Initial Privacy Review Approval Document

1) **System Owner**

   _____ (Signature) _____(Date)

2) **Senior Agency Official for Privacy (or designee)**

   _____ (Signature) _____(Date)

3) **Chief Information Officer (or designee)**

   _____ (Signature) _____(Date)

Appendix B
Privacy Impact Assessment Template

Name of System:
System's Unique ID:

SYSTEM APPLICATION/GENERAL INFORMATION:

1. What is the purpose of the system/application?

2. What legal authority authorizes the purchase or development of this system/application?

DATA in the SYSTEM

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

- **a. Employees**
- **b. External Users**
- **c. Audit trail information (including employee log-in information)**
- **d. Other (describe)**

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

- **a. NARA operational records**
- **b. External users**
- **c. Employees**
- **d. Other Federal agencies (list agency)**
- **e. State and local agencies (list agency)**
- **f. Other third party source**

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

4. 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.)

5. Is there another source for the data? Explain how that source is or is not used?

ATTRIBUTES OF THE DATA

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?

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

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

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

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

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

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

8. Is the data is 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.

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

10. 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?

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

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

2. What are the retention periods for records in this system?

3. What are the procedures for disposition of the records 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 they cannot be destroyed or purged until the schedule is approved.

4. 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.

5. How does the use of this technology affect public/employee privacy?

6. 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.

7. What kinds of information is collected as a function of the monitoring of individuals?

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

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

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

10. Under which Privacy Act systems of records notice does the system operate? Provide number and name.

11. If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

<u>ACCESS TO DATA</u>

1. Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, other)

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.).

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

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)

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?

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 6.

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

8. Who will be responsible for protecting the privacy rights of the public and employees affected by the 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, state how the data will be used and the official responsible for proper use of the data.

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

_____ ___ (Signature) _____(Date)
System Owner (Please include name, title and contact information)

_____ (Signature) _____(Date)
Senior Agency Official for Privacy (Please include name, title and contact information)

_____ (Signature) _____(Date)
Chief Information Officer (Please include name, title and contact information)