1. Contact Information

Department of State Privacy Coordinator

Margaret P. Grafeld
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: 7/27/09

(b) Name of system: Investigative Management System

(c) System acronym: IMS

(d) IT Asset Baseline (ITAB) number: 799

(e) System description (Briefly describe scope, purpose, and major functions):

The IMS is a web-based application designed to consolidate the Bureau of Diplomatic Security's (DS) Diplomatic Security Service (DSS) criminal investigations and other investigative case data. Specifically**,** IMS allows DSS Special Agents and other authorized personnel to retrieve case related data from headquarters, field offices and posts around the world. IMS 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.

IMS facilitates worldwide sharing of investigative information between regional security officers (RSOs), field offices (FOs), and Diplomatic Security Headquarters (HQ), consolidating functionality of the previous DS Case Management System:

- RAMS (Records Analysis Management System)

IMS facilitates the import, export, and electronic storage of case data up to the Sensitive But Unclassified (SBU) level and is available to authorized users over OpenNet Plus. IMS also provides the ability for multiple offices to track case details, share data between all field entities and the DS Investigations Directorate, forward, update case data, send alert messages to headquarters, provide extensive report generation, and produce related case documentation. IMS allows agents to effectively manage criminal and administrative investigations within DSS, using one comprehensive application.

(f) Reason for performing PIA:

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

(g) Explanation of modification (if applicable): Certification & Accreditation

(h) Date of previous PIA (if applicable): October 2, 2008

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

IMS collects and maintains the following types of PII on members of the public, foreign nationals, and U.S. Government employees and contractors who are identified as being directly or indirectly involved in or associated with criminal allegations. All types of information may NOT be collected on each specific group of individuals.

- Legal Identifying Information
  - Full Birth Name (and any name/alias)
  - Gender
  - Date and Place of Birth
  - Race
  - Social Security Number
  - Drivers License Number
  - Birth Certificate Number and corresponding information on parents from birth certificate
  - Baptismal Records (This is legacy information imported from RAMS. This information is no longer collected. Seventy-four baptismal records are maintained by IMS.)
- Contact information
  - Address
  - Phone number
- Biometric Information
  - Gender
  - Race
  - Height
  - Weight
  - Eye Color
  - Skin Tone
  - Hair Color
  - Hair Style
  - Images
  - Age or Estimated Age
  - Body Type (Build)
  - Scars, Marks, & Tattoos
- Criminal History
- Citizenship Status and Information
  - DSP-11 (Passport Application)
  - OF-156 (VISA application)

The Department of Justice (DOJ) requires that all law enforcement agencies obtain a DNA sample from suspects. The DOJ provides each law enforcement agency all the equipment necessary to obtain and mail the DNA sample to the Federal DNA Registry. This registry is maintained by the DOJ and assists in criminal investigations. DS does not store any DNA data within its systems. IMS keeps a record of the submission of DNA data to the DOJ. This record of submission is tracked through a “mailer number” which is associated with the envelope used to return the DNA kit and sample to DOJ. No PII can be obtained from the use of the “mailer number” alone.

b. How is the information collected?

The information collected by IMS is collected though the uploading of documents or images, through web forms, through transfers from the Bureau of Consular Affairs (CA) Consular Affairs Passport Lookout Tracking System (PLOTS) of identified fraud cases,

through DS Law Enforcement investigative and analytical activities. All data is collected and entered/uploaded into the system by DS employees (i.e., Foreign Service and Civil Service criminal investigators, intelligence research specialists, and DS employed contract investigators and intelligence research specialists) as part of their official duties as a member of a law enforcement organization (LEO).

c. Why is the information collected and maintained?

The information collected and maintained by IMS is collected and maintained for the purpose of supporting DSS criminal investigations through the consolidation of investigative data. IMS allows all offices within DSS that utilize the system the ability to investigate and analyze case related and intelligence data from headquarters, field offices, and posts around the world. IMS affords centrally indexed, case tracking and management of information related to passport fraud (PF), visa fraud (VF), and criminal investigative liaison (CIL) cases.

d. How will the information be checked for accuracy?

Assigned personnel will validate data through cross-checking of disparate databases and through interviews. IMS has built-in data validation controls such as sequence checks, range checks, logical relationship checks, and validity checks. Sequence checks and range checks ensure that a control number follows sequentially and any out of sequence or duplicated control numbers are rejected prior to processing. The logical relationship check occurs if a particular condition is true, then one or more additional conditions or data input relationships may be required to be true to consider the input valid. Validity checks are programmed checking of the data validity in accordance with predetermined criteria. For example, an individual's biographical record contains a field for gender and the acceptable status codes are M or F. If any other code is entered, the record will be rejected.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to IMS, are as follows:

- Pub.L. 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended;
- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the sharing of Terrorism Information to Protect Americans).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

IMS collects the minimum amount of personally identifiable information necessary to complete its statutorily mandated functions of supporting DSS criminal investigations through the consolidation of investigative data. IMS allows all offices within DSS that utilize the system the ability to investigate and analyze case related and intelligence data from headquarters, field offices, and posts around the world. IMS affords centrally

indexed, case tracking and management of information related to passport fraud (PF), visa fraud (VF), and criminal investigative liaison (CIL) cases.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the 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.

4. Uses of the Information

a. Describe all uses of the information.

Specifically**,** IMS will allow DSS special agents and intelligence research specialists as well as other authorized personnel to investigate and analyze data from headquarters, field offices and posts around the world. IMS 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. What types of methods are used to analyze the data? What new information may be produced?

DS investigators and analysts are able to retrieve data based on text queries and then use the data to conduct criminal investigative analysis based on data collected and stored in IMS from various sources such as the Form DSP-11, Form OF-156, motor vehicle records, LEO restricted databases (i.e. NCIC, TECS, etc.), and other outside sources. All DS case related data is maintained in the IMS system in order to provide a centrally indexed repository. No new information on the record subject is produced.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Users can input any information from commercial sources, publicly available information, and information from other Federal agencies determined to be germane to criminal investigations.

d. Is the system a contractor used and owned system?

IMS is a U.S. Government owned system which was primarily designed and developed by contractors under the guidance and management of U.S. Government employees. All contractors abide by regulatory guidelines established as part of their contractual arrangement with the U.S. Government and have signed and follow DS's Rules related to the protection and handling of sensitive information. All employees (FS, GS, and contractors) are required to be trained annually on the protection of information as part of the Department of State's Information Security Program. These records are maintained centrally by the Bureau of Diplomatic Security (DS).

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

IMS performs basic internal records management functions on the PII for the purpose of criminal investigations but does not create new information about the record subject. Accounts assigned to users are issued on a "need-to-know" basis which is determined by the office of assignment. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

IMS collects and maintains a significant amount of personally identifiable information (PII). There are inherent risks associated with maintaining this type of information. Records within IMS are only retained in accordance with the Diplomatic Security Records disposition schedule and are not used for purposes outside of criminal investigations.

In an attempt to mitigate these risks, the Department of State has implemented numerous management, operational, and technical security controls to protect the information in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the 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.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The information collected and maintained by IMS is only shared within DS.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

IMS is a web-based application within OpenNet+. In order for an employee of DS to obtain access to IMS, he or she must complete the required training to gain access to OpenNet+; have his or her management's approval; and pass the proper security checks.

Moreover, numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with internal sharing and disclosure including, but not limited to annual security training, separation of duties, least privilege and personnel screening.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

It is possible for an employee with authorized access working for the DSS to use his or her access to this information to retrieve PII on an individual and use this information in an unauthorized manner. In order to mitigate this risk, all DSS employees are required to undergo computer security and privacy awareness training prior to accessing IMS, through which the information is shared, and must complete refresher training annually to retain access to IMS.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

There is no external sharing of PII from IMS.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

PII collected and maintained in IMS is not shared outside the department.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

PII collected and maintained in IMS is not shared outside the Department.

The risks associated with sharing privacy information externally and the disclosure of privacy information is generally higher than internal sharing and disclosure. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering; phishing; abuse of elevated privileges; or a general lack of training. Transmission of privacy data in an unencrypted form (plain text) and the use of un-secure connections are also a serious threat to external sharing. Numerous, operational and technical management controls are in place to reduce and mitigate the risks associated with external sharing and disclosure including, but not limited to formal memorandums of agreement/understandings (MOA/MOU); service level agreements (SLA); annual security training; separation of duties; least privilege; and personnel screening.

8. Notice

The System:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

STATE-36

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notices titled STATE-36, Security Records.

b. Do individuals have the opportunity and/or right to decline to provide information?

The individual is informed of the Privacy Act statement; whereby, the acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use and authority for collection of information submitted are also described in the System of Records Notice titled STATE-36, Security Records.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. The utility of the information in the system about a particular individual will not extend over the allotted time in the Department of State's Disposition of Schedule, as defined in Diplomatic Security Records, Chapter 11. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The Notice offered is reasonable and adequate in relation to the system's purposes and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

IMS contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about 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. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport 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. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The Business Owner DS/P/PL approves and authorizes use of the IMS system. System accounts are maintained and reviewed on a regular basis. The following DoS policies establish the requirements for access enforcement.

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers);
- 12 FAM 622.1-2 System Access Control;
- 12 FAM 623.2-1 Access Controls;
- 12 FAM 629.2-1 System Access Control; and
- 12 FAM 629.3-3 Access Controls

The database enforces a limit of three consecutive invalid access attempts by a user during a 15 minute time frame. After 20 minutes of inactivity, a session lock control is implemented at the network layer.

The information system 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. A system use notification ("warning banner") is displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

Diplomatic Security uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host DS's major and minor applications, including the IMS components, for changes to the DoS mandated security controls.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed, or attempted to perform on an information system.)

11. Technologies

a. What technologies are used in the system that involves privacy risk?

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational, and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the safeguards implemented to mitigate the risk to any Information Technology. IMS has been designed to minimize risk to privacy data.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any Information Technology.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The C&A is due September 2009 and is in progress.