PRIVACY IMPACT ASSESSMENT

Online Auction

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: 7/21/2021
(b) Name of system: Online Auction
(c) System acronym: OA
(d) Bureau: Bureau of European Affairs (EUR-IO/EX)
(e) iMatrix Asset ID Number: 231452
(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:

Online Auction is an online bidding tool for Post auctions. Online Auction increases the sales exposure of Post's excess goods and make the process more efficient for General Service Officers (GSO). It meets this goal by providing a cloud-hosted environment that the public can access, providing a sophisticated but easy to use interface for auction customers, and providing auction controls and auction reporting for post administrators. Sales of excess goods can provide a significant revenue stream for the Department, however there is significant effort required in the logistics of selling an item to the public. Online Auction facilitates those logistical steps and makes the process to create marketing material and advertise sale items more efficient. This system does not take direct payments but produces an internal report showing auction winner, item sold, and sold amount for the purpose of validating the winner and payment due at the time of pickup.

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

- First and last name
- Phone number
- Email addresses

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

22 U.S.C.§2581 General Authority of Secretary of State;
22 U.S.C § 2651a Organization of Department of State;
OMB M-10-06, Open Government Directive, December 8, 2009;
31 U.S.C. § 901-902 Agency Chief Financial Officers;
Presidential Memorandum to the Heads of the Executive Departments and Agencies for Transparency and Open Government, January 21, 2009;
41 U.S.C. §§ 121(c), 545 Disposal of Surplus Federal Property.

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

☒ Yes, provide:

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

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  January 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)):
  1) B-02-005-01
  2) A-03-005-05

- Disposition Authority Number:
  1) DAA-GRS-2016-0016-0001 (GRS 5.1, item 010)
  2) DAA-GRS, 2017-0003-0002 (GRS 5.2, item 020)

- Length of time the information is retained in the system:

  1) Temporary. Destroy when business use ceases.
  2) Temporary. Destroy upon verification of successful creation of final document or file, or when no longer needed for business use, whenever is later.

- Type of information retained in the system:
  Name, Phone number, and Email Address.

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 information collected for this system is obtained directly from the user via the system's registration form, U.S. Embassy Online Auction, which includes a Privacy Act Statement. The information from the registration form is automatically uploaded into the system once the applicant submits it.

(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.

Although the information is not housed on Department-owned equipment, it is housed on the equipment of a contractor working directly for the Department of State in the Microsoft Azure Commercial Cloud. The equipment utilized by these contractors has been screened and vetted by Department security specialists to ensure that they meet minimum requirement standards as established by FEDRAMP and NIST 800-86. These servers are also re-vetted for security standards every three years as required for all Department owned equipment to obtain an authority to operate.

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

The accuracy of the information is the responsibility of the individual entering it. The information entered in Online Auction is obtained directly from the individual during the registration process.

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

Yes, the information is current. Responsibility to keep information current falls solely on the individual. Users can log into the system any time to ensure that profile and bid information is current.

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

The system does not use any information from commercial sources nor is publicly available information used.

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

The Application Development Group (ADG) team carefully consulted Posts on data usage and need. The minimum amount of information required to conduct and complete an auction was defined for collection by the system based on its requirements. These are the only data points that are collected and stored in the system due to this analysis and determination. Thus, the amount of PII collected is minimized to the extent needed to fulfill the system's function.

5. Use of information

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

The intended use of the PII listed in 3(d) is to facilitate bids and to buy (by awarded bid) items being sold by auction to the general public.

(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. The system is designed to use the PII to identify an awarded bidder and to facilitate the sale and transaction of the purchased item. The information collected is necessary and kept solely so the system can perform the functions that it was designed for. No collateral uses exist for the information collected by the system.

(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.

The system uses test data in the development sandbox. The test data does not use real PII.

6. Sharing of PII

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

Internal:
The PII elements listed in 3(d) will be shared with the General Services Office (GSO) and the Financial Management Cashiers Office at Post.

External:
No information will be shared outside of the Department of State.

(b) What information will be shared?

Internal:
All PII elements described in 3(d) are shared with GSO and FMO-Cashiers Office at Post:

- First and last name
- Phone number
- Email addresses

External:
No information will be shared outside of the Department of State.

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

Internal:
Information is shared with the General Services Office (GSO) and the Cashiers Office at Post via a Winners Report, Sellers Report and Lot Report for the purpose of identifying auction winners, items won, and amount owed at time of pickup, these reports may also be used to send the status of items sold and the US dollar amount for each auction lot proceeds.

External:
No information will be shared outside of the Department of state.

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

Internal:
Information is disclosed via OA reports (Winners Report, Sellers Report and Lot Report) generated in the administrative interface of the application. The information can be exported and then emailed or printed to be shared with GSO and the Cashiers Office at Post.

External:
No information will be shared outside of the Department of state.

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

Internal:
Safeguards for sharing the information are: physical copies are sent via sealed and labelled inter-office mail and emails are marked and sent SBU or SBU - Privacy PII in accordance with Department requirements

External:
No information will be shared outside of the Department of state.

7. Redress and Notification

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

Before an individual can register for the system, an approved Privacy Act statement (PAS) appears on the first page. Once registered, the Privacy Act statement is provided at the bottom of each Post auction page. This PAS provides the applicant with notice of what authorizes the Department to collect this information, why the information is being collected, with whom the information will be shared, and whether the information is mandatory.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒ Yes ☐ No

If yes, how do record subjects grant consent?

There is a Privacy Act Statement on the form and record subjects provide consent by submitting the U.S. Embassy Online Auction form. Failure to provide the information may result in the inability to receive the requested service.

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

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

Record subjects have an active log-in to their online accounts. Individuals with accounts can access their information at any time to make edits and updates. Users can update this in their user profile at any time through the help key to correct their information.

Additionally, record subjects can gain access to their information by contacting the Department's Office of Information Program Services for copies of the records retained. Details on this process can be found in the System of Records Notice, STATE-79. Notice of these procedures is provided to the record subject in the Privacy Act statement included on the registration form, U.S. Embassy Online Auction.

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

☒ Yes ☐ No

If yes, explain the procedures.

Correction procedures are the same as those discussed in 7(c). Individuals have access to their profile in the system and can edit their information at any time. Also, within the constraints of an individual auction, users may edit their specific bids. There is a blue help button located in the bottom right corner for users. Users also can submit tickets for ADG Support through Zendesk which is located in the same area as the help button.

If no, explain why not

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

Procedures on how to correct information are provided to record subjects on the site after they register and create a profile. The blue "Help" button remains visible on the page as users navigate through the site, available for users to select at any time.

8. Security Controls

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

Azure (FedRamp Cloud) uses Transparent Data Encryption (TDE) which encrypts the databases, backups, and logs at rest without any changes to your application. Information is sent by Secure Sockets Layer (SSL). Information is protected through the use of FIPS 140-2 approved encryption mechanisms such as SSL 3.0, TLS 1.2 encryption for data-in-transit and inherited OpenNet encryption standards. Furthermore, only administrators with a "need to know" have rights to the system.

(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).

Role	Function	Rights
System Administrator	The System Administrator is responsible for managing the system. Members in this group include ADG developers and support staff. The system administrator will define rights, system trouble-shoot, and run audits adding designated trusted individuals to an Auction Administrator group.	The System Administrator can: • Manage system roles • Grant and remove an Auction Administrator • Run audit and security checks • Manage and monitor application health in production. • Create/edit a Post • Can see users' PII information (name and email)
Auction Administrator	Auction Administrators manage a specific Post(s) which has/have been assigned to the account by a System Administrator. Auction Admin can only see and edit Posts to which the account has been given permissions.	The Auction Administrator can: • Edit a Post • Create/Edit an auction • Add/Edit/Remove an item in the auction • Generate Reports for auction(s) only in their Post(s).

		• Retract a bid and provide a reason for the bid retraction. • Enable/disable user accounts, providing a reason for disabling.
Lot Manager	Lot Managers manage lots within their own Post.	The Lot Manager can: • Create or Edit an item. • View bidding history for an item.
User	A user can see Posts with auctions in preparing or active state. When the auction is active, the user can view an item and if logged on, the user can place a bid.	The User can: • Register an account for OA. • Subscribe to one or more Post auctions. • Submit bids for lots in Posts to which the user has subscribed. • See their own 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.

Users must confirm the email address on file before they can register for an account to access their own profile information and subscribe to an auction to place a bid.

Only a System Administrator approved by Post management can authorize Auction Managers and Lot Managers to access the Administrative Control Panel and the data within. Administrators also remove authorization once a request is submitted through Zendesk.

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

- System Administrators - Grant and remove Auction Managers and Lot Managers' access to the system. As such, system administrators will maintain full administrative access to the system.
- Auction Managers - Controls and manages the Online Auction application at the post level. The auction manager is mainly responsible for creating new auctions and their configuration. During the auction, the auction manager periodically observes and controls the auction process and can retract a bid and/or suspend a user as needed. The auction manager can view, print, and export the auction reports (winners, lots, and sellers). The auction manager must start the prepared and scheduled Auction. The auction manager also has the same access as lot manager.
- Lot Managers - A lot manager controls and manages all the lots in an ongoing or future auction. The lot manager controls how the lots appear on the auction web site by uploading lot information and images. The lot manager sets the values that control the

bidding process: the start price, maximum number of bids, and minimum and maximum and bid increases.
- Users - Access is automatically granted when individuals confirm their email address via an email notice sent to the user email on file. User access includes the ability to access their profile information and the ability to subscribe to an auction to place a bid.

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

OA uses role-based schemes for access management by leveraging the roles established in Azure Identity & Access Management at the platform level. Changes to pre-defined roles or the creation of additional roles are managed through a change control process and cannot be configured.

OA application actions that include data changes are maintained in the system audit logs and available for review by the OA system administrators. For security or access actions, an audit log is available for review by the System Administrator via the Azure Application Insights audit log.

List of audit events that should be recorded are as follows, where applicable: changes in user access permissions, data extractions, specific actions such as reading, editing, and deleting records or fields, change in file access, transaction log details, server log details, etc.

(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. All roles that have access to PII in the system must take the annual mandatory security training PS800 Cyber Security Awareness as well as the biennial mandatory privacy training PA318 PII.