

Privacy Impact Assessment

Name of System: NARA Donor/Gift Records Management System
System's Unique ID: NDEV

SYSTEM APPLICATION/GENERAL INFORMATION:

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

The NARA Donor/Gift Records Management System (NDEV) provides an application for tracking records of monetary donations to the National Archives Trust Fund and the Foundation for the National Archives. The information in the system facilitates the gift solicitation authority of the Archivist of the United States on behalf of the National Archives and Records Administration.

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

44 USC 2112(g)(1); 2305

DATA in the SYSTEM

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

a. Employees: Unique User ID and password

b. External Users: N/A

c. Audit trail information (including employee log-in information) – This system consists of three parts, the operating system, the database, and the application itself. Direct access to the database and operating system on the server is limited to System Administrators. Employees communicate to the server via a client installed on their workstation. The database account used by the client is a generic account, shared by all clients.

Audit trails at the database level and operating system level track System administrator access to the system. Audit trails, with regard to the application are limited to the creation and deletion of donor records.

Audit tools create, maintain, and protect a trail of actions of users and administrators that trace security-relevant events to an individual, ensuring accountability.

d. Other (describe) – Biographical and demographic information for individuals and organizations; background information, interests, affiliations and giving history for donations. The system also includes information on gifts and pledges and miscellaneous information about each gift.

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

a. External users – N/A

b. Employees – Create donor profiles, which include names, mailing address,

telephone numbers and financial data (amount of donation and method of remittance).

- c. **Other Federal agencies (list agency) – N/A**
- d. **State and local agencies (list agency) – N/A**
- e. **Other third party source – N/A**

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

User ID's and passwords are needed to ensure the security of the system and integrity of the data it contains. Personal information is necessary to solicit and track information concerning donors and prospective donors.

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.).

Data solicited from individuals is verified at the time of collection.

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

No.

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?

No

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

Data will be added to the individual's record when they make subsequent donations and attend events.

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

N/A

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

New data is verified at the time of collection.

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

Access to the system is controlled by the client software, which must be installed on individual workstations. Each user account is password protected with passwords that comply with NARA's password policy.

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?

Only internal access is authorized in NDEV. However, the system allows authorized employees to retrieve information by the name of the donor or prospective donor.

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, the data in NDEV can be retrieved by name. There is no collection of SSN's in NDEV.

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

Reports can be produced on individual donors. Such reports include the history of donations and/or gifts and information concerning pledges. This information will be used to process acknowledgement packages. There are three types of users of NDEV. Executive users can only view donor records. The development team can create records, add additional information to a donor record and enter gifts. The system administrator has all access privileges, including creating and deleting records.

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?

Submission of information by individuals is voluntary. Individuals choose to provide their personal information for inclusion in NDEV. If data is collected as a part of the information in Researcher application process, the applicable form offers the appropriate Privacy Act statement notifying the individual of how their information will be used. That information is also covered by a properly published Privacy Act system of records notice, NARA 1 Researcher Application Files

Information in NDEV, collected through other solicitation efforts, is covered by a properly published Privacy Act system of records notice NARA 33, Development and Donor Files.

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

N/A

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?

The NDEV system resides on a Microsoft Windows Internet Information Services (IIS) 5.0 production server with the Windows 2000 operating system. The server is located in the computer room at the Archives II, in College Park, MD. The server grants access to the application from NARA facilities in Washington, DC and College Park, Maryland.

The application provides the ability for authorized users to read, update, or add gifts to a record.

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

The records in NDEV are scheduled in accordance with N1-64-04-4, item 3b. Inactive donor and development files are cut off after two years. Inactive records are deleted after three years.

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.

See above. The disposition schedule for the data in the NDEV system was approved in April 2004, N1-64-04-4, item 3b.

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.

No

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

N/A

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.

N/A. NDEV is used to track NARA's donation records, not individuals.

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

N/A

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

The integrity of the data in NDEV is important to ensure fundraising management. The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification. Therefore security controls are in place to ensure separation of duties, least privilege (users are assigned only the minimum privileges to do their job), individual accountability, audit, discretionary access control and integrity. NDEV is also monitored by the agency's Network Intrusion Detection System. Since NDEV contains privacy data, it is also monitored by Host-Based Intrusion Detection Systems as well.

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

No

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

No.

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

This system operates under the NARA Privacy Act system of records notice NARA 33, Development and Donor Files.

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

There are no modifications to the system or Privacy Act system of records notice at this time.

ACCESS TO DATA

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

The system can be accessed by authorized users and the system administrator. Access in NDEV is allowed for the following users:

NDEV USERS AND ACCESS LEVELS	
USERS	FUNCTION
Executive	<ul style="list-style-type: none"> • View Donor Records.
Development Team	<ul style="list-style-type: none"> • Create Donor Records. • Add additional information to a Donor Record, provided that the record is not a gift. • Cannot delete records. • Enter gifts.
System Administrator	<ul style="list-style-type: none"> • All privileges, including Creating a Record and Deleting a Record.

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.).

NDEV system user accounts are set up following the “least privilege approach,” which assigns users with only the system privileges necessary to complete their job function as outlined in item 1 above. The system administrator is responsible for assigning access permissions. Criteria, procedures, and responsibilities regarding access are documented in the NDEV System Security Plan, Document Version: 1.0, December 2003.

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

User access in NDEV is restricted as outlined in item 1, above.

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.)

A User Responsibility Agreement applies to the users of NDEV. Among the rules of behavior outlined in this agreement are: warnings against attempts to gain access to any system or network to which the individual has not specifically been authorized to use and prohibitions against illegal, fraudulent or malicious activities. This agreement is outlined in the System Security Plan for NDEV. Copies available upon request.

NARA has implemented an agency-wide Security Awareness and Training program for their employees and contractors. The Security Awareness and Training program ensures that NARA system users are aware of their security responsibilities and how to fulfill them. The program includes security briefings, educational brochure(s), security awareness posters throughout NARA facilities, annual refresher training for information technology and security personnel, and a mechanism to track training received by employees and contractors. In addition, NARA system users can access various NARA IT Security publications via NARA Staff Only Intranet.

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?

NDEV is under operations and maintenance with NARA's IT operations contractor. There is no specific Privacy Act clause in their contract, but there is a general, non-disclosure clause in the contract that applies to all the Contractor's activities while under contract to NARA.

6. Do other NARA systems provide, receive or share data in the system? If yes, list the system and describe which data is shared.

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?

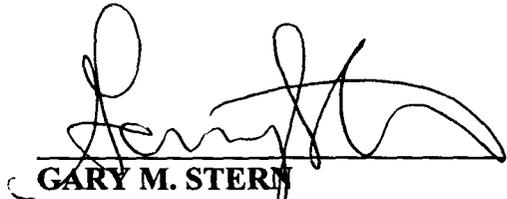
The system owner, system administrator and system users will be responsible for protecting the privacy rights through this interface. The Senior Official for Privacy is responsible for training and implementing NARA's privacy policies.

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.

N/A

The Following Officials Have Approved this PIA

 (Signature) 7/26/07 (Date)
MARVIN PINKERT
Director, Center for the
National Archives Experience (NWE)
Room G-9, AI
Phone: 202-357-5210

 (Signature) 7/25/07 (Date)
GARY M. STERN
General Counsel and
Senior Agency Official for Privacy (NGC)
Room 3100, AII
Phone: 301-837-3026

 (Signature) 7/28/07 (Date)
MARTHA MORPHY
Assistant Archivist for Information Services and
Chief Information Officer (NH)
Room 4400, AII
Phone: 301-837-1992