

## **Privacy Impact Assessment**

**Name of Project:** Archives and Record Center Information System (ARCIS)

**Project's Unique ID:** 6170D

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

### **Purpose of this System/Application:**

Since the early 1950's the National Archives and Records Administration's (NARA) has operated and managed a nationwide Record Center Program (RCP) providing storage and services for records storage in 17 facilities across the country. In 1999, following the passage of P.L. 105-88 and under the direction of the Office of Management and Budget (OMB), NARA instituted a fee-for-service revolving fund which began operations on October 1, 1999, for its records centers' storage and servicing operation.

The Archives and Records Center Information System (ARCIS) will replace an outdated and costly patchwork of computer support systems with a modern integrated system. ARCIS will support streamlined business processes, thereby saving money and providing better service to our customers (Federal agencies who store records with the RCP) who expect real-time, web-enabled access to their holdings and their transaction information.

The scope of ARCIS includes the following:

- Facilitate RCP core processes under the revolving fund: holdings management, center operations and production, customer service, and integration with financial management.
- Provide the RCP with functionality to develop and provide new products and services.
- Provide solutions and means to improve current legacy system limitations.
- Achieve data standardization and integration, eliminate functional redundancy, and integrate with external entities and provider systems, as decided by NARA.
- Comply with the NARA enterprise architecture and be capable of reusing relevant functionality from other NARA applications, where available.
- Scale for future business requirements (both new and evolving), in addition to supporting added functionality and increased business transaction volumes.

### **Section 1: Information to be Collected**

**1. Describe the information (data elements and fields) available in the system in the**

**following categories:**

**a. Employees –includes NARA staff and contractors**

The entity below describes data that will be collected from NARA personnel (RCP employees) who are granted access to the application. (Note: Employees and External Users will provide the same data with a flag denoting type of user)

<b>Name</b>	<b>Description</b>	<b>Column</b>	<b>Type</b>	<b>Length</b>	<b>Required</b>	<b>Pick List</b>	<b>Entities</b>	<b>Comments</b>
Contact/Employee Id	Primary key for a Contact / Employee entity, generated by the system	ROW_ID	VARCHAR	15	Y		Contact, Employee	Primary Key
Email Address	To capture the email address for a contact or employee. This is also a unique identifier for the contact entity.	EMAIL_ADDRESS	VARCHAR	50	Y		Contact, Employee	Unique Identifier
User Id	To capture the login ID for the contact or Employee entity. This is also used when the contact chooses to login to the ARCIS customer portal	LOGIN	VARCHAR	50	N		Contact, Employee	Foreign Key User.User Id
Record Center Id	Foreign key to the Record Center entity	BU_ID	VARCHAR	15	N		Employee	Foreign Key Record Center. Record Center Id
Agency Id	Foreign key to the Agency entity	PR_DEPT_OU_ID	VARCHAR	15			Contact	Foreign Key Agency.Agency Id
Employee Flag	Flag to denote that the person is an employee	EMP_FLG	CHAR	1	Y		Contact, Employee	
Cell Phone Number	To capture the cell phone # of the employee logging into ARCIS	CELL_PHONE_NUM	VARCHAR	40	N		Employee	
Cost Per Hour	To capture the cost per hour of the employee logging into ARCIS	COST_PER_HR	NUMBER	22	N		Employee	
End Date	To capture the end date of the employee logging into ARCIS	END_DT	DATE	7	N		Employee	
Fax Phone Number	To capture the Fax phone number for a contact or employee	FAX_PHONE_NUM	VARCHAR	40	N		Contact, Employee	
First Name	To capture the first name of a contact or employee	FST_NAME	VARCHAR	50	Y		Contact, Employee	

Name	Description	Column	Type	Length	Required	Pick List	Entities	Comments
Job Title	To capture the Job Title of the employee or the contact at the associated agency	JOB_TITLE	VARCHAR	75	N		Contact, Employee	
Last Name	To capture the last name of a contact or employee	LAST_NAME	VARCHAR	50	Y		Contact, Employee	
Middle Name	To capture the middle name of a contact or employee	MID_NAME	VARCHAR	50	N		Contact, Employee	
Prefix	To capture the prefix for a contact entity used while addressing the contact	PER_TITLE	VARCHAR	15	N	PickList MrMs	Contact	
Work Phone Number	To capture the work phone number for a contact or employee	WORK_PHONE_NUM	VARCHAR	40	N		Contact, Employee	
Start Date	To capture the start date of the employee logging into ARCIS	START_DT	DATE	7	N		Employee	
Role	To capture the role of the contact entity defined for an agency.	CON_CD	VARCHAR	30	N	ARCIS Contact Role	Contact	System User, System Administrator
Type	To capture the type of contact entity defined for an agency	CSN	VARCHAR	15	Y	ARCIS Contact Type	Contact	RO, RO-CO
Alternate Contact	To capture an alternate contact person for a contact entity.	CON_ASST_NAME	VARCHAR	50	N		Contact	
Alternate Contact Phone Number	To capture an alternate contact phone # for a contact entity.	ASST_PHONE_NUM	VARCHAR	40	N		Contact	
Comments	To capture any specific details related to the contact entity.	COMMENTS	VARCHAR	255	N		Contact	
Do Not Email Flag	To capture the contact entities preference related to receiving automated emails	SUPPRESS_EMAIL_FLAG	CHAR	1	N		Contact	

**b. External Users**

The entity below describes data that will be collected from other Federal agency employees (RCP customer agencies) who are granted access to the application. (Note: Employees and External Users will provide the same data with a flag denoting type of

user)

Name	Description	Column	Type	Length	Required	Pick List	Comments
User Id	To capture a unique identifier that defines User entity	ROW_ID	VARCHAR	15	Y		Primary Key
Login Name	To capture a unique identifier that defines the Login Name of the user accessing ARCIS	LOGIN	VARCHAR	50	Y		Unique Identifier
Challenge Answer	To capture the challenge answer of the user logging into ARCIS to verify and provide a new password in case the old passport is forgotten	CHALLENGE_ANSWER	VARCHAR	100	N		
Challenge Question	To capture the challenge question of the user logging into ARCIS to verify and provide a new password in case the old passport is forgotten	CHALLENGE_QUESTION	VARCHAR	100	N		

The entity below describes data collected from an individual representing an agency (RCP customer agency) participating with the Federal Records Center program either in the present or in the past having access to the application.

Name	Description	Column	Type	Length	Required	Pick List	Entities	Comments
Contact/Employee Id	Primary key for a Contact / Employee entity, generated by the system	ROW_ID	VARCHAR	15	Y		Contact, Employee	Primary Key
Email Address	To capture the email address for a contact or employee. This is also a unique identifier for the contact entity.	EMAIL_ADDRESS	VARCHAR	50	Y		Contact, Employee	Unique Identifier
User Id	To capture the login ID for the contact or Employee entity. This is also used when the contact chooses to login to the ARCIS customer portal	LOGIN	VARCHAR	50	N		Contact, Employee	Foreign Key User.User Id
Record Center Id	Foreign key to the Record Center entity	BU_ID	VARCHAR	15	N		Employee	Foreign Key Record Center. Record Center Id
Agency Id	Foreign key to the Agency entity	PR_DEPT_OU_ID	VARCHAR	15			Contact	Foreign Key Agency.Agency Id

Name	Description	Column	Type	Length	Required	Pick List	Entities	Comments
Employee Flag	Flag to denote that the person is an employee	EMP_FLG	CHAR	1	Y		Contact, Employee	
Cell Phone Number	To capture the cell phone # of the employee logging into ARCIS	CELL_PH_NUM	VARCHAR	40	N		Employee	
Cost Per Hour	To capture the cost per hour of the employee logging into ARCIS	COST_PER_HR	NUMBER	22	N		Employee	
End Date	To capture the end date of the employee logging into ARCIS	END_DT	DATE	7	N		Employee	
Fax Phone Number	To capture the Fax phone number for a contact or employee	FAX_PH_NUM	VARCHAR	40	N		Contact, Employee	
First Name	To capture the first name of a contact or employee	FST_NAME	VARCHAR	50	Y		Contact, Employee	
Job Title	To capture the Job Title of the employee or the contact at the associated agency	JOB_TITLE	VARCHAR	75	N		Contact, Employee	
Last Name	To capture the last name of a contact or employee	LAST_NAME	VARCHAR	50	Y		Contact, Employee	
Middle Name	To capture the middle name of a contact or employee	MID_NAME	VARCHAR	50	N		Contact, Employee	
Prefix	To capture the prefix for a contact entity used while addressing the contact	PER_TITLE	VARCHAR	15	N	Pick List MrMs	Contact	
Work Phone Number	To capture the work phone number for a contact or employee	WORK_PH_NUM	VARCHAR	40	N		Contact, Employee	
Start Date	To capture the start date of the employee logging into ARCIS	START_DT	DATE	7	N		Employee	
Role	To capture the role of the contact entity defined for an agency.	CON_CD	VARCHAR	30	N	ARCIS Contact Role	Contact	System User, System Administrator
Type	To capture the type of contact entity defined for an agency	CSN	VARCHAR	15	Y	ARCIS Contact Type	Contact	RO, RC-CO
Alternate Contact	To capture an alternate contact person for a contact entity.	CON_ASST_NAME	VARCHAR	50	N		Contact	

Name	Description	Column	Type	Length	Required	Pick List	Entities	Comments
Alternate Contact Phone Number	To capture an alternate contact phone # for a contact entity.	ASST_PH_NUM	VARCHAR	40	N		Contact	
Comments	To capture any specific details related to the contact entity.	COMMENTS	VARCHAR	255	N		Contact	
Do Not Email Flag	To capture the contact entities preference related to receiving automated emails	SUPPRESS_EMAIL_FLAG	CHAR	1	N		Contact	

**c. Audit trail information (including employee log-in information)**

The entity below describes the auditing of various data elements across transactions to ensure accountability of actions performed.

Name	Description	Column	Type	Length	Required	Pick List	Comments
Audit Trail Id	Primary key for an audit trail entity, generated by the system	ROW_ID	VARCHAR	15	Y		Primary Key
User Id	Foreign Key to User entity	USER_ID	VARCHAR	15	Y		Foreign Key User.User Id
Business Component	To capture the business component that is audited	BUSCOMP_NAME	VARCHAR	75	N		
Child Business Component	To capture the child business component that is audited	CHILD_B C_NAME	VARCHAR	75	N		
Date	To capture the operation date of an action that is audited	OPERATION_DT	DATE	7	N		
Field	To capture the field name that is audited	FIELD_NAME	VARCHAR	75	N		
New Value	To capture the new value inserted in a field	NEW_VALUE	VARCHAR	50	N		
Old Value	To capture the original value in a field	OLD_VAL	CHAR	50	N		
Operation	To capture the nature of operation such as create, modify, delete, that is audited.	OPERATION_CD	VARCHAR	30	N		
Record Id	To capture the record id of the transaction being audited	RECORD_ID	VARCHAR	15	N		

**d. Other (describe)** None.

**2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources?**

**a. 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 describe in item 1.b. above.

**b. External users**

Each Federal agency that participates in ARCIS will designate an ARCIS System Administrator (SA). The SA will manage the users for that agency. Potential external users will complete a user registration form that includes the data required for external users. The SA will validate the data and then authorize access.

**c. Employees**

Employee data is obtained directly from the employee via a user registration form and validated from unofficial employee personnel records.

**d. Other Federal agencies (list agency)**

None.

**e. State and local agencies (list agency)**

None.

**f. 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 Oracle Siebel CRM application platform that requires each user be a named and unique individual. Data is collected using dynamic web content in an OLTP context. Dynamic web content is constructed by using Siebel Web Extensions to combine HTML templates with data retrieved from persistent data stores. This pattern is characterized by: (a) the use of a stateful synchronous interface to invoke the application partitions involved with data retrieval and guarantee transactional integrity; (b) the use of security services to provide the level of user authentication and authorization required by the application; and, (c) the use of an SSL connection with customer-facing clients (access for employees can be provided using NARANET). Figure 1 below illustrates this pattern.

The data that is being collected will be used to validate the user, and provide a means

for communicating to the user from the ARCIS web based portal.

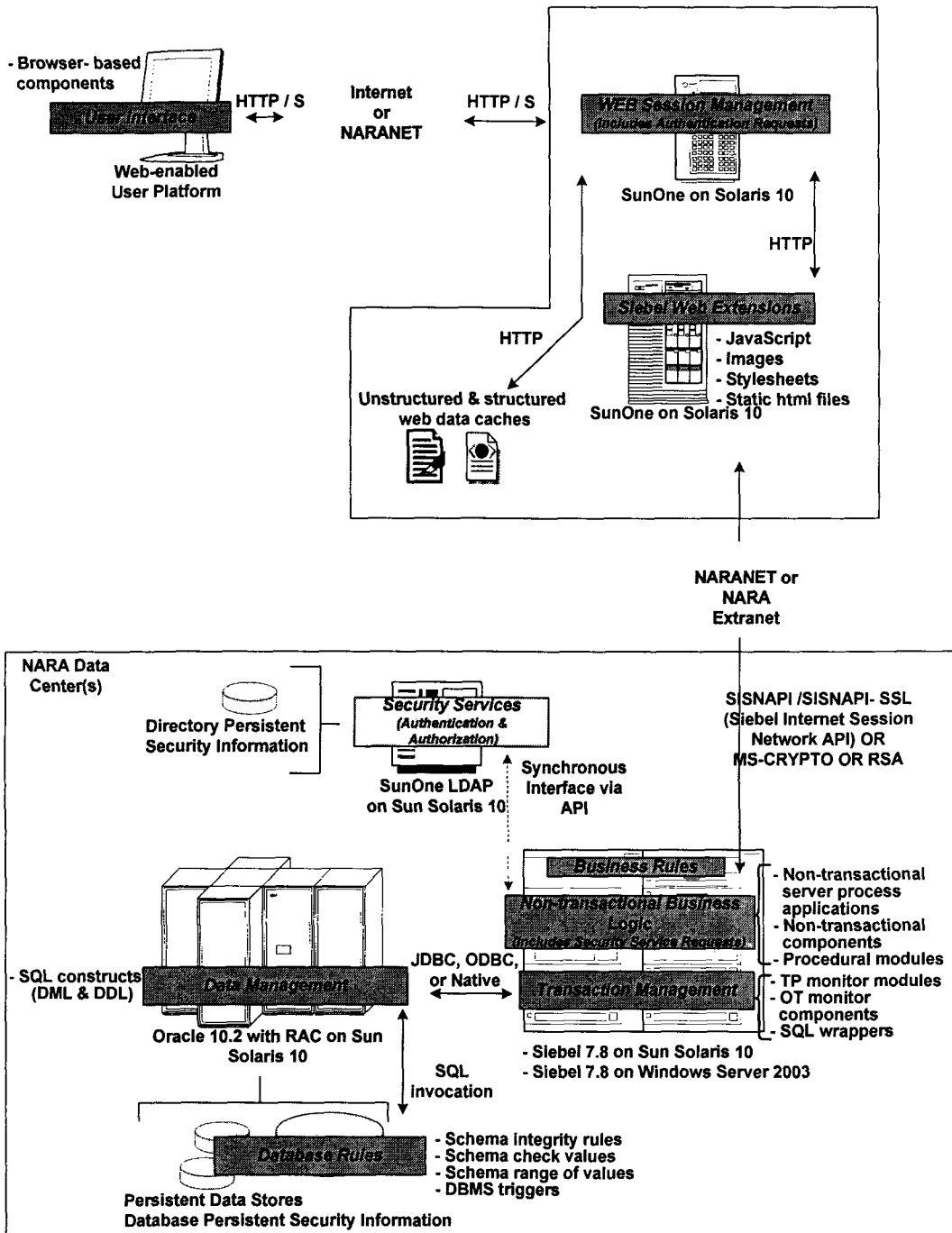


Figure 1

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 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. 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 employee whom they supervise. Administrators will have appropriate clearances and will be briefed on responsibility for securing data. Access will be through user log in 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 shown in the Entity lists contained in Section 1a for NARA staff and contractors and 1b for external users.

**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. 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.

**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. 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)?**

- RCP employees who are involved in transactional flow of RCP 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.).**

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 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.

### **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 (RPC 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 RCP 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)?**

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 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.

**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 is 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? This, and question 2 below, refer to information collections.**

Users must complete the information as required. 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?**

There are no perceived effects on the due process rights of the public, NARA employees, contractors or RCP customer agency employees.

**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 Records Management Staff (NHR) finalize the records schedule. Once the disposition schedule is approved the 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.**

See question 3, above. 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. NARA Standard Certification and Accreditation process was completed by NHI prior to launch on September 2008.

**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 management plan has been completed. ARCIS is using Siebel, a COTS product, as the platform for the application. Siebel contains extensive safeguards to safeguard information. NARA uses Siebel for both CMRS and ENOS. As a result, there were no identified risks in the ARCIS Risk Management plan regarding safeguarding data.

**9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.**

NARA standard Certification and Accreditation process was implemented prior to ARCIS operational start up date of September 2008. 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, Chief, Information Technology, Office of Regional Records Services, NR.

**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**

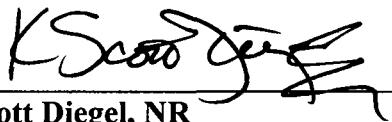
**1. Did any pertinent issues arise during the drafting of this Assessment?**

No.

**2. If so, what changes were made to the system/application to compensate**

N/A.

**The Following Officials Have Approved this PIA**



(Signature)

8/20/2009

(Date)

Scott Diegel, NR  
Chief, Information Technology  
Office of Regional Records Services  
8601 Adelphi Rd, Room 3600  
College Park, MD  
301-837-1658

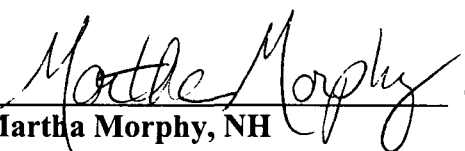


(Signature)

8/31/09

(Date)

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



(Signature)

8/26/09

(Date)

Martha Morphy, NH  
Assistant Archivist for Information Services/Chief Information Officer  
8601 Adelphi Rd, Room 4400  
College Park, MD  
301-837-1992