Privacy Impact Assessment (PIA)

Name of Project: IRS/DHS Consolidated Site

Project's Unique ID: Lee's Summit, MO

Legal Authority(ies):	**44 USC 2108**

Purpose of this System/Application: The system is a large index used to identify, maintain and track open OPF files stored at the Federal Records Center in Lee's Summit, MO. The system is used as a tool to provide reference service on the files for IRS and DHS. The systems reside on Sequel Servers using TAB Fusion software.

Section 1: Information to be Collected

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

Employees		Information about NARA employees who use the system to perform their jobs. The information includes name, login ID and password.
External Users		One user ID, Password for IRS personelists who have read only access allowing them to query the status of a record.
Audit trail information (including employee log-in information)		Changes to tracking information are identified with an employee number or name assigned to the staff member responsible for the action.
Other (describe)		

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

NARA operational records		When the IRS adds an employee, they provide the employee name, SSN, DOB and the Office where the employee is processed. The system can be queried on any of these data elements. Queries are for the purpose of locating or determining the status of a particular record or groups of records in a particular status. SSNs and DOBs are used to confirm the identity of employees.
External users		No public access to the system is available.
Employees		Employees are granted access because of their position and need to know. Access is granted to GS-5s for mailroom and batching responsibilities; GS-7s through GS-11 for duties ranging from mailroom responsibilities to creating reports, and labels to accommodate the growth of the collection.

Other Federal agencies (list agency)		IRS Personnellist assigned to the OPF consolidated site.
State and local agencies (list agency)		None
Other third party source		IT contractors who may have access in order to repair software or hardware are required to sign non-disclosure documentation. Documentation maintained in AFO-LS Administrative files.

Section 2: Why the Information is Being Collected

1. Is each data element required for the business purpose of the system? Explain.
Yes

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?
No

4. How will the new data be verified for relevance and accuracy?
No new elements are added

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?
User logs into the system and is validated by user ID and password. The user retrieves information by pre defined reports and queries. There is currently no option to capture log in information or attempts through the software program or through Sequel Server.

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.
Yes, queries can be based on any of the stated data elements.

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 created on individuals. The data are used to determine the physical location of the paper record. It is not possible to obtain reports by user only by the data elements in the system.

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. The system is used to assist the staff and IRS in locationg the records of the individual ONLY.

12. What kinds of information are collected as a function of the monitoring of individuals?
None

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?
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)?
Authorized NARA employees, IT repair contractors and IRS Personnellist

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 granted according to their duties and responsibilities by the IRS/DHS OPF Program Supervisor. Access and rights are documented in the system. Access is terminated by the NARA Program Coordinator when responsibilities change or the employee leaves NAR A employment. Access termination is accomplished by deleting the individuals name and ID information from the security portion of the application.

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

Users have access to all data. However, not all users have access to the corresponding files and conversely, not all staff who have access to the files have access to 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?

Employees receive annual PII training and receive periodic instruction not to browse in the system or make unneccessary queries.

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?

There is currently no hardware maintenance assistance or agreement. The software assistance is in the form of technical support only. If a technician is called to assist with the application in a hands on situation they are required to sign the non-disclosure agreement.

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?

No Interface

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.

IRS, who provides the data used in the IRS tracking system has limited (read only) access to the system. Access is controlled by the Con Site manager. The information is used to determine the status of the paper record. IRS/DHS provide the information by supplying a disc conatining new hire information. The information from the disc is downloaded and then the disc is returned to IRS. For DHS the disc is provided by overnight delivery and destroyed once downloaded. DHS have no access to the system.

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?

Information in the system is not provided by individuals, but by the IRS and DHS.

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

No determinations are made using the data.

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 is accepted from IRS/DHS at face value. IRS periodically reviews the data to insure accuracy. DHS has no access to the data once provided and downloaded. Accuracy, timeliness and completeness is only verified through the quality of reference service provided.

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?

Operated in ONLY one site.

3. What are the retention periods of data in this system?

Data tracks files that are current and open, therefore no disposition can be applied. IRS/DHS need to maintain a history of where the files have been so no data is purged from the systems. Inactive IRS files that have been forwarded to the NPRC or other agencies are often returned due to the seasonal workforce employed by the IRS. Their historical record is resurrected in the system and there is no loss of information even though the file was temporarily removed from the fileroom. Inactive DHS files are forwarded to DHS personnelist upon request. These files would be forwarded to the NPRC or to another agency by DHS and their history would reflect the withdrawal to DHS. If the file is returned the historical record is resurrected in the system and there is no loss of information even though the file was temporarily removed from the fileroom.

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.

N/A

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?
While no formal risk assessment has been performed, the system is a stand-alone system. It is not connected to the internet or the telephone system. It is located inside of an underground Federal Records Center.

9. Describe any monitoring, testing, or evaluating done on this system to ensure continued security of information.
Migrated system from Microsoft Access to Microsoft SQL Server format in 2/2007 to provide additional security options and monitoring.

10. Identify a point of contact for any additional questions from users regarding the security of the system.
Kristina Curtis, Assistant Director (816) 268-8118 or Sean Murphy, Director, Federal Records Center-Lee's Summit (816) 268-8149

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.
OPM # 1

2. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.
The system is NOT being modified

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)	
(Signature)	10/8/14 (Date)
Name: Sean P.Murphy	
Title: Director, Lee's Summit FRC	
Contact information: 816-268-8149 sean.murphy@nara.gov	
Senior Agency Official for Privacy (or designee)	
(Signature)	10/10/14 (Date)
Name:	
Title:	
Contact information:	
Chief Information Officer (or designee)	
Swarnali Haldar (Signature)	10/17/14 (Date)
Name: SWARNALI HALDAR	
Title: CIO	
Contact information:	