesters
4	**Personal email address**	☑	A,B and C	System will collect personal email addresses of requesters; work emails of users
5	**Personal phone number**	☑	A, B and C	System will collect personal phone numbers of requesters; work emails of users
6	**Medical records number**	☐		
7	**Medical notes or other medical or health information**	☑	C	System will collect date/place of medical treatment and facility name
8	**Financial account information**	☐		
9	**Applicant information**	☐		
10	**Education records**	☐		
11	**Military status or other information**	☑	C	System will collect information necessary to identify a specific military record
12	**Employment status, history, or similar information**	☐		
13	**Employment performance ratings or other performance information, e.g., performance improvement plan**	☐		
14	**Certificates**	☐		
15	**Legal documents**	☑	C	Request attachments may contain a court order or subpoena
16	**Device identifiers, e.g., mobile devices**	☐		

Case Management and Reporting System

	(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. NARA Employees, Contractors, and Detailees; B. External users or Individuals Outside of NARA (such as other Federal agencies); C. Members of the public	(4) Comments
1	**Web uniform resource locator(s)**	☐		
2	**Foreign activities**	☐		
3	**Criminal records information, e.g., criminal history, arrests, criminal charges**	☐		
4	**Juvenile criminal records information**	☐		
5	**Whistleblower, e.g., tip, complaint or referral**	☐		
6	**Procurement/contracting records**	☐		
7	**Proprietary or business information**	☐		
8	**Location information, including continuous or intermittent location tracking capabilities**	☐		
9	***Biometric data:***			
10	**- Photographs or photographic identifiers**	☐		
11	**- Video containing biometric data**	☐		
12	**- Fingerprints**	☐		
13	**- Palm prints**	☐		
14	**- Iris image**	☐		
15	**- Dental profile**	☐		
16	**- Voice recording/signatures**	☐	C	System captures electronic signature of requester online and a signature/authorization on the request attachment.

Case Management and Reporting System

	(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. NARA Employees, Contractors, and Detailees; B. External users or Individuals Outside of NARA (such as other Federal agencies); C. Members of the public	(4) Comments
1	- **Scars, marks, tattoos**	☐		
2	- **Vascular scan, e.g., palm or finger vein biometric data**	☐		
3	- **DNA profiles**	☐		
4	- **Other (specify)**	☐		
5	***System admin/audit data:***			
6	- **User ID**	☑	A and B	System contains user ids
7	- **User passwords/codes**	☑	A and B	System contains masked passwords
8	- **IP address**	☐		
9	- **Date/time of access**	☑	A and B	System contains last login information
10	- **Queries run**	☑	A	System contains audit record of queries ran on specific fields
11	- **Content of files accessed/reviewed**	☐		
12	- **Contents of files**	☐		
13	**Other (please list the type of info and describe as completely as possible):**	☐		
14		☐		
15		☐		
16		☐		

Case Management and Reporting System

3.2 Indicate below the source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	✔	Hard copy: mail/fax	✔	Online	✔
Phone	✔	Email	✔		
Other (specify):					

Other NARA records/sources (list systems):

MPR Registry, Desert Storm/Desert Shield (DSDS); Gulf War (GW), Comprehensive Clinical Evaluation Program (CCEP), Navy/MC Microfiche Index, Army Microfiche Index and Registry Deletes, Case Reference Guide (CRG)

Other government sources of information (list agency and source):

Department of Veteran's Affairs Beneficiary Identification and Records Locator Subsystem (BIRLS)
Department of Veteran's Affairs Veterans Benefits Management System (VBMS)
Department of Veteran's Affairs Source Material Tracking System (SMTS)
Department of Defense, Defense Personnel Records Information Retrieval System (DPRIS)

Non-government sources, check any that apply:					
Members of the public	✔	Public media, Internet	✔	Private sector	✔
Commercial data brokers	✔				
Other (specify): State and Local Agencies					

Case Management and Reporting System

Section 4: Information Sharing

4.1 Indicate with whom the information will be shared and how that will occur, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer. (Check all that apply).

Recipient	How information will be shared			
	Individual users	Whole office/agency	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
Within the office that collected the information	☑	☐	☑	NPRC and select NARA employees access service request and registry data in CMRS
With other offices within NARA	☑	☐	☑	Select NARA employees access service request and registry data in CMRS
With other agencies (list agencies): VA, DoD, NBIB, FBI, NCIS, DTRA	☑	☐	☑	Milrecs users access their (or agency) requests and MPR Registry data dependent on account profile
Public	☑	☐	☐	Requesters can obtain request status information online via Vetrecs site (however, no PII).
Other (specify):	☐	☐	☐	

4.2 For non-archival information, if the information will be released to the public explain how the information will be de-identified, aggregated, or otherwise privacy protected. This question does not apply to archival information stored in a system that will undergo standard archival screening and processing in accordance with NARA 1601.

System sharing information released to the public via Vetrecs online request status check does not contain information requiring privacy protection. Documents digitally delivered are redacted as appropriate.

In accordance with Department of Defense Privacy Act requirements and NPRC business processes information will be redacted as appropriate.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain why.

CMRS and Milrecs Users: PII is not collected on NARA staff including contractors or Federal agency staff utilizing CMRS or Milrecs.

Vetrecs: A banner is displayed on the Vetrecs site that provides Privacy Act of 1974 Compliance Information. The Vetrecs site also provides a link to NARA's Privacy Policy on archives.gov.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

After Vetrecs users review the Privacy Act of 1974 Compliance Information and/or NARA's Privacy Policy they have the option to use the application to create a request or not.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Requesters cannot access information in the system pertaining to their request. Requesters can contact the NPRC Call Center at (314) 801-0800 for information on their request and ask for an amendment or correction of information provided. They can also use the online Check Status forms to provide additional information or to update items already provided. Links to the forms are available at https://www.archives.gov/personnel-records-center/forms. With the CMRS request number requesters can also check the status of a request online at vetrecs.archives.gov. System generated email notifications are sent to requesters to acknowledge receipt of their request. Digital Delivery functionality in CMRS allows for the delivery of completed response packages through a secure portal accessible by the requester. The portal does not require PII to access.

Federal Agency requesters can view their submitted request in Milrecs but are unable to edit the requests. System generated notifications are emailed to Milrecs users at a limited number of specific points during the process. Email notifications are provided on specific request types to alert the requester that their request is completed and ready for viewing.

Section 6: Maintenance of Privacy and Security Controls

6.1 NARA uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

☑	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authority to Operate (ATO):** 11/8/2018 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding Plan Of Action And Milestones (POA&M) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POA&M documentation:** As of March 2022, CMRS has a total of 16 POA&M items. 0 Critical, 2 Highs, 13 Moderate and 1 Low.
☐	**This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:**
☑	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Enterprise antivirus software and endpoint protection deploy to CMRS components.
☑	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Log Correlation Engine (LCE) and AWS CloudWatch is leveraged for logs and auditing
☑	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by NARA policy**.
☑	**Indicate whether there is additional training specific to this system, and if so, please describe:** CMRS Internal users receive annual IT Security and Privacy Awareness Training. See page 15.

Case Management and Reporting System

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

System users access the system with account profiles that are specific to that user's official job duties. Profiles are created with the views and permissions required to accomplish the user's assigned tasks. Accounts are setup with a "userid" and "password" specific to the user. Passwords expire every 90-days. CMRS can only be accessed through a NARANet connection. Audits of user accounts is performed annually. In addition, there are several processes in-place that provide staffing information to the functional administrators which helps to ensure account management when there are staff separations or reassignments involved. The IT Security and Privacy Awareness and Training course details appropriate use and handling of PII data.

Bulk and periodic data is transfered from VA to NARA using AWS S3 to S3 transfer and is encrypted using AWS KMS encryption service. NARA S3 Cloud Object Storage containing the data is a private Cloud Object and data is only accessible via CMRS system when used within AWS WorkSpaces launched in NARANet. In addition NARA S3 Cloud Object has AWS CloudWatch monitoring and alarms setup for change in Cloud Object policy.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by NARA.)

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. However, CMRS Service Requests with a created date of greater than two years are archived annually. CMRS system records are temporary records and are destroyed in accordance with the disposition instructions in the NARA Records Schedule (a supplement to the NARA Files Maintenance and Records Disposition Manual).

Case Management and Reporting System

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "Records" maintained in a "System Of Records," as defined in the Privacy Act of 1974, as amended).

☐ No. ☑ Yes.

7.2 Please cite and provide a link (if possible) to existing SORN(s) that cover the records, and/or explain if a new SORN is being published:

https://www.archives.gov/privacy/inventory/nara-35

Case Management and Reporting System

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to NARA of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

From the context of Systems Development Lifecycle, with every addition of new business functionality, a concerted effort was made to ensure only the minimum data required to accomplish the intended mission, as well as leverage existing data collected when possible without soliciting additional information from its users and customers. Both Privacy and storage impact were root concerns for this activity. Whenever possible, to continue minimizing data collection deliberate efforts were made to leverage existing datasets to derive validation information in-lieu-of soliciting new information from the customer/requester. Lastly, as discussed elsewhere in this document, appropriate notices are displayed to users and customer/requesters regarding the Privacy Rights and the option to opt out of providing PII.

In terms of security controls, an initial security assessment was conducted by NARA's independent assessors. A Security Assessment Package was prepared by the independent assessor that included a Security Assessment Report (SAR), System Security Plan (SSP), Risk Assessment Report (RAR), Plan Of Action & Milestones (POA&M), and Certifier's Recommendation. An ongoing ATO was granted for the system by the appropriate authorizing officials on 11/08/2018. An annual assessment of select security and privacy controls is conducted by NARA's independent assessors. The SAR, RAR, and POA&M are updated accordingly based on the results of the annual assessment. In addition to the annual assessment of security and privacy controls implemented on the system, the NARA IT Security Management Division (IS) and the Operations and Infrastructure Branch (IOO) have installed and monitors NARA's continuous monitoring tools deployed on the system. These tools are used to scan the system for vulnerabilities and configuration compliance and monitor for malicious activity.

Use this page for additional comments; specify which Section or page for which this is a continuation

2.2 Statutes and Federal Regulation:
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
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
Office of Management and Budget (OMB) No. A-130

Section 6.1 Indicate whether there is additional training specific to this system, and if so, please describe:
CMRS Internal users receive annual IT security and Privacy awareness training. In addition, Internal users receive specific training on various CMRS functionality and features. User Guides are also made available for all users.

Characters remaining: 5097

PRINT RESET SAVE