PRIVACY IMPACT ASSESSMENT

IMS-U PIA

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: 8/2022
(b) Name of system: Investigative Management System – Unclassified
(c) System acronym: IMS-U
(d) Bureau: Bureau of Diplomatic Security (DS)
(e) iMatrix Asset ID Number: 799
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

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

(h) Explanation of modification (if applicable): N/A

3. General Information

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

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The Investigative Management System (IMS-U) supports the Bureau of Diplomatic Security (DS) worldwide investigative mission by providing an enterprise-wide investigative case management system for cases involving investigation by DS, most often pertaining to passport and visa fraud investigations. The application captures all case related information, automates, integrates, and improves DS investigative business

processes, establishes a central index encompassing all Diplomatic Security Service (DSS) investigations, provides investigative analysis and analytical processing while creating internal electronic data sharing.

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

IMS-U collects and maintains the following types of PII on members of the public, foreign nationals, government employees, and contractors who are identified as being directly or indirectly involved in or associated with criminal allegations:

- Full Birth Name (and any name/alias)
- Date of Birth
- Place of Birth
- Social Security Number
- Driver's License Number
- Business Email Address
- Home Email Address
- Birth Certificate Number and corresponding information on parents from birth certificate
- Home Address
- Business Address
- Home Phone Number
- Business Phone Number
- Biographic Information:
    - Gender
    - Race
    - Height
    - Weight
    - Eye Color
    - Skin Tone
    - Hair Color
    - Hair Style
    - Images
    - Age Or Estimated Age
    - Body Type (Build)
    - Scar, Marks, & Tattoos
- Criminal History (free text or uploaded documents)
- Citizenship Status and Information (DSP-11 (Passport Application), OF-156 (VISA Application))
- Financial Account Numbers
- Medical Information (free text or uploaded documents)
- Financial Information (free text or uploaded documents)
- Documents from Legal or Administrative Proceedings (free text or uploaded documents)

- Personnel Information (free text or uploaded documents)
- Family Information (free text or uploaded documents)
- Baptismal Records (free text or uploaded documents)

The remainder of this PIA will only address the PII of U.S. persons.

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

- 22 U.S.C. 4801, et seq. (Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Pub. L. 99-399; (1986)) as amended)
- 26 C.F.R. 601.107 (Criminal Investigation Functions)
- 22 U.S. Code 2709 (Special Agents)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 U.S.C. 2714a(f) (Revocation or Denial of Passport in Case of Individual without Social Security Account Number)
- 44 U.S.C. 3501 et seq. (Government Paperwork Elimination Act of 1998 (Pub. L. No. 105-277))

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

☒Yes, provide:

- SORN Name and Number:
  - STATE-31, Human Resources Records, July 19, 2013
  - STATE-36, Security Records, June 15, 2018
  - STATE-26, Passport Records, July 6, 2011
    STATE-39, Visa Records, October 25, 2012

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  - STATE-31, Human Resources Records, July 19, 2013
  - STATE-36, Security Records, June 15, 2018
  - STATE-26, Passport Records, March 24, 2015
  - STATE-39, Visa Records, November 8, 2021

☐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 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 system? ☐☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

Schedule number A-11-012-19a Investigative Management System (IMS)

- Disposition Authority Number:
  N1-059-09-36, item 1a
- Length of time the information is retained in the system:
  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, notify NARA for an independent appraisal of these cases.
- Type of information retained in the system: Master File
  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.

Schedule number A-11-012-19b Investigative Management System (IMS)

- Disposition Authority Number:
  GRS 4.3, item 010
- Length of time the information is retained in the system:
  Temporary. Destroy immediately after verification of successful conversion. (Supersedes GRS 20, item 2a [4]).
- Type of information retained in the system: Input/Source Records
  Hard copy (non-electronic) documents used to create, update, or modify electronic records when the electronic records are retained to meet recordkeeping requirements and are covered by a NARA-approved schedule. Included are such records as hard copy forms used for data input as well as hard copy documents that are scanned into an electronic recordkeeping system.

Schedule number A-11-012-19c Investigative Management System (IMS)

- Disposition Authority Number:
  GRS 4.3, item 020
- Length of time the information is retained in the system: Temporary. Destroy immediately after data have been entered or otherwise incorporated into the master file or database and verified. (Supersedes GRS 20, item 2b).
- Type of information retained in the system:
  Input/Source Records: Electronic records entered into the system during an update process, and not required for audit and legal purposes and electronic records received from other agencies.

Schedule number A-11-012-19d Investigative Management System (IMS)

- Disposition Authority Number:
  GRS 4.3, item 031
- Length of time the information is retained in the system: Temporary. Destroy when business use ceases. (Supersedes GRS 20, item 5).
- Type of information retained in the system:
  Outputs: Electronic files consisting solely of records extracted from a single master file or data base that is disposable under GRS 20 or approved for deletion by a NARA-approved disposition schedule, EXCLUDING extracts that are: Produced as disclosure-free files allow public access to the data; or Produced by an extraction process which changes the informational content of the source master file or data base; which may not be destroyed before security NARA approval.

Schedule number A-11-012-19e Investigative Management System (IMS)

- Disposition Authority Number:
  GRS 4.3, item 030
- Length of time the information is retained in the system: Temporary. Destroy when business use ceases. (Supersedes GRS 20, item 16).
- Type of information retained in the system: Outputs: Printouts derived from electronic records created on an ad hoc basis for reference purposes or to meet day-to-day business needs.

Schedule number A-11-012-19f Investigative Management System (IMS)

- Disposition Authority Number:
  GRS 3.2, item 040
- Length of time the information is retained in the system: Temporary. Destroy when superseded by a full backup, or when no longer needed for system restoration, whichever is later. (Supersedes GRS 24, item 4a [1]).
- Type of information retained in the system: Systems Backups: System Backups and Tape Library Records. Backup tapes maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

Schedule number A-11-012-19g Investigative Management System (IMS)

- Disposition Authority Number:
  GRS 3.1, item 051
- Length of time the information is retained in the system: Temporary. Destroy 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system. (Supersedes GRS 20, item 11a [1]).
- Type of information retained in the system:
  System Documentation includes systems requirements, system design, and user guides.

Schedule number A-11-008-06 Passport and Visa File, Domestic Records Disposition

- Disposition Authority Number:
  N1-059-07-04, item 6
- Chapter 11: Diplomatic Security Records Office of Antiterrorism Assistance

- Length of time the information is retained in the system:
  Records are maintained for 5 years or upon separation of the bearer.
- Type of information retained in the system:
  Files contain correspondence required in the process of applying for diplomatic and official passports and visas for staff personnel and contractors who perform tasks outside the U.S. Files include actual passports returned upon completion of task. Files are arranged alphabetically by individual's name. Files span 2003 to present.

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) On what other entities above is PII maintained in the system?

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

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No ☐N/A

- If yes, under what authorization?
  26 U.S.C. § 6039E (for passport operations);22 U.S.C. § 2714a(f) Revocation or Denial of Passport in Case of Individual without Social Security Number; and8 U.S.C. § 1182 (for Visa operations)

(d) How is the PII collected?

The information collected by IMS-U is collected through direct input from interviews conducted by DS Law Enforcement Investigators, uploading of documents or images, and through DS Law Enforcement investigative and analytical activities. All data is collected and manually entered such as the SSN, and/or supporting documentation can be uploaded/attached into the system by DS employees (i.e. Foreign Service and Civil Service Criminal Investigators, Investigative Analysts and DS employed contract investigators) as part of their official duties as a member of a Law Enforcement Organization (LEO). PII can also be collected and sent in a case referral from CA. If CA identifies potential criminal activity related to passport fraud, they will send a case referral which can include PII on the subject. CA is responsible for initial collection and

verification of the PII sent; however, in the course of the investigation, PII may be updated as needed.

(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.

N/A

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

Assigned personnel validate data through cross-checking of various U.S. Agencies (federal and state) databases and through interviews Access to these disparate databases is at each posts' disposal. It is the investigators responsibility to update PII if, through investigations, they find the data in IMS-U is inaccurate. IMS-U also has built-in data validation controls such as sequence checks, range checks, logical relationship checks, and validity checks.

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

The information is as current as the information received from the data sources. IMS-U personnel will have access to the system to manage data stored within it. It is the responsibility of the investigator to update the information as needed. This will ensure that data remains current if changes are needed. If a case is opened within IMS-U to investigate fraudulent activities, users assigned functional roles can update cases with new information.

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

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

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

The nature of criminal investigation work is such that significant amounts of data are needed and collected to ensure the proper identification of the subject and the ability to contact witnesses. This may constitute significant amounts of PII. All PII listed in 3d above is necessary.

5. Use of information

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

The intended use of the PII in IMS-U is to allow DSS Office Special Agents, Regional Security Officers (RS and team members), and Investigative Analysts to investigate and analyze data from headquarters, field offices and posts around the world. IMS-U affords centrally indexed, case tracking and management of information related to Passport Fraud (PF), Visa Fraud (VF), Regional Security Office, Protective Intelligence Investigations, Professional Responsibility, and Criminal Investigative Liaison (CIL) cases.

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

Yes, the PII collected for use by the IMS-U is required to support DS worldwide investigative mission by providing an enterprise-wide investigative case management system. The PII used in IMS-U helps to identify and distinguish the subjects of Passport and visa fraud investigations. As well as other persons pertinent to the investigation such as victims and witness.

(c) Does the system 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 system will use test data, will it include real PII?
☐Yes ☐No ☒N/A

If yes, please provide additional details.

N/A

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal: There is no internal sharing.

External: IMS-U shares PII with the U.S. Attorney's office and, as part of joint investigation and task forces. It also provides PII to any federal, state, and local authorized law enforcement entities with a need to know.

(b) What information will be shared?

Internal: There is no internal sharing.

External:
All PII listed in 3d is provided to the U.S. Attorney's office for litigation.

In cases where there is a need-to-know, PII listed in 3d is provided to federal, state, and local authorized law enforcement entities based on the active investigation.

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

Internal: There is no internal sharing.

External: The purpose for sharing information with the U.S. Attorney's Office and federal, state, and local authorized law enforcement entities is for investigation and law enforcement purposes.

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

Internal: There is no internal sharing.

External: When sharing with the U.S. Attorney's Office and federal, state, and local authorized law enforcement entities, PII is shared via encrypted email or delivered in hard copy.

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

Internal: There is no internal sharing.

External: All PII provided to the U.S. Attorney's Office and federal, state, and local authorized law enforcement entities is properly marked with the appropriate Classification. PII is shared via encrypted email. When PII is delivered in hard copy, it is carried in a locked bag as required.

7. Redress and Notification

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

No. Due to the nature of record subjects being involved or associated with criminal allegations and fraudulent activities, the records subjects are not afforded any notice prior to data collection per 5 U.S. Code § 552a (j)(2).

(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?

N/A

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

Records subjects are not asked for consent. Data for the IMS-U is derived from investigations of the public, foreign nationals, government employees, and contractors who are identified as being directly or indirectly involved in or associated with criminal allegations and fraudulent activities for Passport Fraud (PF), Visa Fraud (VF), Regional Security Office, Protective Intelligence Investigations, Professional Responsibility, and Criminal Investigative Liaison (CIL) cases.

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

There are no procedures that allow record subjects to gain access to their information. As a law enforcement investigative system owned by the Bureau of Diplomatic Security, in STATE-36, Security Records, 22 C.F.R. 171, permits IMS-U to be excluded from the access and redress provisions of the Privacy Act in order to prevent harm to law enforcement investigations or interests. However, access requests are considered under both the Privacy Act and/or the Freedom of Information Act (FOIA) on a case-by-case basis if made under the procedures outlined in 22 C.F.R. Part 171.

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

☒Yes ☐No

If yes, explain the procedures.

To the extent that material contained in IMS-U is subject to the Privacy Act (5 U.S.C. § 552a) individuals can request amendment of material in the system under procedures set forth in STATE-36, Security Records. 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 U.S.C. § 552a (j)(2). Inaccurate or erroneous information in 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.

NA

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

The mechanism for requesting correction of information is specified in State SORN 36, 22 C.F.R. Part 171, and this PIA.

8. Security Controls

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

As a system, IMS-U is protected by a layered defense in depth approach that limit's user access to the system and the associated data. Once an authorized IMS-U user logs into OpenNet and is authenticated, the end user is granted access to the IMS-U system.

IMS-U's data is stored in an Oracle database, which is protected by role-based access controls configured with the concept of least privilege. The data-at-rest for IMS-U is protected via encryption.

IMS-U restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. IMS-U is scanned to ensure all required security controls are implemented and vulnerabilities are remediated.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

DS IMS-U Application Roles	Description of System Access	PII Access
System Administrators	A limited number of System Administrators have access to the system to conduct standard administrative activities including hardware updates/maintenance, software updates/maintenance, and general troubleshooting. System Administrators have limited access to the application for troubleshooting activities but are not authorized to create or work cases.	All PII data listed in 3d
Developers	A limited number of Developers have access to the system to conduct general troubleshooting activities. Developers have no system administrative privileges. Developers have limited access to the application for troubleshooting activities but are not authorized to create or work cases.	All PII data listed in 3d

End Users	End users are assigned roles based on their office and function within the office. End users are limited to only the roles needed to perform their function. End users creates and/or works cases.	All PII data listed in 3d

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

Access to the IMS-U application is restricted to cleared Department direct hire and contractor employees. The approval process starts by the user having access to OpenNet with a request being placed by the IMS-U user via AccessDS and undergoes a review and approval or denial by the business owner. The business owner determines the level of appropriate access and approves access. Additionally, all access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

DS IMS-U Application Roles	Type of System Access	System Permissions
System Administrators	Front end application and database	Read only for troubleshooting and validating in the application. Read Update, Delete in the database
Developers	Front end application	Read only for troubleshooting and validating
End Users	Front end application	Create, Read, Update, Delete

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

System Administrators: The System Administrators request access via the AccessDS application The system Information System Security Officer (ISSO) and their supervisor is included in this approval chain for privileged accounts.

Developers: Developers request access to the system via the AccessDS application, which tracks the approval chain for this request. Their request includes their justification for access at this level as related to their job duties. The system Information System Security Officer (ISSO), their supervisor, and a representative from the Business Owner office is included in this approval chain for privileged accounts.

End Users: End Users request access to the system via the AccessDS application, which tracks the approval chain for this request. Their request includes their justification for access at this level as related to their job duties. The system Information System Security Officer (ISSO), their supervisor, and a representative from the Business Owner office is included in this approval chain for privileged accounts.

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

IMS-U is monitored by inherited security controls of the OpenNet general support system. Controls built into OpenNet include routers and Network Intrusion Detection System (NIDS). These controls provide network level controls that limit the risk of unauthorized access from all IP segments, to include patch management, configuration management, and segregation of duties. In addition, the application is placed behind a virtual firewall to further limit access to system data. All user actions (e.g., adding or updating a record) within the system are recorded and maintained in a log for auditing. IMS-U's data-at-rest is encrypted.

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

Users are required to complete the PS800 Cybersecurity Awareness Training on an annual basis and must acknowledge in place policies by signing user agreements. Users are also required to complete the FSI course PA318, Protecting Personally Identifiable Information biennially. Each system administrator is required to take the IA-210 training every 3 years.