Privacy Shield Ombudsperson Mechanism

1. Contact Information

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

2. System Information

(a) Name of system: Ombudsperson Mechanism Records

(b) Bureau: EB

(c) System acronym: PSO

(d) iMatrix Asset ID Number: 256427

(e) Reason for performing PIA:

☒ 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?

On December 12, 2016, IRM/IA determined the system did not require an A&A because SCF = Low Impact, Low Cost and eRA= Assurance Level 2.

(c) Describe the purpose of the system:

Ombudsperson Mechanism Records include information about individuals who have submitted requests through the Ombudsperson Mechanism under the EU-U.S. Privacy Shield, Swiss-U.S. Privacy Shield, or any similar mechanism that may be established between the United States and another country or countries constitute an "Ombudsperson Mechanism". The system assists in the overall management of the request review process and the provision of responses thereto by facilitating accurate and up-to-date record keeping.

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

These records will include basic information the Department needs in order to process individual requests; the personal information required by the Department is the requestor's account of interest (such as a telephone number or email address). The foreign government or EU entities who vet and submit individual requests on the requestors' behalf also may submit other personally identifiable information not specifically requested by the Department but that they believe warrants the Department's review. The records also may include information about an individual's request and the processing of that request.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
(a) State Department Basic Authorities Act of 1956, as amended (22 U.S.C. § 2708 et seq.);
(b) Privacy Shield Framework (81 Fed. Reg. 51042)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide:
- SORN Name and Number: Ombudsperson Mechanism Records, State - 83

SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): SORN is in the final stages prior to publication. Expected to publish September 2017.
☐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 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.)
EB bureau has worked with the Records Division to develop a records disposition schedule and is awaiting publication.

If yes provide:
- Schedule number (e.g., (XX-587-XX-XXX)): Schedule in development
- Length of time the information is retained in the system: Records would be held temporarily for up to five (5) years, with longer retention authorized on a case by case basis and only when necessary for a legitimate business use.
- Type of information retained in the system:
The system contains records and data created, received, and maintained for the purpose of tracking and controlling case activity and status. Files created in response to requests for processing by the Privacy Shield Ombudsperson consist of the original request, interim and final replies, and all related supporting files; administrative, managerial, and statistical reports created to track processing of

individual requests; and records relating to general agency Privacy Shield implementation.

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?

System does not collect SSNs.

(c) How is the information collected?

Individuals submit a request via the EU designated individual complaint handling body under the EU-U.S. Privacy Shield or corresponding body under similar arrangements, including the Swiss-U.S. Privacy Shield. The complaint handling body confirms the identity of the requestor and verifies that the request fulfills the criteria established in the applicable Ombudsperson Mechanism. If the request meets the criteria, the complaint handling body then transmits the request to the Ombudsperson via a custom built Microsoft Office 365 SharePoint application.

(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.

The Ombudsperson Mechanism utilizes Office 365's SharePoint application.

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

Section 3.b of the Ombudsperson Mechanism[1] specifies that requests for an Ombudsperson review must be made in writing by the individual acting on his/her own behalf and the individual provides any information that forms the basis for the request, including unique identifiers associated with the types of communications he/she believes may have been accessed through U.S. signals intelligence activities (e.g., email address or telephone number). Under each Ombudsperson Mechanism, the EU or other relevant designated individual complaint handling body verifies that the information is correct.

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

Yes, records maintained in the system are current as of the date a request is submitted by a foreign government or EU entity. Additional procedures to ensure that the information is current beyond the initial submission would be inapplicable to this system.

[1] Found at https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g.

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

The system does not use information from commercial sources. The Department does not intend to make the records publicly available. The PII contained in the records might be publicly available elsewhere. For example, a requestor might include an email address that he or she includes on a personal webpage that is accessible to anyone.

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

Yes. Information is voluntarily provided by the individual acting on his/her own behalf to obtain review of his/her request under each Ombudsperson Mechanism. A SORN will also be published in the Federal Register, as another form of notice.

(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?

Individuals grant consent by providing a written request for review of the requestor's data under an applicable Ombudsperson Mechanism. There are no penalties if information is not provided, but a request may not be able to be fully processed if necessary information is omitted.

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

Click here to enter text.

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

Records are limited to information about an individual's request and the processing of that request. Only the minimum amount of personal information necessary to process each request is requested. For example, the EU complaint handling body, or corresponding body under similar arrangements, verifies the requestor's identity but the Department does not require it to provide proof of verification (i.e. copies of identification documents).

5. Use of information

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

The EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework create a mechanism for companies on both sides of the Atlantic to comply with EU data protection requirements when transferring personal data from the European Union and Switzerland, respectively, to the United States in support of transatlantic commerce. The Frameworks each established an Ombudsperson Mechanism to address appropriate inquiries by individuals relating to U.S. Intelligence Community access to personal data transmitted from the EU or Switzerland to the United States through Privacy Shield and related commercial transfer mechanisms. The information will be used by the Ombudsperson to ensure that requests are properly investigated and addressed in a timely manner, and that the relevant U.S. laws have been complied with or, if the laws have been violated, that the situation has been remedied.

(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, the Department will not put this information to collateral use outside of the scope of the system as discussed in section 3(b) of the Ombudsperson Mechanism[2].

(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?
The system will provide enhanced statistics and management analytics that will aid in the Department's management of the request process and inform its input into Privacy Shield's annual review process.

(2) Does the analysis result in new information?
The system does not create information about an individual.

(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.

Section 2(a) of each Ombudsperson Mechanism states, "The Privacy Shield Ombudsperson will be able to coordinate closely with the Office of the Director of National Intelligence, the Department of Justice, and other departments and agencies involved in United States national security as appropriate, and Inspectors General, Freedom of Information Act Officers, and Civil Liberties and Privacy Officers." For a complete list of additional routine uses, please see System of Records Notice State-83 "Ombudsperson Mechanism Records," to be published in the Federal Register and the Department's website in September 2017.

(b) What information will be shared?

Pertinent U.S. government partners will receive the information contained in each request, which should include any information that forms the basis for the request under the Ombudsperson Mechanism (including name and any unique communication identifier provided by the individual); the nature of information or relief sought; the United States Government entities believed to be involved, if any; and other measures pursued to obtain the information or relief requested, and the response received through those other measures.

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

[2] Found at https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g.

Section 2(a) of the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework Ombudsperson Mechanism states, "The Privacy Shield Ombudsperson will work closely with other United States Government officials, including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies." Under section 2(c), the Privacy Shield Ombudsperson may refer matters related to requests to the Privacy and Civil Liberties Oversight Board for its consideration.

(d) The information to be shared is transmitted or disclosed by what methods?
The information will be transmitted electronically. The SharePoint system will send an email with a hyperlink notifying users that a record is ready for processing. Users must login in order to access the record.

(e) What safeguards are in place for each internal or external sharing arrangement?
In addition to the text of the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework, existing laws, regulations, and policies that govern the work of particular U.S. government entities such as Inspectors General and the PCLOB are sufficient to aid in fulfillment of U.S. government commitments under the Privacy Shield.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Records are limited to information about an individual's request and the processing of that request. Only the minimum amount of personal information necessary to process each request is requested. For example, the EU complaint handling body, or corresponding body under similar arrangements, verifies the requestor's identity but the Department does not require it to provide proof of verification (i.e. copies of identification documents).

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Requests for access to United States Government records may be made and processed under the Freedom of Information Act (FOIA) and the Privacy Act of 1974 (as amended). Individuals who wish to gain access to or to amend records pertaining to themselves should write to U.S. Department of State; Director, Office Information Programs and Services; A/GIS/IPS; SA-2, Suite 8100; Washington, DC 20522-0208. The individual must specify that he or she wishes the Ombudsperson Mechanism Records to be checked. At a minimum, the individual must include: name; current mailing address and zip code; notarized signature or statement under penalty of perjury; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that the Ombudsperson Mechanism Records include records pertaining to him or her.

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

☒Yes ☐No

If yes, explain the procedures.

Correction procedures are the same as those provided in 7(a) above.

If no, explain why not.

Click here to enter text.

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

The record access and amendment procedures described in 7(a) above are included in the SORN, State-83.

8. Security Controls

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

Access to computerized files is password-protected and under the direct supervision of the system manager. Users internal to the Department of State must logon to the Department's OpenNet system, where they can then access the application via single sign-on; users external to the Department must enter a username and password to access the application. Remote access to the network is configured with the OMB Circular A-130 security requirements, which include, but are not limited to, two-factor authentication and a time-out function.

(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.

Ombudsperson Mechanism Records will reside in the custom-built SharePoint site that is a centralized, password protected space. Each user must access it using his/her own unique user ID and password. Accounts will only be created for users, system managers, and developers. When it is determined that an individual no longer needs access, the individual's account is disabled.

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

The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage.

(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 information, including personally identifiable information (PII). Annual refresher training is mandatory. Additionally, State Department employees who handle PII are required to take a Foreign Service Institute (FSI) distance learning course 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.
The system complies with applicable security measures that are outlined in FISMA, FedRAMP, OMB regulations, NIST Federal Information Processing Standards (FIPS) and Special Publication (SP), and Department of State policy and standards. Information can only be accessed by logging into the Office 365 SharePoint platform with a user name and password. Record details will not be transmitted via email or other electronic means.

(f) How were the security measures above influenced by the type of information collected?
The Department of State's Office of Information Assurance (IA) reviewed the System Categorization Form (SCF) and an eAuthentication Risk Assessment (eRA) in order to categorize the Ombudsperson Mechanism information system and the information processed, stored, and/or transmitted by this system, and, as noted in Section 3(b) above, determined an A&A review was not required. The specific security measures and safeguards of the system were designed to be appropriate given the risk to the Department, its operations, its assets, and to individuals.

9. Data Access

(a) Who has access to data in the system?
There are three types of roles for the system: (1) Users - Officials from the EU designated individual complaint handling body or corresponding body who are authorized to upload Ombudsperson Mechanism review requests; (2) Managers – Department of State employees responsible for processing requests in the system and creating/disabling user accounts; and (3) Developers – Department of State employees and contractors assigned to the development and maintenance of the system.

(b) How is access to data in the system determined?
Only Department of State employees with "Manager" roles can approve system access requests. The user's role and responsibilities will determine the level of access. Officials from the EU designated individual complaint handling body or corresponding body under similar arrangements will only be permitted to submit review requests and check a request's status. Only a limited number of Department of State employees or contractors will be granted access to data in the system.

(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.
User access will be limited according to role-based restrictions.

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

Before being granted access to Ombudsperson Mechanism Records, a user must first be granted access to the Department of State computer system. Only a limited number of users will be granted access to the data, following the principle of least privilege and allocated in a highly restricted and controlled process. An inactivity logout will be enabled after a pre-determined period. The system will track when each user logs into the system and the system manager will have the capability of printing audit trails of access from the computer media, thereby permitting regular and ad hoc monitoring of computer usage.