Frankfurt Investigations Database

1. Contact Information

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

2. System Information

(a) Name of system: Frankfurt Investigations Database

(b) Bureau: EUR

(c) System acronym: FID

(d) iMatrix Asset ID Number: 7293

(e) Reason for performing PIA: IA is conducting the ATO process for the first time

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

(f) Explanation of modification (if applicable):

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?

Estimated completion date is December 2018.

(c) Describe the purpose of the system:

The Regional Security Office (RSO) Investigations Database supports the RSO section at Consulate General Frankfurt to manage the security clearance process for Locally Employed Staff (some of which may be U.S. citizens) at the Consulate. The front-end application accesses a SQL Database to generate and update employee records.

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

The main data fields populated by the investigators are the name of the employee, Social security numbers, residences, police records, DOB, Place of Birth, Race, Sex, Citizenship and Address information.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
5 U.S.C 73, Suitability, Security and Conduct. SSNs are collected pursuant to 22 U.S.C. 4802, 22 U.S.C. 2709, E.O. 13526, Chapter 4.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide:
- SORN Name and Number: Security Records State-36
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): 06/15/2018

☐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 .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)):

NC1-084-82-04, item 1c(2)(a)
NC1-084-82-04, item 1c(2)(b)
NC1-084-82-04, item 1d(2)
NC1-084-82-04, item 2

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?
22 U.S.C. 4802, 22 U.S.C. 2709, E.O. 13526, Chapter 4

(c) How is the information collected?
The information is collected during the interview process by the RSO investigators.

(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.

(e) What process is used to determine if the information is accurate?
The information gathered during the interview process is entered manually. This information is corroborated with written reports received from host country authorities. The database is also checked for accuracy and any incorrect information automatically triggers an additional interview to review for accuracy.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
The information is current. Updates are made when additional information is provided.

(g) Does the system use information from commercial sources? Is the information publicly available?
Publicly available and/or commercially available information is typically in the database however information from an individual's credit report may be manually entered if there are adverse actions.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes, notice is provided via a Privacy Act statement. At the beginning of the interview, a copy of a Privacy Act statement is provided to all LESs that work at the Consulate whom are U.S. persons before collecting their PII.

(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?
Yes, individuals can decline to provide the information. However, all information collected in Frankfurt-ID is necessary for background investigations, so declining to provide information could result in the denial of an appropriate clearance for an employment opportunity.

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

(j) How did privacy concerns influence the determination of what information would be collected by the system?
The system only collects information necessary to conduct investigations assigned by the RSO.

5. Use of information

(a) What is/are the intended use(s) for the information?
The intended use for the information is to help the RSO investigators determine employment suitability.

(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.

(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?
(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

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
There is no external or internal sharing of information.

(b) What information will be shared?
N/A

(c) What is the purpose for sharing the information?
As stated above there is no sharing of information.

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

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

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
N/A

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

State-36, Security Records, outlines the steps an individual may take to request access to their information and correct any factual inaccuracies.

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

☒Yes ☐No

If yes, explain the procedures.

When an individual requests and receives a copy of their information (as outlined in State-36) they are provided with written instructions by A/GIS/IPS on how to pursue correcting or expunging their information if they believe it is inaccurate or erroneous. If during the course of an investigation or re-investigation, negative information is developed about an individual, the RSO investigator initiates a re-interview where the individual has an opportunity to correct factual inaccuracies during the interview process. Alternatively, during the investigation or re-investigation process, an individual may contact the RSO investigator to request the opportunity to update their information or report any inaccuracies to the information that they had previously provided for the investigation.

If no, explain why not.

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

At the beginning of the investigation or re-investigation process, the individual is verbally informed by the RSO investigator how they may contact them to supply additional information or correct inaccuracies. When an individual requests and receives a copy of their information (as outlined in State-36) they are provided with written instructions by A/GIS/IPS on how to pursue correcting or expunging their information if they believe it is inaccurate or erroneous.

8. Security Controls

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

The RSO notifies the systems staff who should be granted access to the Frankfurt Investigation database. System administrators are not allowed by policy to view the contents of the database. They can only access the database for the purpose of performing maintenance. The Information Systems Security Officer regularly reviews the Windows audit logs to ensure that only the users in the RSO section have been granted permissions to access the database.

(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.

All access is enforced by user profiles stored in the AGENTS table (a type of access control table) in the SQL Database. There must exist a record with a UserLoginName corresponding to your MS-Windows login name in order to gain access to the Frankfurt Investigations Database.

Only users that are in the AGENTS table have access to the RSO Database. Further there is a "Superuser" flag designating those users allowed to modify the SQL lookup tables (static data). Additionally there is an "Administrator" flag which designates those users allowed to modify the AGENTS table.

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

Windows Audit Logs are recorded on the server each time the application is accessed. The audit logs are saved on the server and are reviewed monthly by the ISSO.

(d) Explain the privacy training provided to authorize users of the system.

All users of the system are required to complete the FSI online course PA 459 - Protecting Personally Identifiable Information.

(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.

Windows security groups are used to limit access to the information. The database is encrypted for data at rest. Two-factor authentication is used to access OpenNet, which houses the system.

(f) How were the security measures above influenced by the type of information collected?

Since the PII stored in Frankfurt-ID is sensitive (names, DPoBs, and SSNs, etc.) the security measures selected for implementation in this database were appropriate for the sensitivity of the PII that is collected and maintained.

9. Data Access

(a) Who has access to data in the system?

RSO Investigators who have been granted access.

(b) How is access to data in the system determined?

Users are granted access to the database when access is requested by the RSO. The access is based on need to know and a Windows security group.

(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.

The RSO investigators are part of a Windows security group that has been granted access the Frankfurt Investigations Database. It is based on need to know. The investigators are able to view employee investigation records in the database. There is role-based access as explained in 8b.

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

The ISSO conducts regular monthly checks of Windows security audit logs.