Privacy Impact Assessment
for the
Foreign Service Officer Bidding System (FSOBS)

April 2023

Contact Point
Truc Dao Nguyen*
Project Manager
(202) 690-3358

Reviewing Official
Carol Remmers*
FAS Privacy Officer
(202) 384-4487

*Original Signatures on File in Cyber Security Assessment and Management (CSAM)

Abstract

The Foreign Service Officer Bidding System (FSOBS) is used by Foreign Service Officers (FSO) when they transition from overseas posts, their previous positions become open for bidding. Bidding is held in several rounds. The FSOBS provides a web-based e-Authentication platform to create bidding rounds, and enter and manage bids for post positions. This PIA is being conducted as part of security assessment and authorization process.

Overview

The foreign Service Act of 1980 sets out certain requirements for the Career Foreign Service Officers in terms of their Domestic and Overseas Tour of Duty. As per those terms, the FSOs have 2 to 5-year limit on their current Overseas assignments before they need to be rotated out to either another overseas post or to a domestic assignment. This rotational onward assignments for officers are determined through a bidding-and-paneling process that culminates with an assignment. The objective of the process is to assign officers to positions for which they are qualified and available, in reasonable anticipation of vacancies, in a manner that is responsive to the needs of the Service and considers the career needs and personal preferences of the officers. The online application used for this purpose is called “FSO Bidding” Application.

The FSO Bidding application requires the biographical information of the bidding Foreign Service Officer, along with their Position preference and a supplemental statement for a successful bid round. The biographical information such as the bidder’s current position and post, their foreign language scores, previous assignments, educational qualification and citation and awards. The source of this data is the agency’s iMART application and is being programmatically shared with the FSO bidding application. The bid preference and the supplemental statement is directly entered into the system by the bidder.

Typically, the main bid round is opened in the system during the fall season of the year, and additionally 1 or 2 “mini-bid rounds” are conducted to fill all overseas and domestic positions that were not assigned during the main round. The bidding process is concluded, when the OFSO committee meets and issues their position placement recommendations to the agency.

The bidding application is a web application developed using Microsoft Dot Net framework and is deployed on Windows Operating system hosted in DISC managed data center. It uses SQL Server for the data store and Department’s e-Authentication system for Identity and authorization. The User interface of the application is developed using Angular-Js.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

The application collects the bid preferences from the FSO along with supplementary statement that justifies why the FSO is the right choice for the position he or she is bidding for. Along with this information, the system also maintains the applicant's education, language scores, previous Washington DC and overseas assignments including assignments to hardship posts and citation and awards.

1.2 What are the sources of the information in the system?

The applicant's profile data such as their education data, citation/awards data, previous overseas assignments and their language scores are being pulled in from iMART system. The applicant's bid preferences and supplementary statements are gathered from the applicants through application data entry screens.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information collected by the system will be used by the FAS Program Area, Foreign Affairs (FA) Management Council to recommend job placements for the Foreign Service Officers to overseas posts.

1.4 How is the information collected?

Part of the information is obtained by reading posts and position related data from iMART system. The rest of the information is provided by the users of the system.

1.5 How will the information be checked for accuracy?

The supplementary data provided by the Foreign Service Officers is validated by FA. The accuracy of the remaining data is determined by iMART system and is also manually verified by FA.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Provisions for bidding are outlined in the contract with AFSA.

1.7 Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

FSOBS collects the following: employee name, biographical information such as the bidder's current position and post, their foreign language scores, previous assignments, educational qualification and citation and awards. The system uses no employee or other information. Data is date and time stamped and only authorized users have access to the data. Data is maintained at DISC in Kansas City and has been assessed and authorized at the Moderate risk category which is sufficient for the data. All FAS PII systems are encrypted at rest and in transit.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The data collected through the application is used by Foreign Affairs management council to recommend placement of Foreign Service officers to vacant overseas posts.

2.2 What types of tools are used to analyze data and what type of data may be produced?

The data collected through the application is used to generate various printable reports. The data is also used to populate form FAS-193 in PDF format and is used to create a Briefing Book used by the FA management council for their position assignment recommendations.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The system does not use publicly available data.

2.4 Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The application uses e-Authentication and role-based access to allow only authorized users. The user's data is further segregated, such that they will not be able to see each other's data.

Section 3.0 Retention

3.1 How long is information retained?

Records are maintained for a minimum of 1 year as defined by NARA records management policy. System backup and storage of the data is provided by DISC consistent with NARA and USDA policy for data retention.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

FSOBS as child system of the MDA System, has undergone a Moderate level assessment and authorization process and consistent with FISMA, NIST, NARA, and USDA guidelines and has been authorized to operate at the Moderate system categorization level.

3.3 Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

All risk associated with data retention are addressed and have been mitigated in the System Security Plan and the Contingency Plan for the MDA/FSOBS.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The information collected by the application is shared with FA Management Council. The shared information consists of the FSO bid preferences, supplementary statements from the FSOs, and actionable reports that the council could use to make placement recommendations.

4.2 How is the information transmitted or disclosed?

The information collected through the application is used to format and print form FAS 193 in pdf format. The printable forms are aggregated into a briefing book, along with other reports such as Post-Position assigned/unassigned user reports, bidding report by user etc,

4.3 Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Information sharing process is done outside the system, and Office of Foreign Affairs (FA) assumes the privacy risks associated with sharing of the information with FA management council.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The data gathered through the application is not shared with any external organizations.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Not Applicable. Data gathered is not shared with any external organizations.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Not Applicable

5.4 Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Not Applicable

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

This system does not require a SORN

6.2 Was notice provided to the individual prior to collection of information?

Before the start of the bidding cycle, FAS FA sends out a circular to the overseas posts informing the Foreign service employees about the upcoming bidding cycle.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

The data solicited by the application is not mandatory, and is required only when the FSO's current assignment is coming to an end in the near future.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The application does not require the users to explicitly consent to data usage. The data collected by the application is used to decide the suitability of the candidate for assignment to vacant overseas posts.

6.5 Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The users of the application are fully aware of why the data is being collected. FA also sends out circular to overseas posts with detailed information about the upcoming bidding cycle.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals have online access to their own data using their assigned control number and their registered e-Authentication account.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Upon detection of erroneous data in the employee profile, users would contact FAS HR with the correct information and HR would update the user profile in iMART system. The FSO Bidding system then periodically downloads the data from iMART system to overwrite any erroneous data with corrections.

7.3 How are individuals notified of the procedures for correcting their information?

Any errors in the user's profile data is caught by the users themselves. At that point they would work with the Agency HR outside the system and get the data corrected in iMART system. Those corrections would eventually flow into FSO Bidding system when it periodically pulls the data from iMART system.

7.4 If no formal redress is provided, what alternatives are available to the individual?

The process is managed within FA.

7.5 Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

With online access to their data and available privacy officer contact information there is minimal privacy risk regarding availability of redress.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

All FAS/MDA personnel with access to the system are screened in accordance with USDA personnel procedures and are only allowed access after training and signing specific rules of behavior.

8.2 Will Department contractors have access to the system?

Yes. They perform the application look up data maintenance and general administration activities. The access is limited to 1 or 2 contractors.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Users are provided annual security awareness training and users with specific security related positions are provided role based training.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The MDA boundary has been certified and accredited for operation including adequate security auditing procedures and technical safeguards to prevent misuse of data. Technically, FSOBS system is integrated with USDA e-Authentication software which requires all users of FSOBS to have an eAuthentication account.
The technical safeguards are the application level and server level safeguard and security measures (Provided by D I S C). The application is protected with eauth and will not allow users to access without approval process.

8.6 Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy risks were identified and mitigated as part of the A&A process for MDA/FSOBS. The system does collect PII data and the primary privacy risks (undesired access) are mitigated by requiring eAuthentication account access and operating the system in the secure USDA DISC environment.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

FSO Bidding system is a web application implemented using Microsoft Dotnet framework, AngularJS and Microsoft SQL Server. The application uses USDA e- Authentication system to authenticate and authorize users. The system runs on hardware provided by DISC and runs on Microsoft Windows 2016 Operating system.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The system is not known to be using any technology that may raise privacy concerns

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

This system does not use any third-party websites or applications.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

None

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

N/A

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

N/A

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

N/A

If so, is it done automatically?

N/A

If so, is it done on a recurring basis?

N/A

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A

10.12 Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A