Submit the completed PIA to
Privacy's SharePoint Customer Center

OFM TOMIS 4.0 PIA

1. Contact Information

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

2. System Information

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

(b) Bureau: M/OFM

(c) System acronym: TOMIS

(d) iMatrix Asset ID Number: 382

(e) Reason for performing PIA: A&A Reauthorization

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

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

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
A&A process is in progress. Estimated date of completion: January 2019.

(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 immunities activities as well as their Courtesies of Port and White House Tours programs. TOMIS is a system 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.

S/CPR uses TOMIS to accredit and manage information for Foreign Missions and Personnel that work for the Department of State (DoS). Once S/CPR or M/OFM 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 also facilitating 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 retained in the system:

- Name
- Date of Birth
- Social Security number (if applicable)
- E-Mail Address; Work/Office E-Mail Address and Personal E-Mail Address
- Home Street Address
- Employment information pertaining to jobs working for Foreign Governments in the U.S.

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

The legal authorities as documented in Office of Foreign Missions Records, State- 81, specific to TOMIS, are as follows:

- OFM Authorities: 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)?

☒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.

N/A

(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 Division 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:

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

- 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)
  - E-Mail Address; Work/Office E-Mail Address and 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) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

- If yes, under what authorization?
Foreign Missions Act
22 U.S.C. 4301-4316

(c) How is the information collected?

- **Notification of Appointment (NOA)**
New information about a foreign national is entered by an authorized eGov System account holder in the requesting foreign mission through the Notification of Appointment (NOA) process. This initiates the creation of a person's account in the TOMIS database. All other processes within TOMIS utilize this data.

- **e-Gov**
The e-Gov system is a data collection program that allows authorized Foreign Mission personnel to submit requests for services to the Office of Foreign Missions and the Office of the Chief of Protocol on line, replacing the paper applications used previously. The e-Gov module is a web-based application in the Department of State's Public DMZ and built using JSP/Java which is served by a WebLogic 8.1 application server. The various services available are menu driven and tailored to meet the user's level of access. The information is collected by filling out a series of on-screen forms and is then stored in an Oracle database as an XML document. Foreign Mission personnel at Embassies, Consulates, and Missions access the e-Gov module via the Internet with their TOMIS e-Gov User IDs and passwords. Business rules and a defined process are used for allocating foreign mission accounts for the e-Gov module. The standard rule is up to two to five

accounts per mission. To qualify for an account, the mission person must be in "active" status in the TOMIS, and therefore have gone through the Protocol accreditation process. Account profiles are managed by OFM through an administration application.

- **OFM and Government Printing Office Interface**
  To improve the quality and security of Office of Foreign Mission's (OFM) Identification Cards, after analysis and research, it was determined that the U.S Government Printing Office (GPO) should produce new cards. There have been modifications made to the TOMIS system to migrate from distributed printing to centralized printing. Within the TOMIS system, print queues are necessary and local printing was disabled. Data transmission from the GPO SFTP server in the GPO DMZ is initiated from The Office of Foreign Missions SFTP server in the State DMZ. Secure Enhanced File Transfer (SEFT) server is used in the State DMZ and has all the security features and requirements needed for secure connection to GPO. Data is archived within the GPO environment and then removed from the GPO DMZ environment to prevent unauthorized file re-transmission. GPO prints and mails the appropriate cards. GPO then sends print confirmation back to OFM. This confirmation is initiated (pulled) from the SFTP server in the DMZ by the TOMIS DB server located in the OpenNet and loaded into the Oracle database in OpenNet.

- **OFM Image Server**
  The purpose of this application is to allow the collection of attachments and supporting documentation to the TOMIS environment. In order to accomplish this goal, the e-Gov application server is used to load images/attachments. This allows the Office of Foreign Missions (M/OFM) and the Office of Chief Protocol (S/CPR) to process all applications and transactions electronically. Allowing the Foreign Missions to submit their applications, along with their supporting documentation, electronically eliminates the need for physical paper, thus increasing production and decreasing processing times. An image/attachment server has been installed in the Database DMZ that initially houses the attachments and supporting documentation Mission users send with their applications. The TOMIS software has been modified to allow for the selection of documents. The only file types that are able to be selected are PDFs and JPEG images. This server has scanning software installed so that each file will be checked for viruses and malicious code. Once the files have been scanned, OFM's image server in OpenNet pulls the attachments from the image server in the State DMZ. Once the attachments have successfully been pulled into OpenNet image server, the documents are deleted from the Database server in the DMZ.

(d) 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

(e) What process is used to determine if the information is accurate?

There are multiple levels of checking the data entered. After entering all the required information into TOMIS, the foreign missions print each subject's information and verify the accuracy with the subject. Once the data is submitted by the foreign missions, M/OFM and Protocol personnel verify the information while processing the requests/notifications. The Office of Foreign Missions and the Office of Protocol 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.

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

Yes, required information must be provided and validated by documentation (passport, visa, letter of authorization, etc.) prior to individual accreditation.

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

No

(h) Is notice provided to the individual prior to the collection of his or her information?

Yes. Notice of the purpose, use, and authority for collection of information submitted are described in the System of Records Notice (SORN) titled Office of Foreign Missions Records, STATE-81. Individuals are also made aware of the collection through a Privacy Act notice available to them through a link on the OFM E-Gov Login web page and are subsequently informed of its approved uses. Oral notice is provided by OFM trainers when instructor led training is provided to Foreign Missions.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?

Individuals do have the right to decline to provide information. However, declining to provide information automatically negates all of their granted immunities and privileges.

- If no, why are individuals not allowed to provide consent?

N/A

(j) How did privacy concerns influence the determination of what information would be collected by the system?

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 reduced to only the essential information necessary to locate, contact and serve to 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 information?

TOMIS contains information regarding all foreign diplomats accredited (officially recognized by the US Government as legal diplomatic representatives of their country) by the U.S. government, as well as employees of foreign and international missions. TOMIS is also used to help determine the citizenship of individuals born to foreign diplomats while in the U.S. who are, thus, potentially ineligible for U.S. citizenship. TOMIS also facilitates vehicle licensing, drivers' licensing, tax information, and security checks.

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 Mission in the United States. This is to include the information regarding the foreign Mission properties themselves. Having this data in a centralized system/database is the primary reason for creation of The Office of Foreign Missions (M/OFM) in the first place. TOMIS was developed to help facilitate this mandate in the Foreign Mission Act.

With this data stored in a centralized fashion in TOMIS, OFM and the Office of the Chief of Protocol (S/CPR) is better able to provide the foreign community the services and benefits they may or may not be eligible for. A few examples of this is to ensure that their immunity status is reflected correctly, provide (if eligible) DoS issued Tax Exemption cards, DoS issued Driver's Licenses, and Bonded Warehouse (Duty Free) privileges.

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

Yes

(c) Does the system analyze the information stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the information?

An aggregation of data from other federal agencies will be gathered to provide a complete picture of the diplomat and his/her family members to ensure that neither the diplomat nor his/her family is a threat to the security of the United States or its citizens. The aggregation includes the collection of information pertaining to criminal activities and abuse of privileges. The different DoS lines of business who use TOMIS and own the data provide requirements for viewing TOMIS data that are then converted into query screens or "canned" reports that are available on the TOMIS menu. Any new reporting needs are given to OFM Systems and new reports are developed. Occasionally, ad hoc queries, using Oracle SQL are

developed based on official requests that are reviewed and approved by OFM Systems management. No data mining tools are available for analyzing data in TOMIS.

(2) Does the analysis result in new information?
No new information results from analysis of information in TOMIS.

(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

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
Consular Affairs (CA) has access to the TOMIS database. Access is granted through the Consular Consolidated Database (CCD). CA employees, subject to Security processes described in Section 8b, Security Controls, are able to view TOMIS information (as described in para: 6(b)) by using a program within CCD. This real-time program as described in para: 6(d), allows CA employees to view TOMIS data through the use of a web browser on OpenNet workstations. No data is electronically transferred from TOMIS to the CCD. TOMIS is used as a fraud detection tool in the passport offices located throughout the United States. Also, OFM has a MOA with the CIA and NLETS to receive a copy of TOMIS data on a monthly basis.

(b) What information will be shared?
Information pertaining to the Mission; individuals' status, position, and travel is shared.

(c) What is the purpose for sharing the information?
TOMIS is used as a fraud detection tool in the passport offices located throughout the United States.

(d) The information to be shared is transmitted or disclosed by what methods?
TOMIS is a web-based application. A user must create a username and password in order to gain access to the data contained within TOMIS. Authorized individuals within Consular Affairs/Passport (CA/PPT) are granted access to TOMIS for the purpose of issuing passports.

(e) What safeguards are in place for each internal or external sharing arrangement?
To receive a TOMIS account, a requester must submit an account request form that has been approved by their office's supervisor. The request form is processed by the OFM System's ISSO. If approved, the request goes to a TOMIS administrator who creates the account. The OFM Helpdesk then sends the requester an e-mail with his or her new account ID. The first time users must call the OFM Helpdesk to obtain their password before they can log on. Regarding any external entity, a MOU needs to be established and approved by the OFM Director before any sharing of data can begin.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Sharing of information within TOMIS is limited to CA/PPT. Potential risk is kept to a minimum in this sharing arrangement with appropriate applied controls. One example of a potential privacy risk resulting from internal sharing would be an accidental public disclosure of information on foreign diplomats in the United States, U.S. Citizens, and Legal Permanent Residents (LPRs) working for foreign governments, such as:

- Name
- Date of Birth
- Social Security number (if applicable)
- Home Street Address; Work/Office E-Mail Address and Personal 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

Another example of a potential privacy risk from internal sharing would be that PII could be accidently corrupted by systems failure during the transmission of data to internal users.

Regarding our external users, the foreign Mission community, we ensure that no TOMIS data resides in the DMZ. The only server they can access is the e-Gov server which contains only the data collection application, e-Gov. All of the TOMIS data is stored on the server behind the firewall on the DoS OpenNet network. This ensures that an external entity cannot access directly or indirectly TOMIS data.

Regarding our internal users (DoS employees), in order to mitigate this risk, all Department employees are required to undergo privacy and cyber security training. Users of TOMIS in DS and CA/PPT have all received privacy and cyber security training, and are familiar with the Department of State's Rules of Behavior for accessing systems with PII.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

TOMIS contains Privacy Act-covered records. Notification and redress are, therefore, rights of record subjects. Procedures for access are published in the system of records notice identified in section 3 above, and in rules published at 22 CFR. The procedures

instruct the individual how to inquire into the existence of such records, how to request access to their records, and how to request amendment of their record.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

TOMIS contains Privacy Act-covered records. Notification and redress are, therefore, rights of record subjects. Procedures for access are published in the system of records notice identified in section 3 above, and in rules published at 22 CFR 171.31. The procedures instruct the individual how to inquire into the existence of such records, how to request access to their records, and how to request amendment of their record.

If no, explain why not.

N/A

(c) By what means are individuals notified of the procedures to correct their information?

Procedures for notification and redress are published in the system of records notice identified in section 3 above, and in rules published at 22 CFR 171.31.

8. Security Controls

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

For internal DoS Employees, 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 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. Access to TOMIS management functionality is limited to Department of State employees. The following Department of State 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
- 12 FAM 629.3-3 Access Controls

Regarding the foreign Mission users, they go through a more rigorous vetting process before they are granted access to the external e-Gov application. They first must submit form DS-4140 (OMB 1405-0105) to the OFM e-Gov HelpDesk. The form must be

completed in its entirety. The user must first be accredited by the Office of the Chief of Protocol and be in "active' status in the TOMIS database. The HelpDesk checks to see if he/she is actually accredited to the submitting Missions. Another check is that the form must have a copy of the Mission's Seal as well as the Chief of Mission signature. This person as well must be in "active" status. All of the measures need to be in place before an e-Gov account is granted to a foreign Mission member.

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

Regarding internal DoS users, 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 Department of State mandated security controls.

Regarding the external users (foreign Mission members), they are only allowed to submit and view transactions that are for their Missions. For instance, a Canadian Embassy e-Gov account holder cannot view any record from the Switzerland Embassy. They can only submit for the Mission. We also limit how many e-Gov account any one Mission can have. Per rule, an Embassy can have up to 10 e-Gov accounts (depending on the population of the Embassy) and a maximum of five e-Gov accounts per Consulate.

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

For both e-Gov and TOMIS, 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. 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 particular 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.

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 Department of State mandated security controls.

(d) Explain the privacy training provided to authorized users of the system.

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

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

Multi-factor authentication is in use, through inherited OpenNet PIV Card use. All electronic transfer of information is accomplished by secure processes (SFTP). Data at Rest encryption will be implemented in the 3rd quarter 2019.

OFM applies and adheres to all DoS information security policies and directives, specifically the following:

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

(f) How were the security measures above influenced by the type of information collected?

The private nature of some of the TOMIS information collected and the small percentage of this type of information collected by TOMIS, caused OFM to be cognizant of adhering to the required security controls, regulations and the additional security constraints in place due to the collection of PII. Only a small percentage of TOMIS information is PII; however all TOMIS information is secured and protected to the same extent as PII.

9. Data Access

(a) Who has access to data in the system?

For internal DoS users, 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 that access is needed to perform the individual's assigned job. 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 e-Gov and are not provided access to TOMIS. Access to TOMIS management functionality is limited to Department of State employees with a need to see the information.

For external foreign Mission users, they must first be rigorously vetted before obtaining an e-Gov account. Once their account is created, they can only view those transactions that are submitted by their assigned Mission.

(b) How is access to data in the system determined?

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. All TOMIS/e-Gov users' profiles contain the roles/permissions the user is granted. These roles/permissions are determined by the user's Mission in the case of e-Gov (Embassies, Consulates, U.N. missions, etc.) and the user's DoS office (OFM/PTSB, OFM/DMV, Protocol, etc.) and their work functions (Tax, Property, Benefits, Drivers' Services, Vehicle Registration, Vehicle Insurance, etc.) in the case of TOMIS. For the Foreign Mission using e-Gov, again, they can only create/view those transactions associated to their Mission.

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.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

No. All users will not have access to all data in the system. User access is restricted by the role of the user and the data access they require to complete their work.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the 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 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 e-Gov and are not provided access to TOMIS. Access to TOMIS management functionality is limited to Department of State employees.

Regarding the Foreign Mission user (e-Gov users), first, they only have access to the e-Gov 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 e-Gov 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 hidden on the OpenNet servers behind the DoS firewall.