1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: January 11, 2010

(b) Name of system: The Office of Foreign Mission Information System

(c) System acronym: TOMIS

(d) IT Asset Baseline (ITAB) number: 382

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

The Office of Foreign Missions Information Systems (TOMIS) supports all Office of Foreign Mission (OFM) operations, and is critical to its mission of national security, public safety, and reciprocity. Launched in November 2001, TOMIS replaced the Office's aging mainframe-based legacy system, providing a modern interface, and using Oracle, an industry standard database as its foundation.

TOMIS is an integrated, custom application system designed to support OFM activities for a client base consisting of 100,000 diplomatic staff, support personnel and their dependents from more than 150 accredited nations. The OFM user community includes OFM offices in Washington D.C., New York, Chicago, Los Angeles, Miami, and San Francisco, as well as affiliated organizations including the DoS Office of Protocol, the U.S. Mission to the United Nations (US/UN), the Interagency Liaison Group (ILG), Secret Service, and DoS Bureaus of Diplomatic Security and Consular Affairs (CA/PPT).

Five integrated subsystems support the mission of these offices:

- Diplomatic Motor Vehicles (DMV)
- Tax
- Customs
- Property
- Travel

(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): The TOMIS system is being migrated from a client/server based architecture to a Web Services architecture. However, there are no changes to the data of database structure associated with this update.

(h) Date of previous PIA (if applicable): March 20, 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?

The TOMIS system collects information on Foreign Diplomats in the United States, US Citizens, and Lawful Permanent Residents working for foreign Governments for the purpose of providing privileges and immunities as outlined in the Foreign Mission Act. Information collected includes:

- Name
- Date of Birth
- Social Security Number (if applicable)
- E-Mail Address
- Employment information pertaining to jobs working for Foreign Governments in the U.S.
- Personal Identification Number created by the Department of State Office of Protocol if the record subject does not have a social security number

b. How is the information collected?

Information is collected through a variety of federal paper and web based applications that all Foreign Diplomats stationed in the United States must complete. These forms must be completed upon arrival in the United States and information is then entered into TOMIS by DS/OFM personnel.

c. Why is the information collected and maintained?

The information collected and maintained by TOMIS is for the purpose of providing privileges and immunities to foreign diplomats such as vehicle licensing, drivers' licensing, tax information, and security checks as outlined in the Foreign Mission Act.

d. How will the information be checked for accuracy?

Verification of information is done by the associated Foreign Missions, and other records from U.S. Federal Agencies (Department of Homeland Security's USCIS and Customs and Border Protections, etc.) After entering all the required information into TOMIS the Foreign Missions print each subject's information and verifies the accuracy with the subject. Required information must be provided and validated by documentation (Passport, Visa, Letter of Authorization, ect.) prior to individual accreditation.

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

- The Foreign Missions Act, 22 USC 4301-4316
- Title 22 – foreign Relations and Intercourse, Chapter 53 Authorities Relating to the Regulations of Foreign Missions. Pub. L. 103-236
- Vienna Convention of Diplomatic Relations and Optional Protocol of 18 April 1961.
- The Foreign Sovereign Immunities Act, Pub. L. 94-583.

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

TOMIS collects the minimum amount of personally identifiable information necessary to complete it statutorily mandated functions. The nature of the information collected, processed, and maintained resulted in an overall security categorization of "High" for TOMIS and establishes the specific privacy and security controls required.

The controls are subject to rigorous testing, a formal certification and accreditation process, and authority to operate is authorized by a Senior Agency Official. Moreover, controls are reviewed annually, and accredited every three years or sooner if the Application (System) has implemented major changes to the existing Application, as defined by OMB Circular A-130.

4. Uses of the Information

a. Describe all uses of the information.

The TOMIS system is a data repository of information used in insuring the fair treatment of Foreign Diplomats within the United States based on a system of reciprocity for the treatment of US Diplomats in the respective foreign countries. Individual ID numbers are created by TOMIS as a means of identifying individuals who are not American citizens and do not have social security numbers.

TOMIS contains information regarding all foreign diplomats accredited to the U.S., officials, and employees of foreign and international missions. It is also used to help determine the citizenship of individuals whose parents were diplomats at the time of their birth in the U.S. and thus potentially ineligible for U.S. citizenship. TOMIS also facilitates vehicle licensing, drivers licensing, tax information, and security checks.

b. What types of methods are used to analyze the data? What new information may be produced?

An aggregation of data from other federal agencies will be gathered to provide a complete picture of the Diplomat and his family member to ensure that neither the Diplomat nor his family members are threats to the security of the United States or its citizens. It includes the collection of information pertaining to criminal activities and abuse of privileges.

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

TOMIS uses information from Federal agency databases, but does not use commercial or publicly available information.

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

TOMIS is a government owned system which was primarily designed and developed by contractors. Users of TOMIS are full-time employees (FTE) and contracting staff. All personnel are required to abide by regulatory guidelines and have signed and follow DS's Rules of Behavior.

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.

As the personally identifiable information contained in TOMIS merits a high security categorization, strenuous security controls are in place to ensure the protection of the PII and negate the threat of function creep. Information in the system is accessed through the use of a logon ID and password. An audit trace is maintained on failed logon attempts which lock the account after three failed attempts. The system also requires the user to frequently change their password. All record creation and modification are recorded with the user's logon and the date and time the creation or modification took place. Key records have a history which would allow the restoration of original data if needed. Requiring users to take privacy awareness training also aids in the negation of function creep.

5. Retention

a. How long is information retained?

Information collected and maintained by TOMIS is retained in accordance with A-10-001-04 OFMIS - Computerized Information System record disposition schedule. The information retained on Foreign Diplomats who have left the country will be used in the determination of acceptance when and if the individual returns to the United States.

Information in TOMIS is to be deleted when no longer needed, as determined and cleared by the OFM Information Systems Manager. If information is deleted, the supporting documentation is retired to the National Archives five years after the departure of the individual from the United States. The reports generated from the system have various retention spans ranging from one to six months. At the end of the retention period, the reports are destroyed.

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

TOMIS collects and maintains names, date of birth, individual ID numbers assigned by DoS Office of Protocol, employment information pertaining to jobs working for Foreign Governments in the U.S., and addresses. The records disposition schedule is appropriate and flexible enough to reduce privacy risk. Records may be destroyed when no longer in use, with the approval of the OFM Information Systems Manager. This balances the protection of privacy with OFM's need to determine whether a foreign diplomat can be accepted back into the United States following their end of their assignment.

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?

Personally identifiable information is shared with Consular Affairs Passport Services (CA/PPT) for the purpose of issuing passports.

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

Authorized individuals within CA/PPT are granted access to TOMIS for the purpose of issuing passports.

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

Sharing of information within TOMIS is limited to CA/PPT. There is no anticipated risk in this sharing arrangement. Users of TOMIS in DS and CA/PPT have all received privacy and cybersecurity training and are familiar with the Department's Rules of Behavior for accessing systems that contain PII. However, it is possible for an employee working for the Bureau of Diplomatic Security or Consular Affairs to use his or her access to this information to retrieve contact information on an individual and use this information in an unauthorized manner. In order to mitigate this risk, all Department employees are required to undergo computer security and privacy awareness training prior to accessing OpenNet, through which the information is shared, and must complete refresher training yearly in order to retain access.

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?

Information collected and maintained by TOMIS is not shared with any outside agencies.

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

No information contained within TOMIS is shared outside the Department of State.

TOMIS is monitored and guided by the inherited security controls of the OpenNet. Controls built into the OpenNet General Support System (GSS), including routers and Network Intrusion Detection System (NIDS), 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.

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

The information that TOMIS collects and maintains is not shared with external organizations.

While personally identifiable information from TOMIS is not meant to be shared externally, 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 general lack of training. Transmission of privacy data in an unencrypted form (plain text), and using unsecure connections are also a serious threat to external sharing. Numerous management, operational and technical 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.

While TOMIS is covered by the Privacy Act, rights granted by the Privacy Act do not extend to Foreign Nationals (FN) maintained in the system.

Provide number and name of each applicable systems 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?

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

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

Individuals do have the right to decline to provide information. However, declining to provide information automatically negates services like receiving identification cards and license plates for vehicles.

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 Schedule, as defined in Office of Foreign Mission Records, Chapter 10. 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. Individuals are made aware of the collection through a Privacy Act notice and are subsequently informed of its approved 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?

TOMIS 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 record 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. As such, privacy risks associated with notification and redress are minimal.

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?

Access to the system is provided by assigned logon and password. An individual wishing to access the information within the system must submit an application for logon signed by the individual making the request and the individual's supervisor indicating access is needed to perform the individual's assigned job. The application has a "must read" area where the individual's responsibility for information safeguard is written. This is where the individual signs that he/she has read and understood his/her responsibilities. This completed application is forwarded to the system's Information System Security Officer (ISSO) for review and approval prior to assigning the logon. The following DoS policies establish the requirements for access enforcement. Foreign Diplomats are not provided access to TOMIS. Access to TOMIS is limited to Department of State employees.

- 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
- 12 FAM 629.3-3 Access Controls

The database enforces a limit of 3 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 TOMIS 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.)

TOMIS is a government owned system supported by contract employees, who support U.S. Government employees in their maintenance of the system.

Contractors who support TOMIS are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain U.S. Government agencies (e.g., criminal law enforcement and homeland security

databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. Contractors involved in the development and/or maintenance of TOMIS hardware or software must have at least a SECRET-Level Security Clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

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. TOMIS has been designed to minimize risk to privacy data. Please refer to 11(b) for further information.

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?

TOMIS has received a full 36 month Authorization to Operate (ATO), which expires March 2010.