PRIVACY IMPACT ASSESSMENT

The Office of Foreign Mission Information System

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: December 2022
(b) Name of system: The Office of Foreign Mission Information System
(c) System acronym: TOMIS
(d) Bureau: OFM
(e) iMatrix Asset ID Number: 382
(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 Office of Foreign Missions Information System (TOMIS) is an integrated, custom application system designed to support the Office of Foreign Missions (OFM) and the Office of the Chief of Protocol (S/CPR) in their accreditation and management of privileges and immunity activities as well as their Courtesies of Port (system coordinating USG escort of foreign leaders, Very Important Persons (VIPs) and dignitaries at US ports) and White House Tours programs.

TOMIS is used to electronically process foreign mission notifications and requests for services, and it provides OFM and S/CPR the ability to manage a wide range of benefits and services to the foreign diplomatic community.

OFM and S/CPR use TOMIS to accredit and manage information for Foreign Missions and personnel that work for the Department of State (Department). Once OFM or S/CPR accredits a foreign national in TOMIS, OFM uses the system to manage a range of benefits and services including the issuance of vehicle titles, registrations, driver's licenses, and license plates; processing tax exemption and duty-free customs requests; and to also facilitate property acquisitions within local zoning law restrictions; thus, strengthening bi-lateral relationships between governments.

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

Type of information collected on U.S. persons (USP) and non-U.S. persons (non-USP) by the system:

- Name
- Date of Birth
- Social Security Number (if applicable) – *USP only*
- E-mail Address: Work/Office e-mail address and personal e-mail address
- Employment information (Name of Job/School)
- Visa (if applicable) – *Non-USP only*
- Visa Foil Number (if applicable) – *Non-USP only*
- Gender
- Current Citizenship
- Birth Country
- Birth City
- Birth Citizenship
- Home Address
- Passport – *Non-USP only*
- Supporting Documentation (if applicable) to include:
    - Birth certificate
    - Marriage license
    - Adoption certification
    - Death notice

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

The legal authorities specific to TOMIS, are as follows:

- 22 U.S.C. 4301 et seq. (Foreign Missions Act)
- 22 U.S.C. 288 et seq. (International Organizations Immunities Act)

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

☒Yes, provide:

- SORN Name and Number:
  Office of Foreign Missions Records, State- 81

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  December 17, 2015

☐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.)

If yes provide (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
  A-10-001-04

- Disposition Authority Number:
  N1-059-98-03, item 1

- Length of time the information is retained in the system:
- Information in the database is deleted when no longer needed, as determined, and cleared by the OFM Information Systems Manager.

- Type of information retained in the system:
  - Name
  - Date of Birth
  - Social Security Number (if applicable)
  - Work/ Personal E-mail address
  - Employment information pertaining to jobs working for Foreign Governments in the U.S.

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?
  22 U.S.C. 4301-4316 (Foreign Missions Act)

(d) How is the PII collected?

The PII collected for OFM is collected through eGov,

eGov is an externally facing subcomponent of TOMIS used by the foreign missions to submit requests to the Department. The requests submitted by the foreign missions via eGov are processed within the Department using TOMIS. eGov and TOMIS communicate with each other. eGov has many requests type at foreign mission's disposal, including:

- The Notification of Appointment (NoA), change, and termination
- Driver's Services (Driver's Licensing, Vehicle Registrations/Insurance, Tags/Decals)
- Bonded Warehouse (Duty Free Purchases)
- Tax privileges (Sales Tax, Gasoline Tax, and Utility Tax) and
- Travel (Courtesy of Port, White House Tours, Travel Controls)

Regardless of the request type, the process is the same. The missions generate a particular request in eGov and that request is then processed by the Department using TOMIS.

Any new information about a foreign national is entered into TOMIS by an authorized eGov account holder in the requesting foreign mission through the Notification of Appointment (NoA) process. The information is processed by eGov and verified with the Consular Affair's Consolidated Consular Database (CCD). Once verified, an individual's account is created in TOMIS.

(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.

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

There are multiple levels of checking the accuracy of the data entered. Once the data is submitted by the foreign missions, OFM and S/CPR personnel verify the information while processing the requests/notifications. The Office of Foreign Missions and the Office of S/CPR verifies the information sent by the Mission by referencing the applicant's visa record via the Consular Consolidated Database (CCD). Required information must be provided and validated by documentation (passport, visa, letter of authorization, birth certificate, marriage license etc.) prior to individual accreditation.

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

Yes. Per the Foreign Mission Act (FMA), the foreign missions are required to notify the Department (in our case OFM) of any substantive changes to their living arrangement, personal and/or professional updates. The foreign missions are directed and required by the Department to use OFM's eGov to submit any changes or updates to keep their information as current as possible. The information in eGov is then transmitted to TOMIS for processing.

(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 the information publicly available.

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

The Congressionally mandated mission of OFM is to provide services and benefits to foreign mission members in the United States. The collection of PII has been minimized to only the essential information necessary to locate, contact and serve foreign mission members. Special attention and all required security controls and regulations are applied to the collection, storage, and dissemination of PII.

5. Use of information

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

The PII collected and stored in the system is necessary to the Department's mission to correctly identify accredited mission members to provide them services and benefits.

(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 main purpose of TOMIS is to create, as mandated by the Foreign Mission Act, a central repository for all foreign nationals and employees assigned to work at the Embassies, Consulates, & UN Missions in the United States. This includes information regarding foreign mission properties themselves. With this data stored in a centralized fashion in TOMIS, OFM and the Office of the Chief of Protocol (S/CPR) are better able to provide the foreign community the services and benefits for which they may eligible. Reflection of a correct immunity status, Department of State issued Tax Exemption cards (if eligible), Department of State issued Driver's Licenses, and Bonded Warehouse (Duty Free Purchases) privileges are a few examples.

(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.

6. Sharing of PII

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

Internal: No information is shared within the Department.

External: Information will be shared with the Intelligence Community (IC) to include the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Federal Bureau of Investigations (FBI).

(b) What information will be shared?

Internal: N/A

External: All the PII elements listed in 3(d) will be shared with the IC.

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

Internal: N/A

External: The information is shared with Intelligence Community (IC) agencies for national security purposes.

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

Internal: N/A

External: The IC has a secure tunnel to a reverse proxy server to access web services OFM has created so they can query TOMIS. TOMIS data is encrypted and made available through secure web services. This information does not flow through the CCD.

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

Internal: N/A

External: For any external entity, a MOU is established and approved by the OFM Director before any sharing of data can begin. In addition to the MOU, OFM has only granted strict and direct firewall access to the IC. To connect to the IC, OFM worked with IRM to establish a reverse proxy server in the Department's DMZ enclave. In order to access the proxy server, IC must first connect through the approved firewall access designated by IRM. They can only access from specified IP addresses confirmed by the Department. Once through the firewall and the proxy server, then they can access the OFM APIs to pull data from TOMIS.

7. Redress and Notification

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

Yes, the externally facing web-based eGov system that is used to obtain this information has an approved Privacy Act Statement (PAS). This PAS provides the applicant with notice of what authorizes the Department to collect this information, why the information is being collected, with whom the information will be shared, and whether the information is mandatory. It also provides the applicant with information pertaining to the System of Records Notice (SORN), STATE-81 which governs the collection of this information where the applicant can learn more about how their PII will be utilized.

Individuals cannot enter their own information into TOMIS. eGov transmits any information entered into the system to TOMIS.

(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?

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

Per the Foreign Mission (OFM Authorities: 22 U.S.C. 4301 et seq. (Foreign Missions Act)), the foreign missions are required by law to notify the Department (OFM) of all arrivals into the country along with any significant updates to their status. These updates include relocation, arrival/departure of family member(s), marriage/divorce, visa changes, and births/deaths.

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

OFM's eGov system provides the foreign missions the ability to gain access and update their information. Any updates in eGov will be updated in TOMIS. The foreign mission community knows to contact OFM's Accreditation, Services, and Benefits office (OFM-ASB@state.gov) to address any issue regarding their information. Individuals are informed of these procedures via Circular and Diplomatic Notes that are periodically disseminated by the OFM Front Office.

Additionally, the Department's Privacy Act practices allow for record subjects to gain access to their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the System of Records Notice, STATE-81. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated with the form utilized for data collection.

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

☒Yes ☐No

If yes, explain the procedures.

The foreign missions are instructed to utilize OFM's eGov system to provide any updates to their information. In fact, they are required to do so per the Foreign Missions Act. Individuals can access eGov to update any information they believe to be inaccurate or erroneous. All updates will be updated in TOMIS.

Furthermore, the Department's Privacy Act practices allow for record subjects to correct inaccurate or erroneous information by contacting the Department's Freedom of

Information Act (FOIA) office. Details on this process can be found in the System of Records Notice, STATE-81. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated with the form utilized for data collection.

If no, explain why not.

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

Each year OFM distributes an updated version of the OFM eGov handbook to all the foreign mission community in the United States. This handbook details the eGov application and outlines the requirements to update and/or correct their information. This handbook is updated every year to include any new applications or processes the Department has implemented since its previous distribution.

Details can be found in the System of Records Notice, STATE-81.

8. Security Controls

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

Multi-factor authentication is in use, through inherited OpenNet PIV Card use. Data at Rest encryption is implemented in the Oracle database. OFM applies and adheres to all Department of State information security policies and directives. Regarding the IC, OFM, with the approval and assistance from IRM, has created a secure channel with the inclusion of a reverse proxy server and secure APIs. Through this connection, they can query the TOMIS database.

Access to the system is provided by assigned logon and password. An individual needing to access the information within the system must apply for logon, signed by the individual making the request and the individual's supervisor, indicating that access is needed to perform the individual's assigned job. The application has a "must read" area where the individual's responsibility for safeguarding information is written. This is where the individual signs that he/she has read and understands his/her responsibilities. This completed application is forwarded to the system's ISSO for review and approval prior to assigning the logon. Foreign diplomats are provided access to eGov and are not provided access to TOMIS. Access to TOMIS management functionality is limited to Department of State employees.

(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).

Only Department of State employees (civil or contractor) and government entities OFM partners with (i.e., the Intelligence Community) have access to the system. Each role below has access to all PII in the system. These employees are cleared with at least a Secret clearance. The roles are:

- **TOMIS Users assigned to OFM/ASB (Accreditation, Services, & Benefits) and OFM/PR (Policy & Reciprocity) –** These are core OFM employees that utilize TOMIS routinely as part of their primary job responsibilities. This includes processing transactions submitted by the foreign mission community, detailed querying to determine/confirm immunity levels, and other tasks as needed.
    - **Note:** Department of State staff assigned to (1) The Office of the of the Chief Protocol (S/CPR), (2) United States United Nations in New York (USUNNY), and (3) American Institute of Taiwan (AIT) also have this same privilege even though they are not assigned in OFM. They need this role to process individuals under their purview.

- **TOMIS Users assigned to OFM/PSP (Property & Special Projects)** – This group manages all of the Mission and Property records in TOMIS. They require full access to both the Mission and Property features in TOMIS. All other OFM personnel only have read-only access to this section.

- **Intel Community Users** – To support the Department's National Security agenda, this group has a secure connection to the TOMIS database to download TOMIS data into their system. They have strict read-only access to the entire TOMIS dataset but no access to TOMIS.

- **OFM System Administrator –** This role manages TOMIS from the system perspective. They ensure the required security patches are installed and the security posture as logged in iPost is at acceptable levels. iPost is IRM's application to manage and track the security composure of the Department's network (https://ipost.state.sbu/Default). They also manage account access and account management.

- **Non-OFM TOMIS Users** – These individuals are not assigned to OFM (nor S/CPR, USUNNY, or AIT). This role only has read-only query capabilities.

- **OFM Database administrator** – Database administrators (DBA) are responsible for the daily maintenance, upgrades; patch/hot fix application, backups, and configuration to the database. They have access to all PII.

(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 data in the system is determined by the organizational role of the user and the data access they require to complete their assigned work. For TOMIS Users, access to data is determined by the function they perform in OFM. This is based on the office they work. For those assigned in ASB, they have full access to the Accreditation and Services/Benefits to TOMIS. This includes Accreditation, Tax, Bonded Warehouse, and Department of Motor Vehicles. They have read-only access to the other portions of TOMIS. For those assigned in PR, they have the same roles as ASB but have access to

the policy-related tables to manage reciprocal data and measurements. Those in PSP have similar access as ASB in addition have full access to the Property and Mission Management applications.

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

With regards to TOMIS users, roles are based on their assigned offices and in some cases bureaus. In order to roles to be granted, a formal TOMIS account access form has to be completed and signed by the individual's supervisor. The supervisor specifies on the form what role the user should have to perform their duties.

An individual wishing to access the information within the system must apply for logon, signed by the individual making the request and the individual's supervisor, indicating that access is needed to perform the individual's assigned job. The application has a "must read" area where the individual's responsibility for safeguarding information is written. This is where the individual signs that he/she has read and understands his/her responsibilities. This completed application is forwarded to the system's ISSO for review and approval prior to assigning the logon. Foreign diplomats are provided access to eGov and are not provided access to TOMIS. Access to TOMIS management functionality is limited to Department of State employees.

Regarding the Foreign Mission user (eGov users), first, they only have access to the eGov data entry system. Second, they can only submit requests or transaction for their associated Mission. There is no TOMIS data residing on any of the DMZ server. All of the TOMIS data pertaining to the person's information and all of the business rules and logic reside on the TOMIS servers in the OpenNet. The foreign mission users do not have access to this data. The data that they submit via eGov is temporarily stored on the DMZ servers. After 30 days, the data entered by the foreign mission is pulled into TOMIS and archived. The foreign Mission user cannot access this data since it is stored on the OpenNet servers behind the Department's firewall.

- **TOMIS Users assigned to OFM/ASB (Accreditation, Services, and Benefits) and OFM/PR (Policy and Reciprocity)** access is determined by the office with which they are assigned.
    - This role applies to the individuals who are assigned to S/CPR, USUNNY, and AIT as they need access to the appropriate areas of TOMIS to process transactions for the foreign mission under their purview.

- **TOMIS Users assigned to OFM/PSP (Property & Special Project)** access is determined by the office with which they are assigned. Only individuals in this office have full access to the Mission and Property applications in TOMIS.

- **Intel Community User –** access is determined by the guidelines established in the OFM's Memorandum of Understanding between OFM and the IC. The contents of which are sensitive. Through a secure and direct connection to the TOMIS database, they have full read-only access.

- **Non-OFM User** have very limited access in TOMIS. They have no access to any processing-based applications in TOMIS. They have general querying capabilities and nothing more

- **OFM System Administrator** needs enhanced access to perform their routine duties. They have administrative accounts assigned by IRM to perform routine system such server patching, share drive management and security architecture.

- **OFM Database Administrator** needs enhanced access to perform their routine duties. They have administrative accounts assigned by IRM to perform routine system such database management and patching and software deployment builds.

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

TOMIS 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. Access control lists, which define who can access the system and at what privilege level, are regularly reviewed, and inactive accounts are promptly disabled. 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 functions a particular user performed – or attempted to perform – on an information system.)

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.

An individual wishing to access the information within the system must apply for logon, signed by the individual making the request and the individual's supervisor, indicating that access is needed to perform the individual's assigned job. The application has a "must read" area where the individual's responsibility for safeguarding information is written. This is where the individual signs that he/she has read and understands his/her responsibilities. This completed application is forwarded to the system's ISSO for review and approval prior to assigning the logon. Foreign diplomats are provided access to eGov and are not provided access to TOMIS. Access to TOMIS management functionality is limited to Department of State employees.

(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.

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially.