Privacy Impact Assessment (PIA)

Name of Project: LL Reference Topic Log

Project's Unique ID: LL Reference Topic Log

Legal Authority(ies):	**44 USC 2110; 36 CFR 1202; 36 CFR 1256.20**

Purpose of this System/Application: The LL Reference Topic Log tracks all reference requests received by the Center for Legislative Archives. The system provides a means to report: number and type of requests; timeliness of response; time period of event being researched; method of response; volume of material supplied; and most requested records (for potential preservation and advanced description).

Section 1: Information to be Collected

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

Employees		Name of LL staff handling the request
External Users		None
Audit trail information (including employee log-in information)		None
Other (describe)		Data on LL researchers: name, contact information (which may include email and phone number), research topic, type of research, description of records pulled.

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)		N/A
State and local		N/A

agencies (list agency)		
Other third party source		The researcher provides LL staff with the information during the reference interview.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
Yes. LL is collecting data to analyze research trends, records needing more descriptive finding aids, high use items requiring holdings maintence or conservation treatment, underserved researcher groups, and timliness of response. Each data element contributes data required for that analysis.

2. Is there another source for the data? Explain how that source is or is not used?
There is no other source for this information.

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, the aggregation will not include any of the personal contact information. The aggregate data is not connected to specific researchers.

2. Will the new data be placed in the individual's record?
The name and contact information for the researcher will be used only to respond to the request. Once the contact information is no longer needed to respond, it will be separated from the record-related data and purged entirely every two years.

3. Can the system make determinations about employees/the public that would not be possible without the new data?
No.

4. How will the new data be verified for relevance and accuracy?
There is no process for verifying data. If reference responses are returned as undeliverable, LL staff will note that in the entry.

5. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
The 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.
Processes are not being consolidated.

7. Generally, how will the data be retrieved by the user?
The only users are LL staff and the NARA administrator responsible for compiling agencywide reference statistics. The NARA administrator responsible for gathering agency-wide statistics will only have access to date fields, and one unique ID field. LL staff can use Access's Find feature to locate a pertinent record. NARA's reference statistician pulls the only number of responses, not personal data about the requester or topic.

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.
Specific entries can be retreived by name. Access's Find feature allows LL staff to search all fields, including name. If questions arise about a specific researcher's request (has LL received it, were any records found, can the same records be pulled for another research visit, etc.) that request can be viewed by searching the name field.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
LL will not generate any reports 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?
The system is not web-based.

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)?
Only LL reference staff and the NARA administrator responsible for compiling agencywide reference statistics will have access to the system.

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?
LL's Assistant Director approves each person granted the system password based on reference need. When any personnel leave, the password is changed. Password authorization is not documented.

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

Authorized LL staff will have access to all fields. NARA's reference statistician will have access only to fields used to count number of written requests and timliness of response. The NARA administrator responsible for gathering agency-wide statistics will only have access to date fields, and one unique ID field.

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?

Each user is responsible for not misusing the system. NARA policy documents include formal guidance that establishes rules for use of IT systems and appropriate handling of privacy information in the records -- both historical records and NARA operational records. Guidance includes NARA directives, IT training courses, and notices regarding appropriate use of government IT equipment and handling of privacy information.

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 not involved.

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.

No.

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?
Each user. See question 4.4.

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 other agencies will have access to the system or its data without a court order.

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?
Researchers may refuse to provide contact information. In those cases LL staff prepare a response to the inquiry and wait to hear from the researcher again. Name and contact information are not required fields in the database.

2. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
There are no "negative determinations" in the system.

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.).
There is no mechanism for ensuring accuracy, timliness, or completeness of data.

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?
The system is only used in LL.

3. What are the retention periods of data in this system?
The personal data will be purged every two years. The remaining data will be destroyed when no longer needed.

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 personal data is authorized for disposal after two years per NARA Disposition Schedule N1-64-87-1, item 1421-1. The reports will be generated only for specific administrative analysis and will be disposed when no longer needed per NARA 203, 1421-3.

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?
No risk assessment as been performed. The data will be stored on the shared drive for the LL office, and access will be restricted based upon NARA's networking protocols, and LAN access mechanisms.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.
The database has been tested by the developers in LL, Brandon Hirsch and Adam Berenbak, and have ensured that information can be accessed only via direct access to the database file, which is secured by NARA's networking protocols and LAN access mechanisms, as well as password that is required to use the application.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
Brandon Hirsch, LL IT Specialist, 700 Pennsylvania Ave., NW, Washington, DC 20408.

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.
NARA 2, Reference Request Files

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.
No.

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?
None.

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

The Following Officials Have Approved this PIA	
System Manager (Project Manager)	
Brandon M. Hirsch (Signature)	1/3/14 (Date)
Name: Brandon Hirsch	
Title: IT Specialist, LL	
Contact information: 202-357-5350	
Senior Agency Official for Privacy (or designee)	
(Signature)	1/7/14 (Date)
Name: Gary M. Stern	
Title: General Counsel and SAOP	
Contact information: 301-837-3026	
Chief Information Officer (or designee)	
(Signature)	1.22.14 (Date)
Name: Michael Wash	
Title: CIO	
Contact information: 301-837-1992	