Privacy Impact Assessment

Name of Project: **Access to Archival Databases**

Project's Unique ID: **AAD**

Legal Authority(ies): **44 USC Chapters 21, 29, 31 and 33**

Purpose of this System/Application:

The Access to Archival Databases Project (AAD) was developed in the interest of simplifying, facilitating, and economizing customer access to a selection of electronic records produced by all components of the Federal Government and for providing continuing access to these records. AAD is a data access utility that provides a single, consistent interface for end user query and access to structured data, with rich, reliable, and flexible search, retrieval, and output capabilities. Phase 3A, Version 3.0 of the AAD permits researchers and NARA staff to search, view, and retrieve records from selected accessioned Government databases directly through the Internet. AAD includes more than 400 database files in more than 40 records series created by more than 30 Federal agencies or in collections of donated historical materials.

Users to the NARA AAD system are Public Users that have access to the system via the Internet. Public users are able to review news and advisories on the AAD system once they have accessed the system. Users also consist of NARA employees who have access to NARA dedicated resources and archive records via NARANet

AAD's primary purpose is to provide the public with access to archival data files that are most appropriate for record-level access via the Internet. The only records that will be made available to the public through AAD services will be archival data files without access restrictions. Records that are restricted from access may contain information that is national security classified or information that is otherwise restricted, and will not be made accessible to the public through the AAD and its operating systems.

Section 1: Information to be Collected

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

a. Employees -Users consist of NARA employees who have access to NARA dedicated resources and archive records via NARANet. NARA users can log on to NARA Staff-Only AAD system using a valid username and password.

b. External Users – N/A

c. Audit trail information (including employee log-in information) – To the extent that information and data is captured as part of the logs in the AAD system, the system administrator conducts *ad hoc* queries and provide reports of a security and data integrity nature as requested by the NARA AAD Project Manger.

The System Administrator utilizes Oracle Auditing Tools to look for any unauthorized changes to monitored data tables associated with agency electronic records or to detect any unauthorized changes on both the public and NARA Staff-only databases.

The System Administrator verifies the integrity of the AAD applications code in the both the public and NARA staff-only subsystem using a digital signature mechanism.

d. Other (describe)) - Users to the NARA AAD system are Public Users that have access to the system via the Internet. Public users are able to review news and advisories on the AAD system once they have accessed the system.

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) Federal agencies are the originators of archival records that are available via AAD. Some records submitted contain personally identifiable information. However, personal information is masked from public disclosure consistent with the provisions of the Freedom of Information Act (5 U.S.C. 552), and only the masked versions of the archival records are provided to the AAD contractor for loading into AAD.

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. User data is needed to establish and maintain user profiles for access to the staff-only portion of the AAD, which restrict access to system features as appropriate.

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?

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?

Data in AAD that is publicly available has been verified against the explanatory documentation provided at transfer, i.e., during accession processing. This step precedes any preparation of the records for loading into AAD. Data is not further verified for accuracy or timeliness; it is assumed to be accurate and timely at the time of transfer from the originating agency.

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?

Users to the NARA AAD system are Public Users that have access to the system via the Internet. Public users are able to review news and advisories on the AAD system once they have accessed the system. Data is retrieved through standardized and ad hoc queries against a database. The only records available to the public through AAD are data files without access restrictions.

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, AAD maintains data transferred to NARA from various federal agencies. It is likely that upon transfer, some data may contain personally identifiable information, including social security numbers or other unique identifiers. However, no restricted information is made available through AAD. Only publicly available data can be accessed through AAD.

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 individual AAD users.

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?

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)?

Users and authorized contractors will have access to all data in AAD. Public users will have access to the publicly available records in AAD through the internet.

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, AAD.

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 AAD

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, AAD 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 AAD. Note, however, that the provisions of the Privacy Act do not apply to the archival data in AAD.

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.

AAD interfaces with several NARA systems.

- **Archival Electronic Records Inspection and Control (AERIC) System**

The Archival Electronic Records Inspection and Control (AERIC) system is used to verify the adequacy of the accompanying documentation for the electronic data files transferred by federal agencies to NARA.

- **Archival Research Catalog (ARC) Interface (ARC)**

ARC is the online catalog of NARA's nationwide holdings, including those from the Washington, DC area, Regional Archives, and Presidential Libraries. ARC allows basic and advanced searching of archival descriptions and information about archival creators.

- **APS Interface - Data Export Module**

This interface is a one-way copy process of updated data from the APS onto removable media for uploading into AAD, including new titles, record counts, file byte sizes, data indicators (e.g., ASCII or EBCDIC), and record lengths, etc.

- **File Transfer Server - File Transfer Services**

The file transfer servers are used to make file based information, such as agency documentation files in PDF file format, available within AAD to users for downloading. The file transfer servers can also be used to transfer scanned document images and PDF files from NARA to the AAD contractor.

- **AAD Home Page Interface on NARANET**

AAD services are launched from the NARA Public Website (www.archives.gov/aad). Currently, all of the AAD help pages, tutorials, and related aids are hosted by this web site. AAD maintains the content for these files as HTML fragments on the AAD website and provides a URL to NARA where they are then formatted and presented within the frames of the NARA website.

- **Document Store - Scan Documentation (Manual Process using COTS products).**

This program layer produces scanned images of selected agency documents for delivery online. The choice of scanner type depends upon the document size, number of pages, and other factors such as:

- Image Quality (Skew, Density, Clarity, Distortion, Font Face and Size)
- Binding of Original
- Background
- Embedded Images
- Staples, Holes, Tears, etc.
- Print Type (Laser, Dot Matrix, Handwritten)

Either a large flat bed (11 x 17) scanner, or an HP ScanJet with automatic page feeder is used.

- **Generate PDF**

This program layer takes scanned images of the previous program layer and converts them into Portable Document Format (PDF) for online delivery.

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

Yes. A Certification and Accreditation has been performed and is approved and a PIA was completed in 2007. There have been no design changes, nor any changes to features made since that time.

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

The AAD system 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)? If so list the agency and the official responsible for proper use of the data, and explain how the data will be used.

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?

AAD does not accept data from the public. The only data in AAD are historical data that have been transferred from other Federal agencies or in donated historical materials for permanent retention by NARA in accordance with the Federal Records Act.

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 AAD are archival records transferred to the custody of the Archivist of the Untied 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.).

Data in AAD that is publicly available has been verified against the explanatory documentation provided at transfer, i.e., during accession processing. This step precedes any preparation of the records for loading into AAD. Data is not further verified for accuracy or timeliness; it is assumed to be accurate and timely at the time of transfer from the originating agency.

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 AAD are records that have been transferred to NARA for permanent retention.

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 above.

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?

Certification and Accreditation has been performed and is reviewed annually by NARA security personnel. The system meets both IT security requirements and all procedures required by federal law and policy to the best of our knowledge.

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?

The last security risk assessment was performed in August, 2007. Any risks requiring mitigation were put into a POAM for the system so that milestones for eliminating weaknesses could be tracked.

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

As part of the normal operations and maintenance of the AAD system, auditing tools are used to look for any unauthorized changes to data tables associated with agency electronic records, AAD applications code, and other unauthorized database actions. System event logs and firewall logs are also monitored for unauthorized access. 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.

Michael Carlson, Director
Electronic and Special Media Records Services Division
(301) 837-1578
Michael.Carlson@nara.gov

Margaret Adams
Electronic and Special Media Records Services Division
(301) 837-1661
Margaret.Adams@nara.gov

Kenneth Grant, IT Project Manager
Electronic and Special Media Records Services Division
(301) 837-1661
Kenneth.Grant@nara.gov

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.

Archival records in AAD are specifically excluded from the access and amendment provisions of the Privacy Act.

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

The Following Officials Have Approved this PIA

_____ (Signature) 9/5/08 (Date)

Michael Carlson, NWME
AERIC System Owner, Director
8601 Adelphi Rd, Room 5320
College Park, MD 20740-6001
301-837-1578

_____ (Signature) 05 Sept 2008 (Date)

Kenneth Grant, NWME
AAD Project Manager
8601 Adelphi Rd, Room 5320
College Park, MD 20740-6001
301-837-1661

A Blaine for Leo Scanlon (Signature) 9/5/2008 (Date)

Leo Scanlon, NHI
Chief Information Security Officer
8601 Adelphi Rd, Room 4400
College Park, MD 20740-6001
301-837-0752

_____ (Signature) 9/5/08 (Date)

Gary M. Stern, NGC
Senior Agency Official for Privacy
8601 Adelphi Rd, Room 3110
College Park, MD 20740-6001
301-837-3026

_____ (Signature) 9/5/08 (Date)

Martha Morphy, NH
Chief Information Officer
8601 Adelphi Rd, Room 4400
College Park, MD 20740-6001
301-837-1992