DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT

The Office of Foreign Missions Information System (TOMIS)

Updated June 17, 2008

Performed by:
Bureau of Administration
Information Sharing Services
Information Programs and Services

What is the purpose of the system/application?

The Office of Foreign Missions Information System (TOMIS) is used to determine and establish immunity and privileges for the foreign diplomatic community located in the United States. Such privileges might include vehicle registration and titling, drivers' licenses, property, sales, gasoline and utility tax exemptions, customs entry, property acquisitions, land use, and travel controls or courtesies.

What is the legal authority for the system?

The following authorities provide for the administration of the program supported by TOMIS:

- Public Law 97-241, The Foreign Missions Act
- Public Law 94-583, The Foreign Sovereign Immunities Act
- Public Law 103-236, Foreign Relations Authorizations Act
- Title 22 U.S.C. Chapter 53, Authorities Relating to Regulation of Foreign Missions
- Vienna Convention of Diplomatic Relations and Optional Protocol (April 18, 1961)

About what categories of individuals is information collected and maintained?

- Foreign diplomatic, consular, administrative, and technical staff; service staff and their immediate families; and honorary consular officers accredited or formerly accredited to the United States.
- United States citizens and legal permanent residents working for foreign diplomatic and consular missions and international organizations within the United States.

What are the sources of the information in the system?

Sources of the information are the individual, their employing foreign government or international organization, and other federal agencies.

What types of information are collected?

- Name
- Sex
- Nationality
- Citizenship
- Type of visa
- Date of birth
- Place of birth
- Residential address
- Employer name and location
- Employee/function title
- Employment start date
- Expected departure date
- Employment termination date
- Vehicle registration data
- Department of State-issued drivers’ license data
- Sales, gasoline, and utility tax exemptions
- Customs clearance data
- Travel controls

Vehicle registration data, Department of State-issued drivers license data, and travel controls information are not collected about individuals who are United States citizens or legal permanent residents.

Customs clearance data are not maintained on individuals who are United States citizens or legal permanent residents, unless the importing of goods is performed by an "honorary consul" for the foreign mission in the performance of their official duties.

How are the accuracy, timeliness, completeness, and relevance of the data ensured?

Verification of information is principally the responsibility of the source entity (e.g., foreign mission, other federal agency). Certain information must be provided in the form of official documentation (e.g., passport, visa, letter of authorization) prior to accreditation of the individual. Form DS-2006, "Notification of Change," is required to report information (or to include information not previously provided) on the original DS-2003, DS-2004, or DS-2005 notification forms. Upon the submission of Form DS-2008, "Notification of Termination," a record's status is changed from "active" to "terminated." If an individual returns to the United States for a subsequent diplomatic or consular assignment, or an employee ends and begins employment with the same or a different foreign mission, their record will be changed from "terminated" to "active."

Will the use of the data be both relevant and necessary to the purpose for which it is collected?

Yes. TOMIS is used only to ensure the fair treatment of foreign diplomats within the United States based on a system of reciprocity for the treatment of United States diplomats in the respective foreign countries.

Will new data or previously unavailable personal data be created through derived data or aggregation of data, and how will it be maintained and filed?

No internal methods are employed in TOMIS that create new, derived, or aggregate information about each individual, and no determinations are made about individuals using such derivative information.

How will records be retrieved? Is a personal identifier used to retrieve records? If yes, describe the identifiers that will be used to retrieve information on the individual.

An individual's record is retrieved by their name or by a unique personal identifying number (PIN) assigned to each record subject. The PIN has no meaning outside of TOMIS, and has no relationship to any other common identifiers such as social security number, passport number, visa number, etc.

What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Reports are only prepared for officers and employees of the Office of Foreign Missions who require them for the performance of their duties, or to support a disclosure authorized by the

applicable Department of State Privacy Act system of records titled STATE-36, Security Records.

What are the retention periods of data in this system?

The Office of Foreign Missions is currently amending its Records Disposition Schedule for TOMIS records because of additional business process automation. Records of all individuals in TOMIS are assigned a status (i.e., "pending," "active," or "terminated") that governs their retention. The majority of hard copy documents (e.g., forms) previously associated with TOMIS no longer exists. Information from hard copy now captured electronically is stored indefinitely in TOMIS. Hard copy is digitally archived and also maintained indefinitely.

What are the procedures for disposition of the data at the end of the retention period? How long will reports are kept? Where are the procedures documented?

The existing Records Disposition Schedule requires that information in TOMIS be retained indefinitely. Supporting hard copy 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 their retention period, reports are destroyed.

Is the system using technologies in ways that the Department of State has not previously employed?

No. TOMIS is a relational database which is not shared by other business applications. No technologies, commonly considered to elevate privacy risk, are employed.

Does the system provide the capability to identify, locate, and monitor individuals? If so, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?

No monitoring of individuals whose information is maintained in TOMIS is performed except as may be accomplished by law enforcement under the authority of a routine use described in Department of State Privacy Act system of records titled STATE-36, Security Records.

If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

Not applicable.

Do related forms include appropriate Privacy Act statements?

All TOMIS forms include appropriate Privacy Act statements.

Who has access to the data in the system?

Only Department of State employees and contractors who have an authorized need for TOMIS in the performance of their duties have access.

What are the criteria for gaining access to the system?

Access to the system is limited to staff of the Office of Foreign Missions. To access TOMIS, the staff member must first be an authorized user of the Department's unclassified computer network. Access to the TOMIS application specifically requires a uniquely assigned user name and password. There is no remote access to TOMIS. Each prospective authorized user must submit a signed user access agreement. The individual's supervisor must sign the agreement certifying that access is needed for the performance of the applicant's duties. The user access agreement includes a rules of behavior where the individual's responsibility to safeguard TOMIS information is described. Completed applications are also reviewed and approved by the TOMIS information system security officer (ISSO) prior to assigning the logon.

Will users have access to all data on the system or will the user's access be restricted?

Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

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

Rules of behavior attached to the user access agreement describe prohibited activities such as browsing. Activity by authorized users is monitored, logged, and audited. All users are required to undergo Department-approved computer security awareness training prior to access and must complete computer security training yearly in order to retain access.

Are contractors involved with the design and development of the system and are they involved with the maintenance of the system?

Yes. All contractors involved in the development, maintenance, and operation of TOMIS must have a Secret Security Clearance and undergo an annual security briefing and Privacy Act briefing from both the State Department and the contracting company. All contracts have approved Privacy Act clauses.

Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

No other systems share data with TOMIS or are interconnected with TOMIS.

Will other agencies share data or have access to the data in this system (Federal, State, local, Other)? If so, how will the data be used by the other agency?

No outside agencies have direct access to the TOMIS database. Agencies desiring information from TOMIS establish a Memorandum of Understanding (MOU) with the Office of Foreign Missions assuring that the information disclosed to the agency is used in accordance with an authorized purpose. The MOU is periodically reviewed for compliance.

Who is responsible for assuring proper use of shared data?

Under the terms of each MOU, the responsibility for assuring proper use is assigned to the information system security officer, and the responsibility may be assigned to others depending on the nature of the MOU.