Privacy Impact Assessment (PIA)

Name of Project: Enterprise Customer Relationship Management

Project's Unique ID: ECRM

Legal Authorities:	**44 USC 2108, 2111 note, and 2203(f)(1) and 36 CFR Chapter XII, 1254.6-8**

Purpose of this System/Application:

The Enterprise Customer Relationship Management (ECRM) implementation enables Information Services (I) to establish a base global configuration that integrates with NARA's Single Sign-On and G Suite, to manage use cases by several different offices across the agency, to include the Executive Task Management System (ETMS), the Research Registration System (RRS), and Pull Database (PullDB).

Executive Task Management System (ETMS)

ETMS is a new centralized and automated solution to task, track, and report on the status of high-level official documents and correspondence for review or signature by the Archivist and/or Deputy Archivist of the United States. The ETMS system contains correspondence that is routed for signature/approval, which includes sensitive PII. This system supports the Executive Secretariat's implementation of NARA Interim Guidance 206-1, Controlled Actions and helps NARA produce well-written and effective official documents that, by content, style, and appearance, align to NARA's mission, strategic vision, and goals; reflect favorably upon NARA; and efficiently and effectively conduct the agency's business.

Researcher Registration System (RRS)

The Researcher Registration System replaces the legacy RRS, which processes a researcher's request for a Researcher ID Card to conduct research at a NARA facility. The new application modernizes the technology and the business process of the legacy RRS system. ECRM provides a more comprehensive and efficient visitor management solution, including:

- researcher self-pre-registration at Archives I and II
- improved process for scanning of researcher cards with increased security at access points
- enhanced access to researcher data reporting
- reduced operating costs

Pull Database (PullDB)

The new system automates the process NARA staff use to fulfill a researcher's on-site request for records. The PullDB application tracks the fulfillment of researcher pull requests at Archives I and II. This application is a more robust, reliable, and flexible environment for staff and researchers that includes:

- end-to-end monitoring of pull requests

- improved notification methods for customers and NARA staff
- enhanced tracking and reporting of pull and request data
- mobile devices access and elimination of current paper processes

This PIA will be amended and revised as additional Use Cases and capabilities are integrated.

Section 1: Information to be Collected

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

Employees		N/A
External Users		RRS: Name, permanent and local address, email address, home and mobile phone number, proof of ID, photograph PullDB: Name and e-mail address ETMS: none
Audit trail information (including employee log-in information)		RRS and PullDB access is limited to staff in the Researcher Registration Office, and includes information relating to authorized users that successfully enter specific research areas, date and timestamps, length of time, and failed access attempts (due to card/access expiration). ETMS access is limited to authorized users only
Other (describe)		N/A

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

NARA operational records		For RRS, card renewals only
External users		N/A
Employees		N/A
Other Federal agencies (list agency)		N/A
State and local agencies (list agency)		N/A
Other third party source		N/A

Section 2: Why the Information is Being Collected

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

RRS: Yes. This is the basic information to establish the identity of applicants for Researcher ID Cards.

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?

No

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

Yes, RRS data for the purpose of identifying applicants for Researcher ID Cards will be placed in an individual's record. The PullDB records the researcher email address with the pull request.

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

Yes, RRS determines who among the public is authorized to enter the Research Center.

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

The RRS data is provided by the individual and validated against a government-issued photo ID. The information is deemed accurate in the absence of conflicting information.

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

RRS data is not being consolidated.

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?

RRS data is searchable by most fields. The most common being the ID number or name.

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.

RRS data can be retrieved by any field, including name and ID number. However, that data is usually

retrieved by personal identifier only when there is a business need to do so. Other extracts are for statistical purposes and do not identify individuals.

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

No reports are produced on individuals unless required to by the Office of the Inspector General (OIG) or law enforcement agencies, which is extremely rare.

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

The RRS application determines whether a person is authorized to use records at Archives I and Archives II.

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.

The RRS uses a card swipe at the guard station to record which Research Rooms are visited by whom and when they visited the first time each day. The card swipe also records each instance of the individual entering and leaving the Research Center.

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

RRS monitors each time the researcher enters or leaves the Research Center and the first time they enter each Research Room each day.

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

For RRS, Physical Controls are in-place which prevent direct access to the badging terminals. Logically, local access is only granted to administrative accounts within the application. Additionally, the ECRM and its Use Cases such as RRS's network is logically separated from the enterprise using a hardened router with specific rulesets in place. RRS does not need to interact with other segments of NARANet. The local workstations are also stand-alone and cannot interface with the badging application or any network component.

The only instance of ECRM interfacing with another system is the web service connection between ECRM (FIPS199 Moderate rated) and Holdings Management System "HMS" (FIPS199 Moderate rated) to allow a return of HMS Search Results to RRS/PULL to allow the Researcher Pull Requests to be updated with the location information on Items searched in HMS. The Pull Request will then be used to physically locate item(s) in A1 or A2 stacks and return item(s) to researcher(s) for use in NARA Research Center.

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)?

RRS data is available to employees in the Registration Office, the RRS system administrator(s), Archival Operations (RD-DC) customer service managers, and to support contractor(s) on an as-needed basis, and a technician. The information might also be available to NARA's computer support contractor, but that is highly unlikely.

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?

For RRS data, access is determined by the customer service coordinator who informs the system administrator that a new person (staff member) in the office requires access. Likewise, when staff leaves and exits with the NA 3009 form, the customer service coordinator or system administrator signs off that the person's access to the RRS has been terminated. These procedures are part of the RRS system documentation and there are written procedures within the office governing these matters.

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

The NARA ECRM application Administrators create account upon approval received from system owner, and assign users to applicable Use case within the ECRM Platform (ETMS, RRS and PullDB currently). The user is assigned to one of the Use Case, based on his/her roles within NARA, and inherits the workflow associated with that system or component. The types of accounts established for ECRM Use Cases are listed below:

1. ECRM System Administrator
2. ETMS Administrator
3. ETMS Archivist
4. ETMS User
5. NARA Standard User
6. NARA Read only user
7. NARA RRS User
8. Pull Station Staff
9. NARA Records Retention User

Each account is controlled by a Profile and a Profile is associated to a user.

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?

There is an audit trail to document unauthorized browsing. The written procedures used during training

emphasize that unauthorized browsing is forbidden.

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?

Contractors are involved on an ad hoc basis with the system maintenance and are covered by appropriate contractual clauses. The ECRM Use Cases include Commercial Of The Shelf (COTS) products. In the event of an incident which requires vendor support, a request is made to the vendor for an on-site visit.

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.

There is an automated tracking of pull requests that requires location information from HMS. This is enabled through a web service connection between RRS (FIPS199 Moderate rated) and HMS (FIPS199 Moderate rated) to allow a return of HMS Search Results to RRS/Pull, and enable the Researcher Pull Requests to be updated with the location information on Items searched in HMS. The Pull Request is then used to physically locate item(s) in A1 or A2 stacks and return item(s) to researcher(s) for use in NARA Research Center.

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

Other systems do not provide or receive data from RRS. Rather RRS pulls data from HMS for location information on Items searched.

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

The RRS interface does not share any of the personal information.

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, except as needed for law enforcement purposes.

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?

For RRS, individuals can decline to provide the information, but they will not be issued a Researcher ID Card and are therefore prevented from conducting research at NARA.

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

For RRS, the researcher can appeal the decision up to review by the Deputy Archivist of the United States.

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.).

RRS data is provided by the person being issued the Researcher ID Card and is presumed to be accurate. The cards are issued for a period of one year, and then must be renewed, at which point the personal information is validated again. 36 CFR 1254 describes the process for applying for a Researcher ID Card and the period it is effective.

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?

For RRS, there is a second site at Archives I. The Customer Services Manager is in-charge of both locations and oversees the operation of both sites. The same set of guidelines apply to both locations.

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

The PII collected is kept within the system and is not purged or removed from the servers until its scheduled disposition.

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.

For the ECRM use cases, the PII collected consists of first and last name, home address and local address if any, e-mail address, telephone number (home, work, mobile). This information is collected for the sole purpose of being issued a Researcher ID Card. All PII data collected is retained indefinitely within the servers and is never purged or removed prior to its scheduled disposition. The records schedule for Researcher Registration and PullDB requires retention of the information for 25 years.

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?

For RRS, NARA regulations require that prospective researchers visiting a NARA research room provide proper and legal documentation in order to be admitted to do research. Any information provided to obtain a Researcher ID Card is done completely voluntarily. We do not share the information except when legally required to do so by the OIG or a Government law enforcement organization, and then only with the NARA Privacy Officer's and/or Office Head's approval.

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

Yes, ECRM has a system security plan and has been authorized by the CIO.

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. The major risk for ECRM is that the servers handling the system fail. When that occurs, NARA staff revert to the paper-based system of issuing ID cards to researchers until service is restored. The risk is minimal because the ECRM infrastructure is provisioned on a Salesforce FedRamp certified Cloud, with full redundancy. Traffic will be picked-up by the secondary site should the primary site become unavailable. Normally a NARA system failure will be linked to a failure of NARAnet.

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

There is an audit trail to cover browsing the records. An Information System Contingency Plan (ISCP) tabletop exercise for various scenarios is conducted with the Information Security staff on an annual basis.

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

Tom McManuels (Information System Security Officer for ECRM) Contact information: 8601 Adelphi Road, Room B551-A, College Park, MD 20740-6001 Thomas.McManuels@nara.gov 301-837-3678, and
Edward Graham (ECRM System owner).

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.

System 1: Records relating to Researcher applications.

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, ECRM runs on a FedRamp certified Software As A Service (SaaS), and comprehensive documentation was established and validated for FedRamp Authority To Operate (ATO).

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)	
EDWARD GRAHAM Digitally signed by EDWARD GRAHAM Date: 2021.04.23 09:14:26 -04'00' (Signature)	(Date)
Name: Edward Graham	
Title: Director Development and Tools Management Division (ID)	
Contact information: 8601 Adelphi Road, Room 2600, College Park, MD 20740-6001 edward.graham@nara.gov 301-837-3732	
Senior Agency Official for Privacy (or designee)	
GARY STERN Digitally signed by GARY STERN Date: 2021.03.31 09:44:05 -04'00' (Signature)	(Date)
Name: Gary M. Stern, NGC	
Title: Senior Agency Official for Privacy	
Contact information: 8601 Adelphi Road, Room 3110, College Park, MD 20740-6001 garym.stern@nara.gov, 301-837-3026	
Chief Information Officer (or designee)	
SWARNALI HALDAR Digitally signed by SWARNALI HALDAR Date: 2021.05.14 09:06:03 -04'00' (Signature)	(Date)
Name: Swarnali Haldar	
Title: Executive for Information Services/CIO (I)	
Contact information: 8601 Adelphi Road, Room 4415, College Park, MD 20740-6001 swarnali.haldar@nara.gov, 301-837-1583	