Privacy Impact Assessment
for the
Foreign Service Officer Appraisal System (FSOAS)

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 Appraisal System (FSOAS) is a web-based application with e-Authentication integration used by Foreign Agricultural Service (FAS) Foreign Service Officers (FSOs) to document their yearly performance, including: performance elements, accomplishments. FAS Office of Foreign Affairs uses the system to rate FSOs and FSOs can also comment on ratings within the system. This PIA is being conducted as part of security assessment and authorization process.

Overview

Foreign Service Officer Appraisal System (FSOAS) is used by FAS Foreign Service Officers posted overseas. FSOAS is owned by FAS. Foreign Service Officers are required to go through a yearly performance appraisal, and they use the "FSO Appraisal" system to submit their self-appraisal data. Appraisal data once submitted is reviewed and commented upon, by the FSO's first- and second-line supervisors. That information is further validated by the Agency's HR personnel. Once the annual appraisal round is over, the collected information is formatted as pdf documents and given to the FAS Program Office, Foreign Affairs (FA) performance appraisal committee for further consideration on FSOs' promotion related matters.

Section 1.0 Characterization of the Information

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

The Foreign Service Officers of the FAS posted overseas need to go through a yearly performance appraisal, and they use the "FSO Appraisal" system to submit their self- appraisal data. Appraisal data once submitted is reviewed and commented upon, by the FSO's first- and second-line supervisors. That information is further validated by the Agency's HR personnel. Once the annual appraisal round is over, the collected information is formatted as pdf documents and given to the FAS Foreign Affairs Office performance appraisal committee for further consideration on FSOs' promotion related matters.

The collected information contains Foreign Service Officer's Accomplishment statement, the performance elements against which the employee's performance is rated, employee's rater statement, employee's reviewer comments, HR comments if any and citations, Awards and Chief of Mission statements in pdf and word documents formats.

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

The application database is initialized with lookup data related to Position titles, Duty Stations, Position Grades and Appraisal Period dates. All other appraisal related data is directly gathered by various actors in the system.

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

The data collected by the system is used primarily to evaluate the Foreign Service Officer's job performance leading to the employee's promotion related matters. This exercise is done on an annual basis every year.

1.4 How is the information collected?

The information is collected through the data entry form within the application. The information is typed in directly by the users of the system. Citations, Awards and Chief of Mission statements are uploaded as PDF and Word documents into the system.

1.5 How will the information be checked for accuracy?

FSO's self-appraisal is verified for factual correctness by their first and second line supervisors and check for legal correctness by the HR personnel.

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

N/A

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

The requirements of the application demand that no privacy related data is needed to meet the application's stated goals. Whenever any such data gets into the system, HR personnel gets involved, and work with the users of the system, so that privacy related data could be purged. The application is also protected by e-Authentication system, to limit access to only those that have OFSO approved accounts. E-Auth level roles are being used to grant access to admin level roles.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The data collected by the application is used by FAS Program Area Foreign Affairs Performance Evaluation board as a basis for deciding promotion related matters.

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

The data collected by the application is reproduced as a printable PDF documents for further manual analysis by the OFSO management council (Performance evaluation board).

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

The system does not use any commercial or publicly available data.

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

All communications to/from the database is conducted using encryption. The system has been assessed and authorized to operate at the Moderate risk categorization level.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

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)?

The FSOAS system, 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 __Privacy Impact Analysis__**: 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/FSOAS system.

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 is shared with OFSO/FAS. Information shared is the self- appraisal of the FSO's along with the rater and reviewer's comments and Citations, Awards and Chief of Mission Statement documents that were uploaded into the system by the Foreign Service Officers

4.2 **How is the information transmitted or disclosed?**

The collected information is formatted and printed onto FAS-436 form in PDF format, one pdf document per employee. FAS HR personnel is responsible for this printing activity, as they have to signoff on the collected data before submitting the PSD documents to the OFSO performance evaluation board.

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

The internal information sharing process is an offline process that involves formatting and printing the data on to FAS-436 form, and so is outside the scope of the system, as far as mitigating the risks are considered.

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 from Appraisal system is not shared with any organizations external to the agency.

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.

N/A

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

N/A

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

N/A

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.

No, it does not require a SORN

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

N/A

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

The employees are generally expected to provide the self-appraisal information and sign and date it, but they have the option of not signing it. In the event they don't want to sign, they need to provide the reason for not signing it.

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 requires that the Foreign Service Officers, Raters and Reviewers sign and date the section where they enter the data. The Signature applied by the users is used as a means of user consent for the use of data by the performance evaluation board.

6.5   <u>Privacy Impact Analysis</u>: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

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

Section 7.0 Access, Redress and Correction

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

Any attempt to login to the system by unauthorized users will be put into a registration queue and an email is generated and sent to OFSO by the system. Designated OFSO employee then approves (or rejects) queued requests by logging into the system and activating the user accounts.

In addition to the account activation, privileged accounts such as Application Admins and HR accounts need to be assigned e-Auth level roles.

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

When the collected data is deemed erroneous or inaccurate by the Raters, Reviewers or HR, a built-in workflow within the application is used to reverted control back to the appropriate users for data correction.

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

The individuals are notified via application generated email, in addition to HR/Rater/Application support personnel manually reaching out to them.

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

The process is managed within OFSO.

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

With available privacy officer contact information there is minimal privacy risk regarding availability of redress.

Section 8.0 Technical Access and Security

.

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

Application is protected by USDA e-Auth system, and user account activation is controlled within the application. A formal email request by the application stakeholders (FAS/OFSO) is required to activate the user's account. Same process is used for user account deactivation. Upon reception of the formal request, application admins will carry out the account activation/deactivation process.

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 privacy training (located in AgLearn).

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

Yes, for the accreditation boundary, Market Development and Administration (MDA).

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

The application is accessible only by the authorized users and is being logged by the application. All changes to the data are also captured with the user that made the change. Only authenticated and activated users (limited to OFSO/FAS and FAS HR) is allowed access to the system. Privileged access to roles such as Admins, Area directors and HR is further controlled by e-Auth level role assignment.

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 the system. 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

9.1 What type of project is the program or system?

Appraisal system is a web application implemented using Microsoft Dotnet framework 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 using any technology that may raise privacy concerns. Additionally, FAS has an active Configuration Control Board (CCB) which meets every Wednesday to discuss all system changes, updates/upgrades and modifications. If new technology were needed for FSOAS or any MDA component, it would have to be completely vetted by the FAS CCB.

Section 10.0 Third Party Websites/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.

Since the system does not use any third party websites or applications, there is no impact on PII.

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?

Not Applicable

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?

Not Applicable

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