Privacy Impact Assessment

Name of Project Archival Electronic Records Inspection and Control Project's Unique ID: AERIC

Legal Authority(ies): 44 U.S.C. Chaps 21, 29, 31 and 33

Purpose of this System/Application:

The Archival Electronic Records Inspection and Control (AERIC) system assists with NARA's mission of making information available to the public by providing a way to check the accuracy of record descriptions and by creating public use versions of restricted files.

AERIC is used to automate the verification of some types of electronic records. The process of verification compares the actual content of records received from a federal agency to the description of those records as represented by the layout and codes provided by that agency. The entry of the record layouts into AERIC has enhanced NWME's reference services by creating a continually growing database of metadata on NWME's holdings, which can be searched in response to requests for specific records. In addition, AERIC can create public-use versions of restricted files. The system is connected to NARA's Intranet (NARANet).

AERIC verifies the content of electronic record files sent to NARA by Federal Government agencies by comparing the data files to their documentation. This process ensures the completeness of the data, the adequacy of the documentation, and the future usability of the records for Researchers.

Two reports that present the information as entered into AERIC are as follows:

- The Record Layout Report lists the fields that have been entered into AERIC from the agency record layout
- The Checklist for Verification Report lists the options chosen by the processing archivist to verify the contents of the data files.

When a file is copied into AERIC, it produces a Load Report that states the total number of records copied into AERIC. After matching the record layout to each record in the file, AERIC creates Verification Reports that provide the results of the verifications. These reports identify discrepancies between descriptions of the records and the actual content of the records.

AERIC has a total of four instances: Unclassified, Title 13, TS and TS/SCI.
The unclassified version of AERIC is accessible by all NARA staff members who verify

the accuracy of electronic record transferred to NARA.

The Title 13 version of AERIC is only accessible to authorized NARA staff members who have received Special Sworn Status from the Office of Security of the Bureau of Census.

Classified versions of AERIC (TS and TS/SCI) are only accessible to appropriately cleared NARA staff members who have received collateral security clearances granting them access to the level of classified material likely to be encountered in the course of their work. Employees with Top Secret security clearances have access to the TS version of AERIC. Those employees holding Top Secret/Sensitive Compartmented Information security clearances have access to the TS/SCI version of AERIC. Standards for evaluating NARA employees for security clearances are outlined in NARA 273, Personnel Security Clearances.

Section 1: Information to be Collected

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

a. Employees – Name and account name.

b. External Users – N/A

c. Audit trail information (including employee log-in information) – Employee login information and work tracking files.

d. Other (describe) – N/A

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

a. NARA operational records – N/A

b. External users – N/A

c. Employees – N/A

d. Other Federal agencies (list agency) – All Federal agencies can supply data consistent with approved records schedules. Some records submitted contain personally identifiable information. Records in AERIC are only retained for verification purposes. Following the verification process all data is deleted.

e. State and local agencies (list agency) – N/A

f. 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.

Yes. All data elements in the system are needed to verify the records and to confirm that only authorized users are gaining access to the records..

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

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?

Data is retrieved through standardized and ad hoc queries against a database. These queries are used to verify the data not to obtain information concerning individuals.

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.

As stated above, AERIC maintains data transferred to NARA from various federal agencies. It is likely that some data may contain personally identifiable information, including social security numbers or other unique identifiers. AERIC is only accessible to authorized NARA staff for the purposes of verifying the data against the explanatory documentation. No data in AERIC is made available to the public.

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.

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.. No

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 – The AERIC System is only available to NWME Staff members within Archives II.

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)?

Authorized users and support contractors.

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.).

Access is determined by the system administrator based on job duties. Technical controls protect against unauthorized access to, or misuse of AERIC

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

Authorized users have access to the data in AERIC.

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)?

Technical controls protect against unauthorized access to, or misuse of, AERIC and facilitate detection of security violations by generating audit logs to record users' activities and warn of anomalous conditions in the network. Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability.

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, there are clauses that warn against unauthorized disclosure of information from AERIC. Note, however, that the provisions of the Privacy Act do not apply to the data in AERIC.

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.

NARANet provides transport service from the user's personal computer to the AERIC application server. AERIC does not connect to any other system.

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

Certification Dates
Unclassified AERIC: January 18, 2006
Title-13 AERIC: July 12, 2006
Top Secret AERIC: December 12, 2006
TS-SCI AERIC: March 7, 2007

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

The AERIC owner and individual users are responsible for managing and securing any personal data which resides in the system. 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)? N/A

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.

AERIC does not accept data from the public. The only data in AERIC is data that has been transferred from other Federal agencies.

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

N/A. The records in AERIC are archival records transferred to the custody of the Archivist of the United States for permanent retention. Archival records are specifically excluded from the access and amendment provisions of the Privacy Act.

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.).**

The data is verified for completeness by matching the data with is explanatory documentation. This documentation is provided by the creating agency at the time of transfer. The document is not verified for accuracy or timeliness; it is assumed accurate and timely at the time of transfer from the originating agency. Specific procedures relating to the verification process are outlined in the AERIC Users Manual.

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?

Data in AERIC is kept in the system for as long as needed to complete the verification process. That period of time can extend from one month to one year.

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.

The data in AERIC is transitory and deleted upon completion of the verification process. However, users create reports during the verification process. Most reports are temporary. The Checklist for Verification and the Load Report are permanent and stored with the documentation package for the data that was verified. Other reports may also be deemed permanent if they add value to the understanding of the data.

5. Is the system using technologies in ways that the Agency has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? 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

Dates for Completion of the Certification and Accreditation Process

Unclassified AERIC: January 18, 2006
Title-13 AERIC: July 12, 2006
Top Secret AERIC: December 12, 2006
TS-SCI AERIC: March 7, 2007

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 Plan of Actions and Milestones (POA &M) process was utilized to addresses and resolve risks.

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

NARA conducts vulnerability scans on all network devices on a monthly basis according to a predefined schedule. A quarterly report of open vulnerabilities is compiled and analyzed. In addition, a subset of NIST 800-53 controls are tested for NARA systems on an annual basis.

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

Mr. Michael R. Carlson, Director/System Owner -- (301) 837-1578
Mr. Theodore C. Haigler, Project Manager – (301) 837-1783

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. N/A

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

for me _____ (Signature) 9/3/08 (Date)
Michael Carlson, NWME
AERIC System Owner, Director
8601 Adelphi Rd, Room 5320
College Park, MD 20740-6001
301-837-1578

Theodore C. Haigler (Signature) Sept 3, 2008 (Date)
Theodore C. Haigler, NWME
AERIC Project Manager, ISSO
8601 Adelphi Rd, Room 5320
College Park, MD 20740-6001
301-837-1783

for Sandra Blanc (Signature) 9/3/08 (Date)
Leo Scanlon, NHI
Chief Information Security Officer
8601 Adelphi Rd, Room 4400
College Park, MD 20740-6001
301-837-0752

_____ (Signature) 9/4/08 (Date)
Gary M. Stern, NGC
Senior Agency Official for Privacy
8601 Adelphi Rd, Room 3110
College Park, MD 20740-6001
301-837-3026

Martha Morphy (Signature) 9/5/08 (Date)
Martha Morphy, NH
Chief Information Officer
8601 Adelphi Rd, Room 4400
College Park, MD 20740-6001
301-837-1992