PRIVACY IMPACT ASSESSMENT

Online Museum Website for the Diplomatic Reception Rooms

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Date of completion of this PIA: December 3, 2021
(b) Name of system: Museum Website for the Diplomatic Reception Rooms
(c) System acronym: DRR website
(d) Bureau: Management (M/FA)
(e) iMatrix Asset ID Number: 321138
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable): N/A

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The Diplomatic Reception Rooms at the Department of State is a place where visitors learn about America's national history, the importance of diplomacy, and the Department of State. The system, a national museum website for the Diplomatic Reception Rooms, will offer its visitors a rich and immersive experience. Visitors who express an interest can sign-up for updates and educational programs on the site. They can also sign-up for tours or donate by accessing links on the website that will redirect them to other sites that process these requests. The purpose of this website is to connect with audiences in ways

that are relevant, timely, and tailored to their specific interests. Collecting PII allows members of the public to access social benefits in the museum's updates, educational programs, tours, and philanthropic opportunities and is important to the Department's public diplomacy.

The Office of Fine Arts (M/FA) will protect the privacy of its online visitors by identifying and collecting the minimum amount of PII required to execute its critical mission of effectively communicating with its audiences. Generally, M/FA does not collect PII about its visitors when they visit our website, unless they choose to provide such information to us. Submitting PII through our website is voluntary. By doing so, the visitor is giving M/FA permission to use the information for the stated purpose.

If the visitor chooses to provide PII on the DRR website, through such methods as completing a web form, M/FA will use that information to help provide that visitor the information or service they requested or to respond to their message.

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

Sign Up for Communications: The Diplomatic Reception Room website collects only email address voluntarily provided by individuals who express an interest in signing up for communications (emails, newsletters, announcements, and programs). This information is collected through a Google form and imported into Salesforce.

Donate Now: Individuals who would like to donate to the Diplomatic Reception Rooms may do so by visiting pay.gov, which they will access through an embedded link in our website that redirects visitors to pay.gov hosted by the Commerce Department. The DRR website does not collect donor information through the DRR website.

Register for a Tour: People may also register for tours by visiting the Tour Office managed by A/OPR/GSM through a link embedded in the DRR website that redirects visitors to Salesforce where Diplomatic Security collects: full name, email, phone numbers and for those wishing to tour the Diplomatic Reception Rooms, other information that identifies visitors personally such a citizenship, date of birth, and government-issued identification. The museum collections are visited by U.S. and non-U.S. citizens alike, and the Bureau of Diplomatic Security records citizenship, date of birth, and government-issued identification for all persons entering the Harry S Truman building. Valid identification includes passport, military identification, driver's license or identification card, alien registration card, permanent resident card, and/or Department of State issued diplomatic card.

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

- Sections 1 and 47 of the State Department Basic Authorities Act of 1956 (22 U.S.C. 2651a and 22 U.S.C. 2713) 5 U.S.C. 301
- Omnibus Diplomatic Security and Antiterrorism Act, 22 USC 4802(a)

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

☒Yes, provide: Individual Name

- SORN Name and Number:
  Digital Communication and Outreach, STATE-79

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  01/27/2016

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

(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 Office 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 (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)): A-03-003-04
- Disposition Authority Number:
  - Pending approval.
  - DAA-GRS-2013-0005-0004 (GRS 3.1, item 020)
- Length of time the information is retained in the system:
  - Museum Operations and Program Support Files (pending approval): Temporary. Cutoff at the end of calendar year or final action. Destroy 20 years after cutoff.
  - Information Technology Operations and Maintenance Records: Temporary. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.
- Type of information retained in the system:

Copies of records made available via a web site. Website administration including frames, templates, style sheets, site maps, codes that determine site architecture, change requests, site posting logs, clearance records, requests for correction of incorrect links or content posted, requests for removal of duplicate information, user logs, search engine logs, and audit logs.

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) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☐No ☒N/A

- If yes, under what authorization?

(d) How is the PII collected?

The Office of Fine Arts (M/FA) operates a museum at the Department of State. Visitors go to the website (diplomaticrooms.gov) where they may voluntarily choose to sign up for further communications. The website will collect information from the individual user through Google Forms, a survey administration software that DRR will manage through the FAN owned and operated Google platform for State Department. That information is collected within the Google system and can be exported as a .csv or .xls file. A member of the DRR team will export that file and manually import (upload) it into Salesforce on a monthly basis. Salesforce is the Department's enterprise contact engagement platform. PII is stored in the Department's Salesforce platform, not on the DRR website.

Salesforce provides contact management, event planning, and email marketing capabilities in a way that is intuitive, accessible, and secure. Salesforce provides the field and domestic offices a unified, consistent way to manage Department contacts to support strategic outreach and engagement efforts.

(e) 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.

Salesforce runs on a FEDRAMP-certified cloud.

Agency Authority to Operate (ATO): The Salesforce environment managed by the R Family (Salesforce Enterprise, iMatrix #7455) secured an agency ATO from the Department's Office of Information Assurance (IRM/IA) in February 2018 to store Moderate-level data, such as PII. Salesforce has prepared the paperwork for a FedRAMP high certification and is currently going through final approval expected for August 8, 2022

As part of the approval to operate (ATO) assessment of Salesforce, the CRM Office completed a Privacy Impact Assessment (PIA) that outlines the data categories and values captured in Salesforce. The PIA was approved and published on December 30, 2020, by the Department's Privacy Office as part of the ATO package.

(f) What process is used to determine if the PII is accurate?

If a visitor chooses to provide PII on the DRR website, that information will be used to help provide the visitor the information or service they have requested or to respond to their message. Accuracy of PII depends on the visitors themselves since visitors have accounts through which they can manage their subscriptions profiles and/or cancel their subscription at any time. The information is not cross referenced via any other external source for accuracy.

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

To ensure information stays current, M/FA will maintain steady communications with online audiences while also making it easy to unsubscribe. In Salesforce, our administrators will deactivate all user emails that are returned to M/FA as undeliverable. Thus, the responsibility to keep information current falls on the individual.

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

No. The system does not use information from commercial sources. The information is not publicly available.

(i) How was the minimization of PII in the system considered?

The minimization of PII was considered during the analysis phase of the system design where it was determined that social security numbers wouldn't be necessary for updates, or educational workshops programs.

5. Use of information

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

The information collected is used to provide users with the information or service they requested or to respond to their message. Activities include signing-up for updates or educational workshop programs. The information received from visitors varies based on what they do when visiting the site.

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

Yes. If a visitor provides us with PII on the DRR website, we will use that information to provide them the information or service they requested or to respond to their message. The information we may receive from visitors varies based on what they do when visiting our site.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:
(1) What types of methods are used to analyze the PII?
(2) Does the analysis result in new information?
(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

(d) If the system will use test data, will it include real PII?

☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal: M/FA will email the Google Form, containing email addresses only, to the IRM Help Desk to upload those email addresses to Salesforce.

External: N/A

(b) What information will be shared?

Internal: M/FA will email the Google Form, containing email addresses only, to the IRM Help Desk to upload those email addresses to Salesforce. This information is not stored in the new museum website.

External: N/A

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

Internal: The information will be shared with the Department's IRM's Help Desk only for purposes of bulk uploading contacts to Salesforce which reduces manual error and saves time for M/FA's administrative staff.

External: N/A

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

Internal: M/FA will email this information to IRM via their state.gov email addresses. The website is not involved in this transmission of PII.

External: N/A

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

Internal: The PII data, which in this case is subscriber email addresses, is encrypted. In addition, M/FA is staffed by cleared employees, who have completed periodic background checks, received cyber security training, and were granted access by executive leadership.

External: N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes. A Privacy Act statement is displayed on the website prior to the collection of a subject's information, explaining why this information is collected, the authorities for

collecting it, a description of the Department's sharing of the information, and whether providing the information is mandatory or voluntary.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII? ☒Yes ☐No

Yes. Generally, the Department does not collect PII about a subject's visit to the website, unless they choose to provide such information. Subjects have the opportunity to decline to provide the information, and many choose to decline. However, failure to provide this information may result in the inability to receive the requested service(s).

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

SORN State-79 contains procedures that allow individuals access to their information stored in Salesforce. Individuals who wish to gain access to records pertaining to themselves should write to Director, Office of Information Programs and Services, A/GIS/IPS; 2201 C Street, N.W.; Room B-266**;** Washington, DC 205208.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

For external subscribers an updated profile link is provided in the email notification allowing the option to update, correct their information and email address, or unsubscribe from future communications at any time. Also, individuals who wish to amend records pertaining to themselves can write to the Director, Office of Information Programs and Services, A/GIS/IPS; 2201 C Street, N.W.; Room B-266**;** Washington, DC 205208.
If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

Subscribers are notified of the procedures to correct their information at the end of all email communications from the M/FA. In addition, subscribers, who have voluntarily elected to receive email communication and have provided email addresses for that purpose, will receive an automated email that allows them to correct their information. All email communications will include options so that online visitors can amend their information by contacting our office and unsubscribe from future communications. Additionally, SORN State-79 provides notice of the procedures for correcting information.

8. Security Controls

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

This system relies on the inherent security controls native to the Department's Open Network (OpenNet). In lieu of single sign-on, the system requires a username and password which prevents unauthorized users from accessing the data.

The focus on information security is critical to public trust and confidence. However, security controls are not a one-time process and require a continuous cycle of monitoring to protect confidential information.

Effective system security starts with the Department's employees, including direct hires and contract personnel, who adhere to the Department's ethical behavior and codes of conduct. Safeguards include:

(a) Continuous Monitoring on Government-Owned Equipment: Employees acknowledge that, by accepting and using a username and login, users have agreed to follow all applicable laws and regulations, maintain account security, report any unusual behavior, only access the system from trusted computers or networks, and meet all requirements outlined in 12 FAM 623.1 and 12 FAH-10 H-112.1-4 when accessing the system.

(b) System Controls for Government-Owned Equipment: When using government owned computers for remote access or remote processing of Department data, users must implement basic home security controls, to include deploying a firewall, anti-spyware, antivirus, and file destruction applications. Upgrades/updates to these applications must be kept current. Further, security patches for operating systems and applications must be applied as soon as possible. Information on firewall, anti- spyware, antivirus, and file destruction software can be found on the DS/SI/CS Home Use Web page.

(c) Single Sign-On and Multifactor Authentication: Okta is also required for accessing Salesforce. Okta is a Department of State single, integrated platform that offers secure access to Department of State (DoS) applications and information. Okta provides single sign-on and multifactor authentication to DoS cloud applications.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Access to PII is limited to Department personnel, including direct hires and contract personnel, who have undergone background security investigations. Working on OpenNet, where access is restricted by multifactor authentication and training is compulsory, personnel are accountable for security infractions and violations arising from PII data breaches. Roles with access to the system include the following: Users (all PII), System administrators (email address), and Database administrators (no PII).

- Users – Users are responsible for communicating directly with those who have expressed an interest in receiving further communications and/or services (emails, newsletters, and education workshop programs) and voluntarily provided M/FA with their details. They can view all PII mentioned in 3(d) as needed for their assigned cases.
- System administrator – System administrators are responsible for the upkeep, configuration, and reliable operation of the DRR website and Salesforce. System administrators create the accounts that access this system. System administrators have logon identifications associated with their name that allows for user auditing. System administrators only have access to applicant email address.
- Database administrators – Database administrators (DBA) are responsible for the daily maintenance, upgrades; patch/hot fix application, backups, and configuration to the database. DBAs have limited backend access and are unable to view any PII.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Access to the DRR website and its salesforce instance is restricted to approved personnel. An executive-level director, the system owner, and information system security officer will review admin user accounts annually and determine whether system access is required in the performance of their official duties. Only those employed by the Department, including direct hires and contract personnel, are considered for system access, since they have completed background investigations, taken PS800 cybersecurity awareness, and agreed to comply fully with Department policies and regulations concerning PII. Internal access controls are assigned in a least-privilege manner to ensure that only personnel who have access to the information are those with a need to do so to perform their official duties.

(d) How is access to data in the system determined for each role identified above?

Access to the data in the system is determined by assignable permissions based on a need to know to perform job functions.

- Users – Access to this system is restricted to cleared DoS direct hire and contractor employees. DoS employees and contractors receive their access by requesting access from leadership in the Office of Fine Arts as well as in the Bureau of Administration in compliance with internal policies.
- System administrator –Access to Salesforce is restricted to cleared DoS direct hire and contractor employees. They will access Salesforce and DRR website through their fan.gov accounts. This requires a two-factor authentication granted by the system administrator.
- Database administrators – Access to Salesforce is restricted to cleared DoS direct hire and contractor employees. They will access Salesforce and DRR website through their fan.gov accounts. This requires a two-factor authentication granted by the system administrator.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

Access to the system is restricted to Department personnel, who have agreed to follow all applicable laws and regulations, maintain account security, report any unusual behavior, only access the system from trusted computers or networks. In addition, system administrators who have at least a need to know and have been approved by the system owner and the executive-level director have access to the data. System administrators have access only to their applicable subset of data as required by their job function.

The level of access granted to this system restricts the data that may be viewed and the degree to which data may be modified. Administrative activity is monitored, logged, and audited. The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include object created, object deleted, object modified, object rights modified, and custom access level modified. The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data. Internal and external access safeguards (i.e., firewalls, intrusion detection devices, etc.) are employed to identify and prevent unauthorized access by outsiders that attempt to access the system, or cause harm to, the information contained in the applications. The audit logs from these devices are automatically consolidated, summarized, and reviewed by the cloud service provider. Department access information is logged and audited periodically. Any field history tracking is enabled for six months.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

There is no specific role-based training. Personnel are trained annually during the Department's PS800 - Cybersecurity Awareness course which has a privacy component. This training is required prior to providing access to the system and at least annually thereafter. Every two years, personnel are also required to complete PA318 - Protecting Personally Identifiable Information.