

PRIVACY IMPACT ASSESSMENT

Falcon on IRM ServiceNow

1. Contact Information

A/GIS Deputy Assistant Secretary

Bureau of Administration
Global Information Services

2. Information on the Collection

- (a) **Date of completion of this PIA:** February 2023
- (b) **Name of collection:** Falcon
- (c) **Collection acronym:** Falcon
- (d) **Bureau:** South and Central Asian (SCA)
- (e) **iMatrix Asset ID Number:** 177245 (SNOW iMatrix ID)
- (f) **Reason for performing PIA:**

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

- (g) **Explanation of modification (if applicable):**
Inclusion of sharing to a new entity (AAR Corporation).

3. General Information

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

- (b) **Is this collection undergoing an Assessment and Authorization (A&A)?**
 - Yes
 - No
 - N/A

If yes, has the privacy questionnaire in Xacta been completed?

- Yes
- No

- (c) **Describe the purpose of the collection:**

In October 2021, the Office of the President and the Department of Homeland Security agreed to the Operation Allies Welcome (OAW) Eligibility Criteria for Afghans Fleeing Afghanistan. This eligibility includes, among others, a) immediate relatives of a U.S. Citizen; b) immediate relatives of a Lawful Permanent Resident and c) immediate relatives of Afghans previously relocated to the United States through OAW. Effective October 1, 2022, the U.S. government relocation effort transitioned from OAW to Enduring Welcome (EW).

The State Department needs to identify people who fall into this eligibility criteria. While the State Department has, to date, been relying on incoming requests via email to manage the intake of these requests, several problems have presented themselves: a) the volume is unsustainable from a manpower perspective – many more people have been separated from their families than previously anticipated; b) the data collection process via email is prone to errors and incomplete; c) data validation with existing U.S. Government databases is complicated by these errors and incompleteness; d) as it has not been publicly advertised, the current system is inequitable.

To rectify these inefficiencies and others, the Department proposes using an online ServiceNow form available on the Department's website to acquire the most current and accurate data possible to inform its relocation assistance efforts. The PII collected through the form will be stored in Afghanistan Coordination Task Force-Data Base (ACTF-DB), a location within the e-Records system and then shared with Falcon, a ServiceNow based user interface custom-built for SCA Coordinator for Afghan Relocation Efforts (CARE). The data collection and storage will enable the Department to build a current picture of how many Afghans may be eligible for relocation and to assist them to depart Afghanistan by manifesting them on flights. The Afghan Family Reunification online form helps avoid unstructured requests for assistance, such as those that arrive via e-mail messages, which may not include important information, such as family size and their biodata, and which often require entry into other systems to facilitate responses. This form is integrated with other elements of the Department's evolving information technology platform used in crisis-management situations, enhancing the efficient handling of individual cases. Lastly, the Department of Homeland Security's United States Citizenship and Immigration Services (USCIS) agency will be a technical partner in this effort as the family relationships of the prospective travelers will need to be reviewed for relocation eligibility.

(d) Describe the personally identifiable information (PII) that is collected, used, maintained, or disseminated:

- On U.S. Persons: Name, DOB, contact information, location (city/state/country), U.S. travel dates, passport number
- Non-U.S. Persons: Name, DOB, immigration status, case number (e.g., visa petition case number, Alien Registration Number (A #), HummingBird Number (specific to OAW), USCIS receipt number, contact information, location (city/state/country), U.S. travel dates, gender, preferred spoken language, passport number & expiration date, nationality

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

- U.S.C. 301 (Secretary of State's authorities with respect to Management of the Department of State);
- 22 U.S.C. 2651a (Organization of the Department of State);
- 22 U.S.C. 3921 (Management of the Foreign Service);
- 8 U.S.C. 1101-1537 (Immigration and Nationality Act of 1952, as amended).

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

Yes, provide:

SORN Name and Number:

- Visa Records, STATE-39

SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

- November 8, 2021

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

N/A

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified collection? 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 collection?

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-03-005-05 (Intermediary Records)
- Disposition Authority Number: DAA-GRS-2017-0003-0002 (GRS 5.2, item 020)
- Length of time the information is retained in the collection: Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
- Type of information retained in the collection: CARE Family Reunification Form data

4. Characterization of the Information

**(a) What entities below are the original sources of the information in the collection?
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 collection?

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

(c) If the collection 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 from the ACTF-DB which obtains the PII directly from the record subject via the electronic DS-4317 Afghan Family Reunification Form. The information from the form is stored in ACTF-DB and then automatically uploaded into Falcon once reviewed.

(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.
Information processed in IRM ServiceNow is stored in the ServiceNow Service Automation Government Cloud Suite which is a FedRAMP-certified cloud service provided by ServiceNow Corporation. ServiceNow implements NIST approved encryption modules to ensure protection of data at rest and in transit. ServiceNow's datacenters are included within the ServiceNow security authorization boundary.

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

The data comes into Falcon from ACTF-DB and before being loaded into Falcon, cross-referenced with U.S. Government databases to determine validity, which in turn helps confirm eligibility for relocation from Afghanistan to the U.S. The name, DOB, nationality, and identifying number (e.g., passport number or A#) will be used to query existing databases to validate the requestor's identity, date of entry into the U.S. (for parolees) and determine if there is an approved I-130 family petition for the people requesting to travel to the U.S. Only validated data entries are loaded from ACTF-DB into Falcon.

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

The Afghan Family Reunification form is a data intake method. The underlying ACTF-DB record will initiate creation of a Falcon record, following above validation measures, and the Coordinator for Afghan Relocation Efforts (CARE) Contact Center will periodically conduct outreach to people based on contact information in the form to keep it current. Updates to entries will be recorded directly in the Falcon record. The individual initially completing the form will not have access to make updates themselves thus it is the responsibility of the individual requesting services to ensure that the information provided is current upon submission of the original form.

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

No, the collection does not use information from commercial sources, nor is the information publicly available.

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

The PII items listed in Question 3(d) are the minimum necessary to perform the actions required by this system. The requirements were reviewed for validating identities and relationships and information required to manifest someone on a flight with several State Bureaus (e.g., PRM) and with other Departments (e.g., USCIS).

5. Use of information

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

The PII will be used to determine if people in the U.S. are eligible to request their eligible family members be reunified with them, to review the relationships between family members to confirm eligibility and to manifest them on flights out of Afghanistan. It will also enable the Department to build a current picture of how many Afghans may be eligible for relocation and to progress with assisting them to depart Afghanistan, including manifesting them on flights out of Afghanistan.

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

Yes, the purpose of this system is to accurately assess the eligibility of individuals to receive relocation services and manifesting them on flights out of Afghanistan. No collateral uses exist for the information collected by the system.

(c) Does the collection 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 collection 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:

- Bureau of Information Resources Management (IRM) Center for Analytics (CfA)
- Bureau of Population, Refugees, and Migration (PRM)

External:

- U.S. Citizenship and Immigration Services (USCIS)
- Contractors:
 - Great Hill Solutions
 - Deloitte Consulting LLP
 - Advanced C4 Solutions (AC4S)
 - Allen Aircraft Radio Corporation (AAR Corp)

(b) What information will be shared?

Internal: All PII listed in 3(d) will be shared with IRM CfA and PRM.

External:

- U.S. Citizenship and Immigration Services (USCIS): All PII listed in 3(d)
- All contractors will have access to name, DOB, contact information, and passport information. Great Hill Solutions, Deloitte Consulting LLP will

also have access to marriage and birth certificates and identifying numbers (e.g., A#, visa case number).

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

Internal: Information will be shared with IRM CfA and PRM to validate identities and relationships, to create refugee cases for processing, and to store data.

External:

- Information will be shared with USCIS/DHS to validate identities and relationships and with contractors to confirm travelers are ready for travel and manifest on flights out of Afghanistan.
- Information is shared with contractors to assess readiness (acquiring visas etc.) and facilitate traveler movement to the airport.

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

Internal: The information is shared internally within the Department by using the ServiceNow secure e-mail feature.

External: If required and approved to share information externally, Department of State enterprise identify management services features are used to authenticate users and limit access to just those organizations and individuals approved for access to the system and information.

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

Internal: SCA/CARE maintains control over permissions for all information on the IRM ServiceNow application to ensure that only authorized personnel with a “need to know” have access to the information. Once the user no longer needs access to the information, SCA/CARE personnel remove user’s access permissions.

External: For information shared with external users, SCA/CARE relies on IRM ServiceNow SSL/TLS encryption of all transmissions combined with multi-factor authentication of external user access to the information.

7. Redress and Notification

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

Yes, the information comes from the ACTF-DB which obtains the information from the electronic DS-4317 Afghan Family Reunification Form that has an approved Privacy Act Statement (PAS) on the first 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. It also provides the applicant with information pertaining to the System of Records Notice (SORN) STATE-39 that governs the collection of this information where the applicant can learn more about how their PII will be utilized.

(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?

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

The information on record subjects is directly pulled from ACTF-DB. Applicants provide their information via the DS-4317 which is then stored in ACTF-DB. That information is then shared with this system weekly for CARE to use. Consent is received to collect the information by ACTF-DB when the applicant completes DS-4317.

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

The Department's Privacy Act practices allows for U.S. applicants to gain access to their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the System of Records Notice, STATE-39. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated with the form utilized for data collection.

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

Yes No

If yes, explain the procedures.

Records subjects can resubmit a new form to correct inaccurate or erroneous information. Additionally, the Department's Privacy Act practices allow for U.S. applicants to correct inaccurate or erroneous information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the System of Records Notice, STATE-39. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated with the form utilized for data collection.

If no, explain why not.

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

The CARE Contact Center will reach out to individuals requesting services periodically to verify data, including at least once prior to manifesting. At that point, they could

provide updates or corrections. Additionally, details on how record subject can correct their information can be found in the System of Records Notice STATE-39. The Privacy Act Statement provided to U.S. applicants point to the SORN, which addresses the necessary procedures record subjects must follow to correct their information.

8. Security Controls

(a) **How is all of the information in the collection/system secured?** IRM ServiceNow encrypts all data (in transit and at rest) with FIPS 140-2 approved encryption modules that protects all data stored in IRM ServiceNow.

(b) **Explain the different roles that have been created to provide access to the collection and the PII (e.g., users, managers, developers, contractors, other).** PII Provider provides Falcon its initial information. The PII provider will only have access to the information they provide during the time of data entry.

- **Database Administrator:** will be responsible for basic data quality (e.g., confirming complete phone numbers, A numbers, SIV case numbers, etc.) and will move the data between ACTF-DB and Falcon. The Data Manager will have access to all data entered by the PII Provider.
- **Data Validator:** will determine if the PII provided is associated with a known entity. They will have minimum access to PII's Provider's information.
- **CARE Case Manager:** (federal employees and contractors) will work with the PII to manifest the individuals for relocation travel (if eligible) and contact the individuals to ensure they are ready to travel. They will have access to all PII.

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

The following procedures are used to establish and limit access: 1) Collection Owner uses IRM-provided processes to request and approve user access to the IRM ServiceNow system and Collection Owner application; 2) Collection Owner uses IRM enterprise identity management service to authenticate all users prior to granting access to the system and Collection Owner PII; 3) Collection Owner specifies the role assigned to each user which controls access and permissions to the ServiceNow application and 4) Collection Owner, with assistance from IRM ServiceNow team, implements Access Control Lists (ACL) rules to specify the access and permissions granted to authorized users of PII data to implement least privilege access to the PII.

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

Access is determined on a need-to-know basis depending on the accessor's duties as outlined in 8b.

- **PII Provider:** As the PII Provider is the provider of information on DS-4317 and thus it is their and their family members' data that is collected on DS-4317 and stored in Falcon. However, they will not have access to the submitted records of this data following submission.

- **Database Administrators:** Database administrators work on the functionality of the system and require full access to the backend of the system to deal with any technical difficulties that may arise. They also are responsible for granting and removing access to the system for all relevant Users. Once database administrators rotate out of this specific unit their access to the system will be terminated.
- **Data Validator:** Data validators will be given access to specific records by database administrators and once a response – validation or disproof – of the data is received, access will be withdrawn to those records.
- **CARE Case Manager:** Case Managers only need access to the system while working on the specific project of pre-flight travel preparation and manifesting, so the Database Administrator will approve access for those employees who are assigned to work on the particular project for the time assigned to this unit. Once the project ends, system administrators will remove users' access to the system.

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

All access to and activity on IRM ServiceNow is audited. All audit data is correlated and reviewed by IRM ServiceNow security operations personnel and State Department Diplomatic Security to detect unauthorized access and misuse.

(f) Are procedures, controls or responsibilities regarding access to data in the collection 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.

Regarding the roles identified in 8b that have access to the PII in this system, they are all required to take the annual Department Cyber Security Awareness Training, PS800 and the biennial mandatory PII Training, PA318 Protecting Personally Identifiable Information.