

Privacy Impact Assessment (PIA)

Name of Project: National Archives Catalog

Project's Unique ID: NAC

Legal Authority(ies):	44 USC 2101, et seq.
------------------------------	----------------------

Purpose of this System/Application: National Archives Catalog (formerly Online Public Access) system was created by NARA to serve as the primary method for search, access, and distribution of publicly available, digital NARA content. At a high level, NAC holds a copy of publicly available NARA digital content, provide methods for downloading this content by the public, maintains and make available renditions (for example, images at different resolutions) of the content designed to make the content more useful for the public, provides methods to search this content and associated metadata so that users can easily find the content they wish to access. This includes maintaining a search engine index over the content, providing a search user interface to the content, providing APIs and other methods for end-users to access the content programmatically.

Section 1: Information to be Collected

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

Employees	Name (First, Last), UserID, and associated email address..
External Users	To the extent that contractors have accounts on NARA systems, the information available about them will be the same as information discussed above for employees: Name (if provided, First, Last), UserID, associated email address. Members of the public have the ability to have an account established, after providing the necessary information to have such an account created: Name (First, Last), UserID, and email address. Users have the option of displaying their full name to the public.
Audit trail information (including employee log-in information)	The system will have a log of various user actions to include logins and actions taken and processed by the system.
Other (describe)	N/A

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

NARA operational records	None
External users	Only information provided by external users when registering for an account.
Employees	Only information provided by employees when creating an account.
Other Federal agencies (list agency)	N/A
State and local agencies (list agency)	None
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 UserID is necessary in order to authenticate the user. The email address is necessary for sending system notifications. Name is necessary to identify submitters.

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?
 The system does not make determinations about the user.

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?

NARA staff and government contractors responsible for managing and operating the NAC system will have access to the PII data about NAC system users. Help Desk staff responsible for responding to users requests for assistance will have access to data necessary to provide such response. NAC users performing system management can retrieve user account information by a search on a unique user identifier or user name. Reports containing user name, agency, role, and account status (active or terminated) are published to NARA staff monitoring user account usage. The public NAC users supply the NAC user account information, but do not have access to it within the system.

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

No existing processes are being consolidated.

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

Data will be retrieved by the end user via the user interface of the application only after user identification and authentication.

The following restrictions on user access to information apply to NAC.

- For NARA operational PII data – NARA Delegated Account Representatives (DAR) will have user account information for those users they recommend for NAC accounts. The DAR will not have access to any other NAC user information. Appropriate NAC system maintenance staff will have access to all user account information. Appendix C contains account information.
- For archival materials in NAC – the information that will be processed by NAC is substantially the same as that which is currently made available electronically or on paper. Therefore, access restrictions will be (at a minimum) the same as currently in place. As specified in 5 U.S.C. 552a(1)(3), federal records transferred to NARA are not subject to most of the Privacy Act provisions. NARA's implementation of FOIA regulations (36 CFR 1250) governing access to records containing personal information, will also apply to the access of electronic materials that will be contained in NAC.

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.

No.

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

The system keeps track of an individual's activity on NARA's internal systems. If an employee or contractor misuses the system, information about that misuse may become part of their record.

Reports are not produced specifically on public users or individuals. Regular reports can be generated on system accounts that have passed thresholds for inactivity or expiration. These reports are generated for maintenance of the system and are not determined by individual's information.

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

NAC differentiates users to determine access to the system. NAC allows everyone to access data stored on the system, but requires users to register in order to save results and provide additional features. Specific NARA employees have elevated access to manage and approve user comments and tagging abilities.

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?

NAC differentiates users to determine access to the system. NAC allows everyone to access data stored on the system, but requires users to register in order to save results and provide additional features. Specific NARA employees have elevated access to manage and approve user comments and tagging abilities

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

NAC uses session cookies to maintain sessions for users, but does not create persistent cookies for user

identification

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)?

NARA staff and government contractors responsible for managing and operating the NAC system will have access to the PII data about NAC system users. Help Desk staff responsible for responding to users requests for assistance will have access to data necessary to provide such response. NAC users performing system management can retrieve user account information by a search on a unique user identifier or user name. Reports containing user name, agency, role, and account status (active or terminated) are published to NARA staff monitoring user account usage. Authorized employees of other Federal agencies retain responsibility for determining who should have access (and what those access rights are) to records stored in the NAC system. The NAC users from external agencies supply the NAC user account information, but do not have access to it within the NAC system. Public users will have access to NAC. NAC only contains data determined applicable for public release

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?

The system employs role-based security. The following restrictions on user access to information apply to NAC:

- For NARA operational PII data, NARA Delegated Account Representatives (DAR) will have user account information for those users they recommend for NAC accounts. The DAR will not have access to any other NAC user information. Appropriate NAC system maintenance staff will have access to all user account information. Appendix C contains account information.
- For archival materials in NAC, the information that will be processed by NAC is substantially the same as that which is currently made available electronically or on paper. Therefore, access restrictions will be (at a minimum) the same as currently in place. As specified in 5 U.S.C. 552a(I)(3), federal records transferred to NARA are not subject to most of the PA provisions. NARA's implementation of FOIA regulations (36 CFR 1250) governing access to records containing personal information, will also apply to the access of electronic materials that will be contained in NAC.

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

Explain.

Access to information in the system is restricted by the system administrator based on job duties and need to know.

User access is determined by role. Some NARA users have access to all data. Agency users are given access to their own data and may be further segregated by their role within the agency. System maintenance staff (by virtue of their elevated privilege) have technical access to the data, but are not given permission to access the data unless it is required to perform a specific task to maintain the system. NAC differentiates users to determine access to all data on the system. Registered users are given the ability to create supplemental data such as comments or keywords, but are not given any

other elevated privilege on the system.

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?

Authorized users of the System are subject to the NARA personnel security controls. NARA personnel security controls are described in section I of NARA IT Security Handbook Operations Controls. This protocol reminds users to only use the system for the purpose for which it was created and consistent with their authorized duties. This message is reinforced in annual security training and is reinforced with issuance of NARA policy guidance on this topic.

User and administrative accounts are monitored and verified on a monthly basis with the ISSO submitting a request for a system generated account list from the Technical POC with submission to the System Owner for attestation.

Management operational and technical controls to prevent misuse of data by those with privileged access will be selected in accordance with NIST SP 800-53/FIPS PUB 200. These NAC system components that implement these controls detect unauthorized access and unauthorized monitoring. Transportation of NAC PII data outside the boundary of NAC physical control is encrypted to prevent unauthorized access. Continuous monitoring is in place to periodically review security controls to determine the effectiveness and viability.

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. Privacy Act contract clauses were inserted in their contracts and other regulatory measures addressed.

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.

Yes. NAC interfaces with DAS. DAS includes standardized descriptions of both non-electronic and born digital holdings, as well as links to other descriptive contents.

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?

General responsibility for protecting personal privacy information in materials in NARA's custody rests with the Archivist of the United States in accordance with the FOIA, 5 U.S.C. 552, as amended; the Privacy Act, 5 U.S.C. 552a, as amended; the Federal Records Act, 44 U.S.C. 2108; and the Presidential Records Act, 44 U.S.C. 2204 and 2207.

The NAC Designated Approving Authority will have the responsibility for protecting the privacy of personal information that is required submit an account on the NAC system.

For records not yet transferred into NARA's legal custody, NARA will act under the direction and on behalf of originating agencies to protect privacy.

The NARA Senior Agency Official for Privacy is the NARA General Counsel (NGC). The General Counsel will provide legal guidance and has overall responsibility and accountability for ensuring NARA's implementation of information privacy protections, including NARA's full compliance with federal laws, regulations, and policies relating to information privacy.

The NAC Designated Approving Authority will have the responsibility for ensuring the controls implemented within NAC are protecting the privacy of personal information that is specifically stored within the NAC system. The responsibility of the NARA Office of the Inspector General (OIG) includes, but is not limited to ensuring compliance with laws regulations and internal policies in carrying out the NAC program.

As such the OIG may conduct audits and investigations concerning all aspects of the NAC program such, the OIG may conduct audits and investigations concerning all aspects of the NAC program, including compliance with laws, regulations, guidelines and internal policies. NARA has no direct control over the proper use of privacy data by another agency. It is assumed that the other agency has designated an agency level official responsible for privacy per OMB M-05-0S8, "Designation of Senior Agency Official for Privacy," and that, in cooperation with the agency's Inspector General, that SAOP will be responsible for assuring proper use of data.

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?

Submission of the requested information is voluntary; however, refusal to provide such information by members of the public will result in the inability to access the additional features of the Catalog (saved searches, tagging, transcription, etc). Refusal to provide this information may also result in the inability to perform certain job related tasks because an individual will be unable to gain access to the system.

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?

Records stored in the system are public use copies of permanently valuable records in the Archives of the United States.

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 unclassified that cannot be destroyed or purged until the schedule is approved.

Disposition instructions for documents and metadata are defined by Chapter 15 of the NARA Records Schedule.

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.

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

Security scans are completed by NARA IT Security. Monitoring will be provided by the Amazon Web Services (AWS) cloud provider.

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

The points of contact are Andrew Wilson, Kwame Boakye Gyan, Richard Steinbacher, Carol Lagundo and Keith Day.

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?

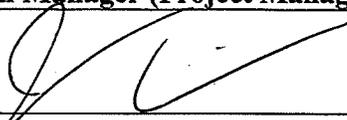
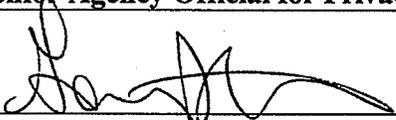
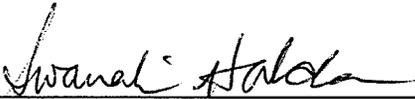
N/A

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

System Manager (Project Manager)	
	11/7/2017
(Signature)	(Date)
Name: Jason Clingerman	
Title: System Owner	
Contact information: 8601 Adelphi Road, Room 3100 College Park, MD 20740-6001 jason.clingerman@nara.gov	
Senior Agency Official for Privacy (or designee)	
	10/25/17
(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 301-837-3026, garym.stern@nara.gov	
Chief Information Officer (or designee)	
	11/21/2017
(Signature)	(Date)
Name: Swarnali Haldar	
Title: Executive for Information Services/CIO (I)	
Contact information: 8601 Adelphi Road, Room 4415, College Park, MD 20740-6001 301-837-1583, swarnali.haldar@nara.gov	