Privacy Impact Assessment

Name of Project: Automated Collection Management Database (ACMD)

Project's Unique ID: ACMD (iO)

Legal Authority(ies): 44 U.S.C. 2108, 2109, 2111, and 2112; also NARA 101, Part 4.2.e.

Purpose of this System/Application: Presidential libraries and the Presidential Materials Staff (Washington, DC) use iO to document and manage their museum (artifact) collections in a systematic manner. Each organization creates and manages data about its own unique collections.

Section 1: Information to be Collected

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

a. Employees: Usernames and passwords are available for those employees with access to the system. Names would not be included among name authority records unless the employee gave a gift to the President or donated or loaned an artifact to a Library.

b. External Users: N/A

c. Audit trail information (including employee log-in information): iO tracks the username of the last user to modify a record as well as the username of the user who first created the record.

d. Other (describe): iO functions as a catalog for the museum collection, and also assists with managing certain museum processes (acquisitions, cataloging, location and condition histories, loans and exhibitions). iO also includes authority records: the "People Authority" (background information for 'donors', 'makers' (e.g. artists, authors or manufacturers of collection objects) or other individuals associated with the collections); "Publications Authority" (books and other materials with collection item citations); and "Keyword Authority" (controls keyword associations, optionally as part of a hierarchical thesaurus). Authority records may be linked to one or more catalog records as needed.

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

a. NARA *operational records*: N/A

b. External users: N/A

c. Employees: N/A

d. Other Federal agencies (list agency): For the iO system at the Presidential Materials Staff, which manages and stores material on courtesy storage for the White House, data regarding Presidential Gifts is imported from incumbent White House Gift Office.

e. State and local agencies (list agency): N/A

f. Other third party source: Entries into the system are directly composed into the system, often based on paper records describing the objects. For some Library's iO data, imports have been taken from archived White House and/or Presidential Materials staff data.

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?

Yes. The Presidential Libraries have paper records to document their artifact collections. Some Libraries also have archived data from the White House Gift Office.

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?

N/A

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?

Passwords and usernames are required to access the system. System users are validated and have permissions commensurate with their job responsibilities.

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?

At the individual workstation, the system has search and browse functions for retrieving data.

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.

Data is retrievable by a unique entry of the donor's name or other textual elements in the Name Authority records (alternate names, title or occupation, city/country or other address elements, occasionally a date of birth. As explained above, occurrences of both an address and a date of birth are seldom.

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 can report on which artifacts an individual or institution loaned, borrowed or donated to a Presidential Library or gave to a President. Museum staff uses these reports to manage the artifacts collections.

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

N/A

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?

No.

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)?

Limited NARA collections staff, system administrators, some contractors and interns and other individuals who's designated task is to support museum collections operations under NARA supervision.

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.).

The local iO SA (usually the Museum Registrar or Curator and/or FOSA) approves and manages user accounts and roles on the system. The system requires a username and password.

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

The system has three system roles: Managers may add records, edit records, and delete records. Staff users may add records and edit records, but not delete them. The Visitor role is for NARA staff that simply needs to view records in the catalog, but may not add or edit records. In addition, the acquisition and legal areas of the data may further be restricted by assigning field permissions to each of the roles.

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)?

System users (NARA staff) are validated and have permissions commensurate with their job responsibilities.

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?

The system is supported by NARA's IT contractor, and the Office of Presidential Libraries has a service contract with the vendor. There is not a Privacy Act clause in the support contract with the vendor. However, the vendor rarely works directly with sets of the data in ACMD (iO), but instead, supports functions at the system level. The Libraries use the vendor for getting instructions on how to run a particular kind of query or how to deal with an error message that might appear, for example.

The vendor signs a Confidentiality Agreement if they are contracted to do extensive work with the data, such as assist with migration of data from another system into ACMD (iO).

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 8.

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?

N/A

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?

N/A

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.).

Quality control is conducted at the discretion of the museum staff entering the information.

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?
There is a Data Standards Working Group that issues guidance on consistent use of the system and data. Although all of the Presidential Libraries use the same software, the data is not shared among sites.

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

The artifacts described in ACMD (iO) are records that have been transferred or donated 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.

See 2 above.

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?

It meets most of NARA's IT security requirements. For requirements that are

identified which are not currently met, a mitigation response will be developed and tracked through a POAM. .

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?

An updated risk assessment for iO was completed in FY 2010. Configuration settings and process controls were identified as items to be resolved and tracked through a plan of action and milestones.

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

A full assessment of the security controls for the iO system was completed in FY 2010. In addition, there are several tools used to continuously monitor security-related activity for iO, such as network and host based intrusion detection, log monitoring through a security information manager (SIM), and other monitoring agents that run on iO servers,

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

Kim Koons, iO System Owner and ISSO

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 3. Donors of Historical Materials Files.

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

The ACMD (iO) system is not being modified at this time.

Conclusions and Analysis

1. Did any pertinent issues arise during the drafting of this Assessment?

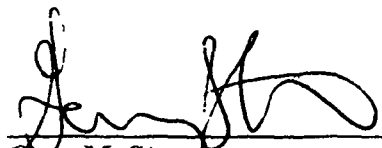
No.

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

The Following Officials Have Approved this PIA

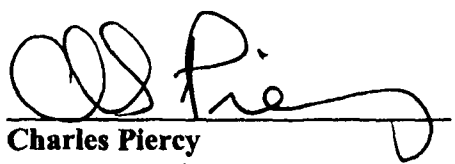
_____ (Signature) _____(Date)

Kimberly Koons
System Owner, ACMD (iO)
700 Pennsylvania Avenue, NW
Washington, DC
Room G7, A1
202-357-5082



_____ (Signature) _____(Date)

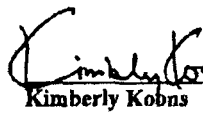
Gary M. Stern
Senior Agency Official for Privacy
8601 Adelphi Rd,
College Park, MD
Room 3110
301-837-2024



_____ (Signature) 9/30/2010(Date)

Charles Piercy
Acting Chief Information Officer
8601 Adelphi Rd,
College Park, MD
Room 4400
301-837-1583

The Following Officials Have Approved this PIA



(Signature) Oct 7, 2020 (Date)

Kimberly Kobns
System Owner, ACMD (iO)
700 Pennsylvania Avenue, NW
Washington, DC
Room G7, A1
202-357-5082

_____ (Signature) _____ (Date)

Gary M. Stern
Senior Agency Official for Privacy
8601 Adelphi Rd,
College Park, MD
Room 3110
301-837-2024

_____ (Signature) _____ (Date)

Charles Piercy
Acting Chief Information Officer
8601 Adelphi Rd,
College Park, MD
Room 4400
301-837-1583