Privacy Impact Assessment

Name of Project: Records Management Application – Phase II

Project's Unique ID: RMAII

Legal Authority(ies): 36 CFR Subchapter B

Purpose of this System/Application:

RMA II is a records management application solution where selected user groups are able to store and retrieve electronic files. To access the RMA II system, all users must be within NARANET and have an authenticated user name and password that is synchronized with Novell. Any outside NARANET firewall connections are not possible.

FileSurf is the primary application within the RMA II system. FileSurf has two distinct interfaces available from the desktop, FileSurf desktop client and FileSurf web client. The FileSurf desktop client serves as the users' main access to the system. The FileSurf web client serves as the users' secondary option to archive, search and retrieve. Through both interfaces, records will be added, edited, searched, and moved depending on the Access Control Levels (ACL's) of the user. Access to reports and administration will also occur via both interfaces.

RMA II supports the Archives II Customer Service (NWCC2) in the processing of approximately 250,000 e-mail requests for information per year using MDY Advanced Technology Inc.'s FileSurf™ email repository and search functions. NWCC2 receives email requests that originate at the NARA web site inquiry page (http://www.archives.gov/global_pages/inquire_form.html). Once the request has been filled, NWCC2 utilizes the RMA II Application to archive email responses and forwards. RMT users have seven different workflows for filing and archiving records that are received from other departments or agencies. RMT users utilize the RMA II Application to meet this objective.

RMA II also supports: the Records Management Team (RMT), the Office of General Counsel (NGC), the NARA Rocky Mountain Region (Denver), and the Office of the Archivist in the process of preserving records that are generated during their daily activities.

Section 1: Information to be Collected

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

Privacy information contained varies greatly depending on the individual data owner needs.

a. **Employees --** Individual e-mail and/or documents that may contain personally identifiable information, including, but not limited to, social security numbers, banking information and/or home addresses. In no case are PII data stored in a comprehensive manner that would provide for easy search and retrieval.

b. **External Users --** Individual e-mail and/or documents that may contain personally identifiable information, including, but not limited to, Social security numbers, banking information and/or home addresses. In no case are PII data stored in a comprehensive manner that would provide for easy search and retrieval.

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

Extensive audit trails are in place to track the actions of users on RMA II. These audit mechanisms help to ensure that users are responsible for their actions.

Information system owners identify authorized users and their respective access authorizations. Emergency and temporary access authorizations to the information system are explicitly approved by designated organization officials, monitored, and removed as soon as no longer required. Where appropriate, access is authorized based on time and/or location. Security administrators set parameters in security software to provide access as authorized and restrict assess that has not been authorized. This includes access to files, load libraries, batch operational procedures, source code libraries, security files and operating system files.

Comprehensive account management ensures that only authorized users can gain access to information systems. Account management includes:

- Identifying types of accounts (individual and group, conditions for group membership, associated privileges)
- Establishing an account (i.e., required identification, approval, and documentation procedures)
- Activating an account
- Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators)
- Terminating an account

d. **Other (describe) -** N/A

2. **Describe/identify which data elements are obtained from files, databases,**

individuals, or any other sources?

Data elements obtained vary greatly depending on individual data owner needs.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.

Each privacy data elements contained in RMAII are for the business purpose of the individual data owner. RMAII is a system designed to provide controlled access to data by authorized users who are the owners of that data. The system serves as a repository and does contain personally identifiable information (PII), as identified by individual data owners in the agency survey of PII data. The system does not have any mechanisms that are designed to recognize, process or extract PII data, and does not have any mechanisms designed to protect PII data other than the access controls which limit user access to the data they are authorized to see. Individual data owners are responsible to manage and secure any PII data that resides in RMAII according to agency directive.

2. Is there another source for the data? Explain how that source is or is not used?

N/A

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?

No.

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

N/A

3. Can the system make determinations about employees/the public that would not be possible without the new data?

N/A

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

N/A

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

N/A

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

N/A

7. Generally, how will the data be retrieved by the user?

FileSurf™ has two distinct interfaces available from the desktop, FileSurf™ desktop client and FileSurf™ web client. The FileSurf™ desktop client serves as the users' main access to the system. The FileSurf™ web client serves as the users' secondary option to archive, search and retrieve. Through both interfaces, records will be added, edited, searched, and moved depending on the Access Control Levels (ACL's) of the user. Access to reports and administration will also occur via both interfaces.

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.

Potentially, all electronic documents in the RMA are text searchable; however, retrieval is based on the needs of the individual data owner.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

This is applicable to individual data owner. The system does not have any mechanisms designed to recognize, process or extract PII data.

10. Can the use of the system allow NARA to treat the public, employees or other persons differently? If yes, explain.

N/A

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.

N/A

12. What kinds of information are collected as a function of the monitoring of individuals?

N/A

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

N/A

14. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?

N/A

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)?

Following are the categories of users that configure, operate, and maintain the RMA II during normal use:

Domain Administrators. Members of the administrators group are the most privileged users in the system. Administrators have full access to all devices included in the system, including servers and network devices (firewalls, routers, switches, etc.).

FileSurf Users. Members of the User group are considered to be non-privileged users. They will have read-only and/or read-write access to the FileSurf application with the proper privilege settings as governed by their job function.

Database Administrators. Members of this group are the most privileged users of the database. They have full access to all databases in the system including adding, deleting, and modifying all database configuration.

FileSurf Administrators. Users in this group have FileSurf application administrative privileges. Privileges include, but are not limited to, modifying, deleting, and adding application and web application settings.

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.).

Each user or process is authorized the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

Information system owners identify authorized users and their respective access authorizations. Emergency and temporary access authorizations to the information system are explicitly approved by designated organization officials, monitored, and removed as soon as no longer required. Where appropriate, access is authorized based on time and/or location. Security administrators set parameters in security software to provide access as authorized and restrict assess that has not been authorized. This includes access to files, load libraries, batch operational procedures, source code libraries, security files and operating system files.

Comprehensive account management ensures that only authorized users can gain access to information systems. Account management includes:

- Identifying types of accounts (individual and group, conditions for group membership, associated privileges).
- Establishing an account (i.e., required identification, approval, and documentation procedures).
- Activating an account.
- Modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators).
- Terminating an account.

Separation of duties among system personnel is divided as best as can be due to the limited number of personnel involved with RMA II.

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

Data is restricted based on individual data owner requirements. RMAII does not have any mechanisms designed to protect PII data other than the access controls which limit user access to the data they are authorized to see. Individual data owners are responsible to manage and secure any PII data which resides in RMAII according to agency directive.

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)?

RMA II users are subject to NARA-wide personnel security controls. NARA personnel security controls are described in the NARA IT Security Architecture, IT Security Requirements dated 28 February 2007. The related controls are outlined in the System Security Plan for RMAII.

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?

RMAII is operated and maintained by contractor personnel. To the extent that personally identifiable information is filed into the RMAII, we ensure the proper physical and technical safeguards are in place to protect that information from inadvertent disclosure. Moreover, the appropriate clauses concerning the protection of personal or other sensitive information has been inserted in the contract for RMAII.

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 8.

RMA II does not directly share data with any other system in NARA nor is RMA II interconnected with any other NARA system. It merely captures, indexes and stores documents and request e-mails from the normal business process of the NWCC2 and RMT User Groups.

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

N/A

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

Individual data owners are responsible to manage and secure any PII data which resides in NARANET according to agency directive. 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.

No.

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?

N/A

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

N/A

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.).

N/A

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?

RMA II has not established a disposal phase. The disposition instructions will vary by office and type of record created and stored in RMA. Based on the user or user group, all data records within RMA have built in retention schedules as outlined in Files 203, the NARA Records Disposition Schedule.

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 is consistent with the approved records schedule for the types of records created and stored in RMA.

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

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. No risks were found.

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

The system has been subjected to regular security certification and accreditation review.

10. Identify a point of contact for any additional questions from users regarding the security of the system.

Richard Marcus, NHR.

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.

The RMA was not designed to collect or extract personally identifiable information subject to the provisions of the Privacy Act of 1974, as amended. However, personally identifiable information may be introduced into the system by an individual user in the course of performing his or her duties, and such information may be covered by a system of records applicable to that office, function, or individual. NARA has not published a system of record notice covering this random occurrence of personally identifiable information in the system. Moreover, no such notice is required.

It should be noted that some personally identifiable information in RMA may be covered by one or more of the Privacy Act system of records notices referenced below:

NARA 2 – Reference Request Files
NARA 14 – Payroll, Time and Attendance Files
NARA 18 – General Law Files
NARA 28 – Tort and Employee Claims Files
NARA 30 – Garnishment Files
NARA 32 – Alternate Dispute Resolution Files
NARA 34 – Agency Ethics Program Files

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

As referenced above, the RMA was not designed to collect or extract personally identifiable information subject to the provisions of the Privacy Act of 1974, as amended. Modifications to the RMAII would not require amendment or revisions to our existing Privacy Act systems.

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

The Following NARA Officials Have Approved this PIA

(Signature) 9/4/2008 (Date)

Richard Marcus
NARA Records Manager
8601 Adelphi Rd,
College Park, MD
Room 2350
301-837-1942

(Signature) 9/4/08 (Date)

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

(Signature) 9/5/08 (Date)

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