DS FBIC PIA

1. Contact Information

PIA Completed By: Name: Alain Luong Title: AISSO Phone: 703-875-5627	**System Owner:** Name: Stephen B. Dietz, III Title: Executive Director
Program Manager: Name: Bryce Bhatnagar Title: Chief Technology Officer	**IT Security Manager:** Name: Moses Whitlow Title: DS Enterprise Compliance Branch Chief
A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services	

2. System Information

(a) Name of system: Diplomatic Security Federal Bureau of Investigations Connectivity

(b) Bureau: DS/EX

(c) System acronym: DS FBIC

(d) iMatrix Asset ID Number: 4516

(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): Modified to capture all Biometrics software that utilize the DS FBIC boundary.

The previous iteration of DS FBIC included the Crossmatch Live Scan Management System (LSMS) only. The new iteration of DS FBIC includes new subcomponents that will increase the avenues for data entry into FBIC as noted in Section 3c.

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?
DS FBIC has a full authorization to operate as of September 21, 2018 with an expiry date of September 30, 2021.

(c) Describe the purpose of the system:
DS FBIC contains several biometric software applications to support case investigations activities in support of the Bureau of Diplomatic Security's (DS) various missions. Persons or subjects of the investigations can be US, Non-US, contractor, government employee (see. Section 4a boxes, everything is selected) tied to case investigations.

While each Biometric Software is different in design, each system collects and sends the same PII data utilizing the same boundary.

DS FBIC Components:

1. Crossmatch Live Scan Management System (LSMS) for Windows. LSMS is a biometrics collection software, installed on OpenNet workstations.
2. ARES is a biometrics collection software able to be installed on approved Android Phones to facilitate mobile enrollments
3. ARES Gateway is a database used for the consolidation and submission management of mobile biometric enrollments to external agencies such as the FBI (organization that owns FBIC).

These applications are used by Diplomatic Security to collect Biometric and Identity data. The information collected within these applications is sent to external federal authoritative databases to establish and verify an individual's identity and criminal records in support of vetting and law enforcement efforts.

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

DS FBIC collects and stores the following information:

- Full name
- Date of birth
- Country or place of birth
- Country of Citizenship
- Gender
- Physical description (hair and eye color, height and weight)
- Passport number
- Race
- Global Unique Identifier (GUID)
- Telephone numbers
- Email Address
- Office of employment
- Social Security Number or other national identification numbers

- Driver's license number
- Biometric data: Fingerprints, Irises and facial templates/images.

However, as PII collected from non-U.S. citizens is not covered by the provisions of the Privacy Act and the E-Government Act, the remainder of this PIA addresses the PII collected and maintained by DS FBIC on U.S. persons only. DS FBIC also collects and maintains the responses received from external agencies.

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

The legal authority for the collection of information is the same as that which established the Bureau of Diplomatic Security: The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Pub. L. 99-399; 22 U.S.C. 4801, et seq. (1986)) as amended. This legislation is cited in 12 Foreign Affairs Manual (FAM) 012, Legal Authorities.

Additional authorities are as follows:
- 26 Code of Federal Regulations (CFR) 601.017, Criminal Investigation Functions, April 1, 2007
- 22 U.S. Code 2709, Special Agents, January 3, 2012

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

☒Yes, provide:
- SORN Name and Number: See Below
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): See Below

  - STATE-31, Human Resources Records, July 19, 2013
  - STATE-36, Security Records, June 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)): See Below
- Length of time the information is retained in the system: See Below
- Type of information retained in the system: See Below

Schedule Number	Length of Time	Type of Information
A-03-005-23 Personnel Security and Access Clearance Records	Temporary. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.	Description: Records of people not issued clearances. Includes case files of applicants not hired. Records about security clearances, and other clearances for access to Government facilities or to sensitive data, created to support initial favorable eligibility determinations, periodic reinvestigations, or to implement a continuous evaluation program. Includes: • questionnaires • summaries of reports prepared by the investigating agency • documentation of agency adjudication process and final determination Note: GRS 3.2, Information Systems Security Records, items 030 and 031, covers Information system access records. Exclusion: Copies of investigative reports covered in items 170 and 171. Disposition: Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use. (Supersedes GRS 18, item 22a) DispAuthNo: DAA-GRS-2017-0006-0025 (GRS 5.6, item 181)
A-11-012-19a Investigative Management System (IMS)	Temporary. Destroy/delete master file data 100 years after case closes. NOTE: If the Bureau of Diplomatic Security becomes aware of any significant or precedent-setting cases that may warrant preservation,	An electronic tracking system used to control and document criminal investigations. Information covers case background, case allegations, case documented interviews, evidence, surveillance videos/audio tapes, pictures, post records and foreign government records, and related investigative information.

	notify NARA for an independent appraisal of these cases.	
A-11-027-01a DOS Clearance System	Disposition: N/A	The DOS Clearance System (DOSC) is the personnel security and suitability processing system and archive. The DOSC contains the security and suitability case files with their associated forms, reports, analysis, memoranda, worksheets, authorizations, etc. It tracks the various processing steps and activities involved with investigations and the determinations made regarding security clearances, public trust certifications and suitability. The system covers the entire process and interfaces with other external databases for information.
B-08-002-03a Security Case Files	Disposition: Card and destroy 1 year after case is closed.	Description: Security investigative files involving attempted penetration, fraud, loss of diplomatic pouches, and other cases not pertaining to investigations of individuals who are or may be employed by the Department or other Federal agencies. The record copies of these cases are retained by the Office of Security.

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?

Bureau of Diplomatic Security: The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Pub. L. 99-399; 22 U.S.C. 4801, et seq. (1986))

(c) How is the information collected?

Authorized individuals obtain biometric (fingerprints, irises and facial images) data using fingerprint and iris/facial capture devices. The biographical information is obtained by authorized individuals. All data entered/uploaded into DS FBIC by authorized individuals

is part of their official duties, to facilitate embassy/post access, vetting, and in support of existing law enforcement investigative efforts. The PII is collected on persons or subjects of the investigations who can be US citizens, Non-US citizens, contractors, government employees (see. Section 4a boxes, everything is selected) tied to case investigations. The subjects of the investigations are: criminal, persons related to the criminal case e.g. family friends, and background investigations for employment.

All phones used in conjunction with FBIC to collect privacy data for various types of official investigations (background, criminal, job related, US persons, Non-US Persons, persons associated to a case etc.) are government owned phones and connected to government owned equipment. The phones connect to the DS managed/govt. owned Mobile Device Manager (MDM), which is a server that is in the DS managed DMZ network segment. The MDM connects to OpenNet so the phones can upload the data to where it needs to go.

The phone connection to the MDM is via Virtual Private Network (VPN) and is encrypted. The connection between the MDM and OpenNet is encrypted.

(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?

Authorized Personnel will review the initial documentation and identification provided to them and validate against proper identification (i.e., embassy badging or national identification card). Any changes to biographical data thereafter will require a new enrollment of the individual, if authorized personnel wish to resubmit the information.

In addition, DS FBIC has built in data validation controls to include validity checks to ensure all mandatory information has been collected before completion. Sequence checking and quality controls are conducted against the biometric data collected to ensure proper fingerprints have been collected and the quality of iris/fingerprint data is compliant with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-76, and Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information ANSI/NIST-ITL 1-2011 NIST SP 500-290.

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

The biographical information is as current as the information received from the data source. All biometric information collected is current as of the collection date and no additional steps are taken to ensure it remains current.

(g) Does the system use information from commercial sources? Is the information publicly available?
No, the system does not use information from commercial sources.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes, both civil and criminal subjects are notified prior to the collection of their information. Civil subjects are required to sign a Privacy Act Statement, Criminal Subjects are notified verbally.

(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?
Civil applicants may decline to submit biometric and biographical data; however the background check is often a prerequisite for employment.
- If no, why are individuals not allowed to provide consent?
Criminal subjects under investigation or suspected of a crime, are not required to provide consent.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
The collection of PII is limited to the required components of a civil and criminal investigation. These required components can be used for nefarious purposes, which requires applying all DoS approved risk mitigation techniques and IT security safeguards inherent to OpenNet. The application of the DoS approved risk mitigation processes and technologies will significantly reduce the likelihood of compromise of the system's information.

5. Use of information

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

The intended use of DS-FBIC is to Support Department of State law enforcement and investigative efforts. DS-FBIC is used to verify the identity of individuals in a civil or criminal investigation.

(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. It was designed for identity verification.

(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?
N/A

(2) Does the analysis result in new information?
N/A

(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 internal sharing.

External sharing:

The information may be shared with:

- A Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments.

  That includes but is not limited to:
  - Department of Homeland Security (DHS)
  - Department of Defense (DoD)
  - Department of Justice (DoJ)
  - Other agencies and entities involved in national security; U.S. border security, official government business or federal law enforcement

(b) What information will be shared?

Electronic Biometric transmission (EBT) files contain all information collected within the system defined in Section 3(d) of this document. DS FBIC shares an EBT file with all external agencies defined in Section 6a of this document.

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

The purpose for sharing the information collected within DS FBIC is to establish and verify a person's identity for background, criminal, and case investigative purposes.

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

The information collected is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

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

Safeguards in place for External sharing arrangements include secure transmissions using FIPS 140-2 approved encryptions using Secure Socket Layer (SSL) / Transport layer Security (TLS) and encrypted Virtual Private Networks (VPN). Memorandums of Understanding/Agreement (MOU/MOA) are in place with external agencies. All external communications are encrypted. Regularly administered security and privacy training informs authorized users of proper handling procedures. Audit trails track and monitor usage and access.

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

The primary risk is misuse by employees and contractors. Misuse may result in or emotional distress for applicants whose PII is compromised. In addition to administrative burdens, data compromises may escalate to financial loss, loss of public reputation, public confidence, and civil liability for the Department of State and other agencies.

To appropriately safeguard the information, numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include memorandum of understanding (MOU) arrangements with external agencies. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. An audit trail provides a record of all functions authorized users perform or attempt to perform.

7. Redress and Notification

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

DS FBIC contains Privacy Act-covered records. Notifications and redress are, therefore, rights of record subjects. Procedures for notification and redress are published in the Privacy Act System of Records Notice (SORN) STATE-31 and STATE-36, and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

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

☒Yes ☐No

If yes, explain the procedures.

To the extent that material contained in DS FBIC is subject to the Privacy Act (5 USC 552a), individuals can request amendment of material in the system under procedures set forth in (SORN) STATE-31 and STATE-36. This amendment procedure is available only to information on non-criminal investigations. All information pertaining to criminal investigations is excluded from the Privacy Act under 5 USC 552a (j)(2). Inaccurate or

erroneous information in DS FBIC criminal investigative files will only be subject to amendment or correction at the request of the federal law enforcement agency which originated the material.

If no, explain why not.

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

The mechanism for requesting correction of information is specified in SORN STATE-31 and STATE-36 & 22 C.F.R. Part 171. The procedures inform the individual how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record if permissible.

8. Security Controls

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

The system is secured within the Department of State intranet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

Access to applications is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user's supervisor and the Information System Security Officer. Data shared with other government agencies is carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by Authorizing Officers of each agency.

Applications are configured according to the State Department Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institute of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(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.

To access the system, persons must be authorized users of the Department of State's unclassified network which requires a background investigation and an application approved by the supervisor and Information System Security Officer. Account request procedures are in place to determine what access users need in order to perform official

duties. All requests must be approved by a Supervisor, Information Systems Security Officer (ISSO) and CJIS Security Officer (CSO).

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

The DS FBIC System Owner and ISSO, in conjunction with Security team, periodically scan and monitor information systems for compliance with State Department Security Configuration Guides, conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems for changes to the Department of State mandated security controls.

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

DS FBIC users are required to attend a security briefing before access to Department systems is granted. This briefing also includes a privacy orientation. Users are also required to complete Cybersecurity Awareness Training, which includes a privacy component, on an annual basis and must acknowledge security and privacy policies in place by signing user agreements. System administrators and privileged users are required to complete a separate security awareness briefing provided by the Information System Security Officer (ISSO) as well as sign an Acknowledgement of Understanding and Rules of Behavior statement.

(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.

Numerous management, operational, and technical security controls are in place in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports. In addition, these controls are subject to rigorous testing, formal assessment, and authorization. Authority to operate is authorized by the Department's Chief Information Officer (CIO). Security controls are reviewed annually and the system is assessed and authorized every three years or sooner if significant or major changes are made to the existing application.

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

The DS FBIC is categorized as a "High" risk system in accordance with FIPS 199. In light of this, NIST SP 800-53, Rev. 4 "High" security controls were applied in accordance with OMB to ensure the security of the application as a whole, including the protection of PII.

9. Data Access

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

Data Access is based on the following roles:

Administrator: Administrators whom have taken appropriate training for the purpose of troubleshooting and performing routine maintenance.

User: Users that have taken appropriate training and have been approved will have selective data access depending on location and duties

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

Access is determined based on requests which are approved by the supervisor, Information Systems Security Officer (ISSO) and CJIS Security Officer (CSO). Access is based on role, position and location. The user is granted only the role(s) required to perform officially assigned duties.

(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.

Only application administrators will have access to all data in the system. Separation of duties and least privilege is employed, and users have access to only the data that the supervisor and ISSO approve to perform official duties.

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

Role based access control is in place to prevent the misuse of data by users who have access to the data. The role based access is configured for "least privilege", which establishes separation of duties (e.g. IT personnel have limited access to enrollment data). In addition, DS FBIC has built in system audit trails that are automatically generated to deter and detect the misuse of data by authorized users.