

Privacy Impact Assessment (PIA)

Name of Project: Access to Archival Databases

Project's Unique ID: AAD

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

Purpose of this System/Application:

The Access to Archival Databases simplifies public access to a selection of accessioned electronic records in the National Archives of the United States. 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. Through a web portal, AAD permits researchers and NARA staff to search, view, and retrieve records from selected accessions. AAD includes more than 600 database files in more than 40 records series created by more than 30 Federal agencies or in collections of donated historical materials.

The only records that are made available to the public through AAD are archival data files without access restrictions.

Section 1: Information to be Collected

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

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.
External Users	Researchers may browse AAD by visiting https://aad.archives.gov/aad/ No log in information is required
Audit trail information (including employee log-in information)	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.
Other (describe)	n/a

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

NARA operational records	n/a
External users	n/a
Employees	n/a
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, privacy information is withheld from public disclosure consistent with the provisions of the Freedom of Information Act (5 U.S.C. 552).
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.

The contents of accessioned datasets or records is determined in the records scheduling process. Records available within AAD are those which have been determined to be permanently valuable to the United States.

Account information for NARA users is collected and maintained for proper administration of the system.

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?

Researchers may combine the publicly available records on AAD with other collections of publicly available information to create previously unavailable data about an individual. NARA hopes that by making records available to the public via AAD, more uses for the information will be discovered over time.

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

No. If researchers use information in archival records to reach new conclusions, NARA does not incorporate that data into its holdings or otherwise track it.

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

The system cannot make determinations on its own. Researchers may use the data provided to make such determinations.

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

NARA does not validate research based on its holdings. This is the role of academics and other researchers.

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

AAD's security plan is incorporated within that of the Electronic Records Archives, or ERA. All records contained in AAD are available to the public, thus the security of the system focuses on ensuring it is not vulnerable to attack or its contents altered.

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 contained in AAD may be retrieved based on standard and ad hoc queries, and through browsing <https://aad.archives.gov/aad/>.

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.

Archival Data within AAD may be retrieved by a variety of personal identifiers. These identifiers were collected by the creating agency, and have been determined to be appropriate for public release by NARA. For example, the Defense Casualty Analysis System, which is a listing of U.S. military officers who died as a result of either a hostile or non-hostile occurrence in the Korean War, Vietnam War, Gulf War, or War on Terrorism, may be queried by service member name, birthday, home city, home state, date of death, etc. As new data sets are added to AAD, more information may be queried.

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

Researchers may do a significant amount of biographical research on individuals and produce reports from publicly available information. NARA does not track the use of the reports or who has access to them.

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.

This system will not be used by NARA for such tasks. Researchers may use the historical records available through the system to do so.

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

No information is collected by NARA.

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

AAD's system security controls are used prevent unauthorized monitoring of NARA data.

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

While AAD does not use persistent cookies, some aggregate user data is collected: i.e., number of visitors, what series queried, and potentially queries per series by domain. This data does not, and cannot, be used to identify individual web visitors.

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.). Are safeguards in place to terminate access to the data by the user?

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

Access by researchers to archival data is determined in accordance with NARA's policies and procedures for screening archival records and data. These procedures ensure that, when needed, public use versions of archival data are created until such time as the entire dataset may be open and available.

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)? How will these controls be monitored and verified?

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 access and amendment 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 7.

Other NARA systems (AERIC, APS, and ERA) are used to copy data or metadata that is then manually uploaded to AAD. While content is shared or passed through these other systems, there is no direct connection/interface with AAD.

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?

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?

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. To the extent an individual would have had an opportunity to decline to provide information and consent to its use, it would have been at the point of collection by the creating agency.

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

No, NARA does not alter archival records in the holdings, and the access and amendment provisions of the Privacy Act do not apply to archival records. To the extent an archival record led to a negative determination regarding an individual, that individual’s recourse was with the creating agency at the time the determination was made. Archival records are historical, and fixed in time. The Privacy Act provisions allowing for updates to individual records do not apply to records in NARA’s holdings.

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 the accession processing. This step precedes any preparation of the records for loading into AAD. Data is not 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 archival 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.

n/a

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?

A risk assessment for AAD was completed in October 2015. Two risks were identified related to possible exploits of the system and are being mitigated.

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

The system is monitored in accordance with NARA IT security policies.

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

Theodore Hull, Director
Electronic Records Division
301-837-1824
Theodore.Hull@nara.gov

Lynn Goodsell
Electronic Records Division, Reference Branch
301-837-0468
Lynn.Goodsell@nara.gov

Michael Haines (ISSO for AAD)

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?

While AAD is part of NARA's ERA system, a decision was made to evaluate ERA's component systems separately for privacy purposes. This ensures a greater level of detail in the privacy

documentation and transparency for the public.


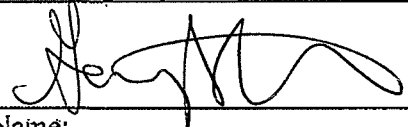
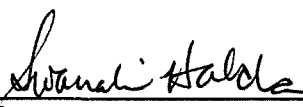
2. If so, what changes were made to the system/application to compensate?

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)	
	(Signature) 8/16/2016 (Date)
Name: Leslie Johnston	
Title: Director, Development & Tools Management	
Contact information: leslie.johnston@nara.gov	
Senior Agency Official for Privacy (or designee)	
	(Signature) 9/30/16 (Date)
Name: Gary M. Stern	
Title: General Counsel & SAOP	
Contact information: garym.stern@nara.gov	
Chief Information Officer (or designee)	
	(Signature) 10/3/2016 (Date)
Name: SWARNALI HALDER	
Title: CIO, Executive for Information Services	
Contact information: SWARNALI.HALDER@NARA.GOV	