

Gift Registry PIA

1. Contact Information

A/GIS/IPS Director

Bureau of Administration

Global Information Services

Office of Information Programs and Services

2. System Information

- (a) Name of system: Gift Registry
- (b) Bureau: M/EDCS
- (c) System acronym: Not available
- (d) iMatrix Asset ID Number: Not available
- (e) Reason for performing PIA: Click here to enter text.
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
 - Yes
 - No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.
- (b) What is the security Assessment and Authorization (A&A) status of the system?

Gift Registry utilizes the Department's enterprise-wide SharePoint services, which have been vetted by IRM/IA and were granted iMatrix numbers 2741 and 2742.
- (c) Describe the purpose of the system:

To conform with 2 FAM 964 guidelines, the Office of Emergencies in the Diplomatic and Consular Services (M/EDCS) has provided an official format to facilitate entry and reporting of the gift registry. This form allows the gift officer to easily enter and edit gifts into the official Gift Registry. The registry must be maintained at post and in the bureaus and is retrievable from a central database.

The gift registry will account for all donations received on behalf of the Department of State or its regional bureaus or posts for the purposes of: 1) maintaining an historical

record, 2) properly allocating donations given for a particular purpose, 3) determining future solicitation and gift acceptance, and 4) providing donors with acknowledgment letters for tax purposes.

- (d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The system collects and maintains the full name, title, address, and relevant business affiliations of individual donors.

For corporations, foreign governments, foundations or other entities, a contact may be designated. The PII for that contact can include name and title.

The system uses addresses for the potential purposes of uniquely identifying an individual.

The system doesn't disseminate information, but users are able to export the information to spreadsheets which are intended to be shared at the post and regional bureau level.

- (e) What are the specific legal authorities and/or agreements that allow the information to be collected?

Foreign Service Buildings Act of 1926, Sec. 9, as amended (22 U.S.C. 300); State Department Basic Authorities Act of 1956, Sec. 25, as amended (22 U.S.C. 2697); Foreign Assistance Act of 1961, Sec. 695(d), as amended (22 U.S.C. 2395(d)); Migration and Refugee Assistance Act of 1962, Sec. 3(a)(2), as amended (22 U.S.C. 2602); Foreign Gifts and Decorations Act, as amended (5 U.S.C. 7342 and 22 CFR 3); Acceptance of travel and related expense from non-Federal Sources (31 U.S.C. 1353); and Mutual Educational and Cultural Exchange Act of 1961 (Fulbright-Hays), Sec. 105(f) and Sec. 108A, as amended (22 U.S.C. 2455(f) and 22 U.S.C. 2458(a)) 41 CFR 301 and 41 CFR 304.

- (f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

- SORN Name and Number: Official Gift Records and Gift Donor Vetting Records State-80
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): May 28, 2015

No, explain how the information is retrieved without a personal identifier.

[Click here to enter text.](#)

- (g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes No

If yes, please notify the Privacy Division at Privacy@state.gov.

- (h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? Yes No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-08-007-04
- Length of time the information is retained in the system: 5 Years
- Type of information retained in the system:

Per record Disposition schedule: copies of telegrams, letters, memoranda, general correspondence and other related material which pertain to monetary and real estate contributions to the U.S. Government. FMP is the principal support bureau, keeps all official records, maintains an automated database relating to such projects and authorizes acceptance of all donations.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes No

- If yes, under what authorization?

[Click here to enter text.](#)

(c) How is the information collected?

Management Officers at post enter in the information through a SharePoint site.

(d) Where is the information housed?

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

- If you did not select "Department-owned equipment," please specify.

[Click here to enter text.](#)

(e) What process is used to determine if the information is accurate?

Donor letters and/or checks are received for each gift received. Management officers will be entering in the names and addresses using these documents received directly from the donors. Only names and addresses are entered.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The system is recording names and addresses for a specific point in time; the name and/or address does not need to change if the donor's information changes.

(g) Does the system use information from commercial sources? Is the information publicly available?

No.

(h) Is notice provided to the individual prior to the collection of his or her information?

A donor form should be completed which contains a Privacy Act statement, thereby providing the individual notice when he/she completes the form.

- (i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? Yes No

- If yes, how do individuals grant consent?

- Click here to enter text.

- If no, why are individuals not allowed to provide consent?

- Individuals are choosing to donate gifts; they can choose to refrain from donating.

- (j) How did privacy concerns influence the determination of what information would be collected by the system?

Name and address are included to ensure propriety of donations and that a donor can be contacted if a donation is rejected or an acknowledgment letter needs to be sent for tax purposes. No additional information is collected.

5. Use of information

- (a) What is/are the intended use(s) for the information?

The full name, title, and address collected by the system are used only to identify unique donors.

The relevant business affiliations of individual donors collected by the system are used to ensure there are no conflicts of interest so that the gift can be accepted.

- (b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes.

- (c) Does the system analyze the information stored in it? Yes No

If yes:

- (1) What types of methods are used to analyze the information?

- N/A

- (2) Does the analysis result in new information?

- N/A

- (3) Will the new information be placed in the individual's record? Yes No

- (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

- Yes No

6. Sharing of Information

- (a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The information will be used by the Posts who capture the data and by M and M/EDCS who are the system owners. Outside of the offices in the Department of State responsible for collecting/tracking gifts, the information will not be shared.

(b) What information will be shared?

No information sharing occurs outside the offices responsible for collecting/tracking gifts.

(c) What is the purpose for sharing the information?

N/A

(d) The information to be shared is transmitted or disclosed by what methods?

N/A

(e) What safeguards are in place for each internal or external sharing arrangement?

N/A

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed? N/A

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

As the information collected is for basic contact of an individual, it is not necessary to allow the individual access to it. The individual would not need to access it, as he/she already knows his/her contact information.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes No

If yes, explain the procedures.

[Click here to enter text.](#)

If no, explain why not.

The individual is the supplier of information. The individuals are the donors and the information being captured is entered into the system by DOS users at Post. The donors do not have access to the Gift Registry system. Not having access to his/her information would not result in any detriment to the individual.

(c) By what means are individuals notified of the procedures to correct their information?

See section 7(b).

8. Security Controls

(a) How is the information in the system secured?

Records are viewed only by the users who created them. All users must be authenticated Windows users on OpenNet and are, thus, subject to the enterprise-wide controls inherent to all users of the Department of State network. The view that is exposed to users at Post

contains a SharePoint filter that programmatically excludes any data records that were not entered by the user.

Records are accessible by MEDCS users. MEDCS users are able to view all records. S/ES-IRM system administrators also have access to all data to provide administrative support.

- (b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

SharePoint built-in mechanisms grant access to M/EDCS users through the M/EDCS Security Group. If a user transitions out of M/EDCS, their name will be removed from the security group, and they will no longer have access. If they leave the Department, they will no longer have access to the network or a Windows account on OpenNet through which to obtain access. All other users can only view records they created.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Users will only be able to see records they have created.

- (d) Explain the privacy training provided to authorized users of the system.

All users are given cyber security awareness training which covers the procedures for handling Sensitive But Unclassified (SBU) information, including personally identifiable information (PII). Annual refresher training is mandatory. In addition, all Foreign Service and Civil Service employees and those Locally Engaged Staff who handle PII are required to take the Foreign Service Institute distance learning course, PA 459, instructing employees on privacy and security requirements, including the rules of behavior for handling PII and the potential consequences if it is handled improperly.

- (e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? Yes No
If yes, please explain.

System requires Windows authentication, which is only granted to authorized employees of the Department of State.

- (f) How were the security measures above influenced by the type of information collected?

Users should not be able to access donation information from other posts or regions, but since this information isn't consistently retained, users were restricted to viewing only their own records. Since only authenticated users should be allowed in the system, SharePoint's use of Windows authentication was leveraged.

9. Data Access

- (a) Who has access to data in the system?

M/EDCS has full access to all records created. All other users will only be able to access the records they have entered.

- (b) How is access to data in the system determined?

Access to data in the system is determined through the use of SharePoint security groups.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? Yes No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Authenticated users outside of M/EDCS will only be able to access records they have created.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

This site is a SharePoint site that uses Windows authentication to determine whether a user is a member of M/EDCS. All other users will only be able to view information they entered themselves.