Privacy Impact Assessment (PIA)

Name of Project: Archival Records Center Information Systems (ARCIS)

Project's Unique ID: 6170D

Legal Authority(ies):	**44 USC 2108, 2110, and 2907**

Purpose of this System/Application:

The Archival Records Center Information System (ARCIS) is an IT system for NARA's Federal Records Centers Program (FRCP) and its customers. It is a web-based system developed by the Federal Records Centers (FRCs) to improve the way the other agencies do business with the Federal Records Centers across the country.

ARCIS automates and streamlines FRC workflow processes and includes an online portal through which NARA's customer agencies transact business with the FRC. The system also allows agencies to track transactions electronically, giving them instant access to information about their records.

ARCIS application provides two interfaces, both of which are browser based. The two types of interfaces: Customer Interface and Employee Facing Interface as described below:

• Customer Facing Interface: The Customer Portal provides a standard interactivity client for NARA customer to browse and place an online order.
• Employee Facing Interface: The Employee Portal is used to facilitate operational workflow and for application and systems administration functions.

ARCIS uses Oracle 11g DBMS, Oracle Business Intelligence Enterprise Edition version 11.1.x, Oracle Siebel Application version 15.10 for Service Base, Reports, and Service Analytics running on an Oracle (Solaris 10) operating system.

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 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.
External Users		The requester or veteran name, address, phone number, e-mail address and signature; any information necessary to identify a specific military record including Agency Record group, Agency Location, Job Title, Location, and Phone and Fax Numbers, specific units of assignment, military rank, and date/place of medical treatment.
Audit trail		The ARCIS System Administrator reviews and analyzes the event logs on a

information (including employee log-in information)		weekly basis for unusual patterns of activity 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 An extensive set of audit trails have been included in ARCIS to monitor usage by users. The core activity of ARCIS is to assist in processing FRCP business transactions. Each business transaction is processed through a number of steps from inception to completion. Movement from one step to the next is reviewed and approved by an authorized ARCIS user. ARCIS audit trails record this process including data and time and the user who has authorized the activity.
Other (describe)		Agencies must provide some uniquely identifiable information about any file being requested from the FRCs so that the proper records can be located. Each Agency identifies their records according to their own indexing scheme of their choosing. ARCIS and NARA do not dictate, evaluate, or monitor what information is in these folder identifiers, but are aware that the possibility exists that this field contains sensitive PII because when an Agency requests a file, the index or description of the file is entered into a free-form text field. Therefore, the Agency could enter PII, particularly when it is necessary to recall a file. This activity of requesting files using a description or agency defined index has been standard operating procedure for the FRCP since its inception. While this field does not expect PII, it is treated as such. ARCIS also contains copies of CMRS registry files to make it easier employees using either system to access the information. These registery files 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. Additionally, NPRC utilizes several databases of information for use with reference service objectives. The various databases are as follows: Desert Storm/Desert Shield (DSDS); Gulf War (GW), Comprehensive Clinical Evaluation Program (CCEP), Navy/MC Microfiche Index, Army Microfiche Index and Registry Deletes (MPR only). The DSDS, Navy /MC Microfiche Index and Army Microfiche Index databases were converted from Access databases to registry tables or as updates to existing tables within the Archives and Records Center Information System (ARCIS). The remaining databases, GW, CCEP and Registry Deletes exist in and are accessed through Access databases. Deleted MPR Registry record entries are also contained within ARCIS.

Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?		
NARA operational records		Federal agencies that are customers of the RCP must sign an annual agreement that obligates funds to pay for the storage and servicing of records. Data from the signed agreements is stored in the Records Center Billing System (RCPBS). An interface between RCPBS and ARCIS has been established to link this data. This data forms the basis for establishing the agency external users described in above.
External users		None
Employees		Employee data is obtained directly from the employee via a user registration form and validated from unofficial employee personnel records.
Other Federal agencies (list agency)		Other Federal Agencies use the ARCIS Customer Portal to monitor their assets stored at the FRCs and to transact business with the FRCP. While the data collected about these external users is identical to internal users, the actual information is collected and provided by the designated Administrator(s) for that Agency.
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, each data element is required. ARCIS is built on the Siebel Platform that requires each user be uniquely identified.

Data sets provided are for veteran's service and medical records. They are reviewed and deemed adequate and necessary for processing requests being fulfilled by NARA.

2. Is there another source for the data? Explain how that source is or is not used?
No

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 ARCIS. The data will be maintained completely within the ARCIS database.

2. Will the new data be placed in the individual's record?
Yes, ARCIS will be used to accumulate performance data on Federal Record Center Program (FRCP) employees. The performance data will be used to assist FRCP managers to complete performance ratings on employees. Printouts of the data will be retained and associated with the performance rating.

3. Can the system make determinations about employees/the public that would not be possible without the new data?
Yes, determinations concerning employee performance can be made using the data available in ARCIS. See item 2 above.

4. How will the new data be verified for relevance and accuracy?
The Privacy Act of 1974 requires that agencies only maintain data that is accurate, timely and complete about individuals. These requirements are statutory and apply to the collection of personal data collected and maintained in ARCIS. To ensure data in the system is verified for accuracy there will be two levels of review. Employees will be able to review data relative to themselves for accuracy. Secondly, supervisors and managers will review the data daily to ensure accuracy and timeliness.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
ARCIS has in place a set of extensive controls to prevent unauthorized access or use. These controls will adhere to NARA IT security controls. In general, only NARA managers and ARCIS System Administrators will have access to this data. Managers will only have access to employees whom they supervise. Administrators will have appropriate clearances and will be briefed on responsibility for securing data. Access will be through user login and password control that adhere to NARA standards for uniqueness. Passwords will be changed every 90 days.

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

Processes are not being consolidated.

7. **Generally, how will the data be retrieved by the user?**
Users will retrieve data from the ARCIS web portal after properly logging into the application. Users will have access only to data that has been authorized by a System Administrator, consistent with the employees' official duties. Once validated as an authorized user, users will retrieve data using pre-built queries and reports defined within the ARCIS application. In addition users will be able to query the database to request data.

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.
Yes, the data is retrievable by any of the fields listed in Section 1, Question 1 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?**
For all users, ARCIS can produce reports on system usage. This includes reports on access date and time, transactions conducted and information accessed. In addition, for NARA employees and contractors, ARCIS can produce reports on employee performance. See response to Section 3-2.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.
No

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.

Yes, users (both NARA and other Federal agency personnel) must log into ARCIS with unique user id and password. 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 ARCIS. The audit logs are reviewed on a

weekly basis.

12. What kinds of information are collected as a function of the monitoring of individuals?
Each business transaction is processed through a number of steps from inception to completion. Movement from one step to the next is reviewed and approved by an authorized ARCIS user. ARCIS audit trails record this process including data and time and the user who has authorized the activity. There is capability to monitor the work processes of RCP employees, as well as the employees of other agencies that have access ARCIS.

13. What controls will be used to prevent unauthorized monitoring?
The Siebel COTS software being used to develop ARCIS has extensive security controls built into the core functionality of the system. Furthermore, the ARCIS SSP identifies the implementation of security controls appropriate for the Moderate baseline based on the NIST 800-53 Rev 4. Only authorized system administrators and application administrators will have the authority to perform system monitoring. These individuals will have the appropriate clearances before monitoring authority is granted.

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
No

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)?
• FRCP employees who are involved in transactional flow of FRCP business lines. This includes staff who process transfers and dispositions, managers who assign work, staff who receives and dispatch new transfers of records and process reference requests.
• Contractors employed by NARA to provide system administration. ARCIS is a component of the NARA IT infrastructure. NARA uses Optimos, Inc. to provide operations and maintenance.
• Federal agency users provided access by Agency system administrators. Federal agency customers will be able to view data for their agency.

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?

Standard NARA procedures will be used prior to granting anyone access to ARCIS. User access is initiated by the completion of an access request form by the user. That form is reviewed and approved by the user's supervisor and then routed to the ARCIS Help Desk to facilitate a user's access to the system. Annually, all user accounts will be reviewed for accuracy and updated as appropriate. These procedures will be documented in the ARCIS User and Operations Manuals.

Due to the volume of external users that make use of the ARCIS Customer Portal to manage assets and due to the difficulties inherent in trying to maintain and accurate roster of those external users and their access rights, ARCIS is transitioning away from the old policy (see paragraph above), to a policy where each Agency is responsible for creating and managing their own users.

In this new policy each Agency has a Super Administrator, Administrators, and Users.

a. Super Administrators: Each Federal agency that uses the ARCIS Customer Portal must designate at least one ARCIS Super Administrator (SA). Each SA is responsible for determining and managing all of the Customer Portal users for their agency. The SA is also allowed to create special users known as Administrators.

b. Administrators: Administrators are responsible for creating ARCIS Customer Portal Users and assigning rights to those users. In some special cases, as determined by the SA, an Administrator may be able to create other Administrators and give them rights that they possess in their profiles.

c. Users: Users can only access those Agency's records stored in ARCIS according to the rights granted by their Administrators. Users can only create transactions for the management of the Agency's assets, according to the rights granted by their Administrators.

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

Access will be restricted. Agency users (FRCP customers) will only be authorized to view data for their agency (unless specifically given authority for additional access). Further, the access within agency data can be restricted to a specific group of named individuals. In addition, user rights will be restricted to modify data and the modified data will have complete audit trails. Access to user data (both Federal agency and RCP staff) will be restricted by the System Administrators and FRCP managers and limited to access necessary to perform official duties.

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?

Access to the data is restricted (as mentioned above). Audit trail functionality is included to identify any unauthorized access. User training and the ARCIS User Manual will include information advising users of the penalties for unauthorized browsing of 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, contractor personnel are involved in the design, development, testing and implementation and general support of ARCIS. Contractor personnel work for NARA. Appropriate security and privacy clauses are contained in the contract consistent with the Federal Acquisitions Regulation (FAR 1452.224-1 and FAR 52.225-01) and NARA guidance.

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.

Federal agencies that are customers of the FRCP must sign an annual agreement that obligates funds to pay for the storage and servicing of records. Data from the signed agreements is stored in the Records Center Billing System (RCPBS). An interface between RCPBS and ARCIS has been established to link this data.

7. Have the NARA systems described in item 6 received an approved Security Certification and Privacy Impact Assessment?

RCPBS has an approved Security Certification issued by NARA's CIO dated June 30, 2008. RCPBS was evaluated using the guidance in OMB-M-06-16 and determined not to contain PII data.

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The ARCIS System Owner is responsible for protecting the privacy rights of the public and employees affected by the interface. NARA's Senior Agency Official for Privacy and Chief Privacy Officer are

responsible for ensuring compliance with the privacy rights of the public and NARA employees.

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.

Yes, other agency users will have access to data in ARCIS. As outlined above, user access will be limited to data relative to their agency. Limitations on access are defined and authorized by the appropriate system administrator.

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?

All users are Federal government employees or contractors. The data that is collected is a required condition in order to be granted access to ARCIS.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Employees have visibility into their productivity and are able to review their performance metrics. They must sign logs each week indicating they are correct.

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.).

ARCIS will adhere to NARA standards for ensuring data accuracy. Annually, a review will be completed for all users to ensure that information is correct. This process will be documented in the ARCIS User and Operations Manuals.

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?
ARCIS records are currently unscheduled, and as such cannot be destroyed. The ARCIS Project Team is working with the NARA Corporate Records Management staff (CM) to finalize the records schedule. Once the disposition schedule is approved, this PIA will be updated.

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.
Disposition procedures will be contained in the ARCIS Operations Manual.

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.
No

6. How does the use of this technology affect public/employee privacy?
N/A

7. Does the system meet both NARA's IT security requirements as well as the procedures required by federal law and policy?
Yes, the ARCIS is in the O&M phase of the System Development Lifecycle. ARCIS was granted an ATO on July 13, 2009.

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?

Yes, a risk assessment has been performed on the ARCIS 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's standard Certification and Accreditation process was implemented prior to the ARCIS operational startup date of September 2008. ARCIS was granted an ATO on July 13, 2009. ARCIS is monitored using standard NARA monitoring and testing to ensure continued information security.

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 Scott Diegel, System SME, Scott.Diegel@nara.gov, 301-837-1658.

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.

Data in the system is used to accumulate performance data on FRCP employees and to assist FRCP managers in complete performance ratings on employees. Data collected for this purpose will be kept among the records in NARA 22, Employee Related Files.

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

N/A

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)	9/27/18 (Date)
Name: David Weinberg	
Title: Director, Federal Records Center Program	
Contact information: 301-837-3115	
Senior Agency Official for Privacy (or designee)	
(Signature)	9/25/18 (Date)
Name: Gary M. Stern	
Title: General Counsel	
Contact information: 301-837-1750	
Chief Information Officer (or designee)	
(Signature)	10/5/2018 (Date)
Name: Swarnali Haldar	
Title: Chief Information Officer	
Contact information: 301-837-1583	