PRIVACY IMPACT ASSESSMENT

User Manager WebSecurity (UMWS) PIA

1. Contact Information

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

2. System Information

(a) Name of system: User Manager WebSecurity

(b) Bureau: Consular Affairs

(c) System acronym: UMWS

(d) iMatrix Asset ID Number: 4377

(e) Reason for performing PIA: Click here to enter text.

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

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?
The system received an Extension of Authorization to Operate (ATO) on May 8, 2017. The authorization is valid until rescinded or the expiry date of July 31, 2019.

(c) Describe the purpose of the system:

The UMWS supports the Bureau of Consular Affairs passport mission requirements and operations. UMWS is a single sign-on application with a monitoring capability that allows Department of State (DoS) users to be assigned privileges/accounts to access Passport systems to perform specified tasks supporting the management of passport services. The UMWS application is used to manage user accounts (including profile data and roles) and to capture user event logs, sensitive PII record searches, and information in the Privacy Reporting Database for auditing purposes.

The user interface for UMWS system is via the Microsoft Internet Explorer browser. The UMWS application is used to manage user accounts for the following applications:

- Passport Information Electronic Records System (PIERS) Record Services (RS) and all RS Web applications
- Management Information System (MIS)
- Passport Records Imaging System Management (PRISM Web)
- Passport Lookout Tracking System (PLOTS)
- Travel Document Issuance System (TDIS) Web Inquiry

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

- Name
- Place of Birth
- Date of Birth
- Social Security Number
- Passport Number
- Family Member (Parents) information (possibly)

UMWS DoS personnel access accounts: Name, Business Phone Number, Office Location, Office Email Address, Business Title.

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

- 22 U.S.C 2651a (Organization of Department of State)
- Executive Order 11295, August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- Executive Order 9397, November 22, 1943; Executive Order 13478, November 18, 2008
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- Executive Order 11295, August 5, 1966; (Authority of the Secretary of State in granting and issuing U.S. passports)

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

☒Yes, provide:

- SORN Name and Number:
  STATE-26 - Passport Records, March 24, 2015
  STATE-05 - Overseas Citizens Records and Other Overseas Records, September 8, 2016

☐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 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, Length of time the information is retained in the system, and Type of information retained in the system:

A-03-003-12 System Access Records
Description: These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: user profiles, log-in files, password files, audit trail files and extracts, system usage files, and cost-back files used to assess charges for system use.

Disposition: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

DispAuthNo: DAA-GRS-2013-0006-0004 (GRS 3.2, item 031)

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 (DoS business information to assigned privileges to access Passport systems to perform specified tasks).
☐ 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?

26 U.S.C. 6039E (Information Concerning Resident Status) and
22 U.S.C. 2714a. (f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
Executive Order 9397, November 22, 1943; Executive Order 13478, November 18, 2008

(c) How is the information collected?

No information is entered into UMWS by applicants. UMWS data is from other CA systems (CA PIERS, MIS, PRISM Web, PLOTS, and TDIS Web Inquiry) to UMWS via the MS Internet Explorer browser.

(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.

(e) What process is used to determine if the information is accurate?
No information is entered into UMWS by applicants. Information in the Privacy Reporting Database in UMWS is transmitted from other CA systems listed in paragraph 3(c). Privacy Information in these systems is checked for accuracy against submitted documentation, administrative procedures and other CA systems.

Information to establish DoS user accounts are verified for accuracy by the supervisor submitting Account Request documentation for DoS personnel to provide access to specified information via UMWS.

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

No information is entered into UMWS by applicants.

The Privacy Reporting Database information in UMWS is retrieved from the CA systems listed in paragraph 4(c). Currency is the responsibility of the individual completing the application for specific services via the CA systems. Applicants can modify or amend records by accessing the website where the record was established in the source CA system. Information can also be updated during the adjudication process for services requested.

DoS personnel user account information is updated by the respective supervisor.

(g) Does the system use information from commercial sources? Is the information publicly available?
No, the system does not acquire information from commercial sources nor is it publicly available.

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

N/A. UMWS does not collect information directly from the public for the Privacy Reporting Database. Information is provided from other internal systems identified in paragraph 4(c). The notice is provided to applicants upon submission of applications for passport services. Individuals grant consent via the passport application process for the specified service requested. All application forms containing PII have Privacy Act Statements stating the purposes for soliciting the information on the form. Additionally, notice of the use of personal information is provided through the two SORNs mentioned above in paragraph 3(f), STATE-26 and STATE-05.

(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?

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

UMWS does not collect information directly from the public. Information in the Privacy Reporting Database in UMWS is acquired from other internal CA systems identified in paragraph 4(c).

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

The Department of State understands the need for PII to be protected. Accordingly, the PII in UMWS is handled in accordance with federal privacy regulations and is the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. The PII is limited to only what is required for the system to perform the functions for which it is intended to support, providing structured query capabilities on the management and processing of passports.

UMWS does not collect information from the public.

5. Use of information

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

UMWS information is used by the Bureau of Consular Affairs Directorate of Passport Services, other Consular Affairs offices, and the Bureau of Diplomatic Security to manage the processing of passports.

The personnel PII in paragraph 3(d) is used to provide access privileges to specific passport information in order to perform functions and monitor search activity of customers' sensitive information for auditing purposes.

(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, the PII assists in the operations and management of the passport process. UMWS tracks user activity and access to specified passport systems ensuring execution of role-based permissions in conducting passport operations.

(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?
(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

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
The information is shared internally within the Bureau of Consular Affairs personnel via CA passport systems to perform passport tasks associated with the following systems:

- UMWS interfaces with CA PIERS, MIS, PRISM Web, PLOTS, and TDIS Web Inquiry, allowing users to be assigned privileges to access systems to perform only specific approved functions.
- The CA UMWS does not share information externally.

(b) What information will be shared?
Information in paragraph 3(d) is shared to grant permissions to access specific CA Passport systems to perform functions and to log search activity of sensitive information by DoS personnel.

(c) What is the purpose for sharing the information?
The information is shared to assist the Department of State in managing the activity of the passport application process and to perform required functions to process passports by the various passport offices.

(d) The information to be shared is transmitted or disclosed by what methods?
All information is shared using Department of State approved secure Information System Connection Ports, Protocols and Services. All of the CA passport systems addressed in paragraph 6(a) reside on the Department's secure internal network, OpenNet.

Information is shared internally via systems and accessed by CA personnel to support passport operations. Internal information is shared by direct secured communications (database to database) using transport and message level security interfaces with other Consular Affairs systems.

(e) What safeguards are in place for each internal or external sharing arrangement?
Supervisors along with information system security officers (ISSOs) determine the access level depending on job function and level of clearance.

Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of Sensitive but Unclassified (SBU) information. Access to electronic files is protected by inherited security controls from the DoS domain infrastructure. All accounts are under the supervision of system managers. Audit trails track and monitor usage and access. Defense in depth is deployed as well as roles assigned based on least privilege. Finally, regularly administered security and privacy training informs authorized users of proper handling procedures.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Privacy concerns regarding the sharing of information focus on two primary sources of risk:

1) Accidental disclosure of information to non-authorized parties:

   Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to- know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

2) Deliberate disclosure/theft or information to non-authorized parties regardless whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, Sensitive but Unclassified, and all higher levels of classification, and signing a user agreement.

2) Strict role based access control, based on approved roles and responsibilities, authorization, need- to-know, and clearance level.

3) Implementation of management, operational, and technical controls regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
The system contains Privacy Act-covered records; therefore, notification and redress are the right of record subjects. Procedures for notification and redress are published in the following System of Records Notices (SORNs):

SORN STATE-26: Requests for passport records issued from 1925 to the present should be submitted to the Department of State; Passport Services; Law Enforcement Liaison Division; Room 500; 1111 19th Street, NW., Washington, DC 20522-1705.

SORN STATE-05: Requests for Overseas Citizens Records and Other Overseas Records are to be submitted to the Director; Office of Information Programs and Services, A/GIS/IPS; SA-2, Department of State; 515 22nd Street NW., Washington, DC 20522-8100.

Individuals may also visit the Department of State public site and/or the Department of State Privacy Act/FOIA web site for the privacy policy which includes instructions on how to obtain access to records by contacting the listed offices by phone or by mail.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.
The CA UMWS does not collect information directly from the public. The information is acquired from other CA systems listed in paragraph 3(c). Individuals must follow processes of the source systems used to apply for the specific passport service to request correction of information. Notice to correct personal information is provided at the source site where applicants apply for specific services.

Individuals can also follow procedures outlined in SORNs STATE-26 and STATE-05 as depicted in paragraph 7(a) above and procedures posted on the Department of State's Privacy website at www.state.gov/privacy.

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

The CA UMWS does not collect information from the public. The information is acquired from other CA systems listed in paragraph 3(c). Individuals must follow processes of the source systems used to apply for the specific passport service to request correction of information. Notice to correct personal information is provided at the source site where applicants apply for specific services.

Individuals can also follow procedures outlined in SORNs STATE-26 and STATE-05 posted on the Department of State's Privacy website at www.state.gov/privacy.

8. Security Controls

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

The CA UMWS is secured within the Department of State intranet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

UMWS personnel access accounts are created and assigned the appropriate level of privileges approved by the supervisor. The user can then perform the tasks associated with the privileges authorized. Additionally, the UMWS monitors user activity for certain types of sensitive record searches and stores a log of these searches in the Privacy Reporting database. This log records information about the user who performed the search and the details of the search results, including all PII. This information is used to track DoS user activity for auditing.

CA Systems are configured according to State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and are tracked until compliant or acceptably mitigated.

(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.

To access the system an individual must be an authorized user of the Department of State's unclassified internal network (OpenNet) which requires a background investigation and an application approved by the individual's supervisor and the Information System Security Officer. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports to be restricted. Information System Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the UMWS audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data. If an issue were to arise, administrators of the system would review (audit) the logs that were collected from the time a user logged on until the time he/she signed off. This multilayered approach to security controls greatly reduces the risk that PII will be misused.

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

In accordance with Department of State computer security policies, mandatory security (PS800 Cyber Security Awareness) and privacy (PA459 Protecting Personally Identifiable Information) training is required for all authorized users. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(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.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and reporting, identification and authentication of organizational users, information system monitoring and numerous media controls.

The Information Integrity Branch (IIB) provides administrative life-cycle security protection for the Department of State's information technology systems and information resources. All systems must comply with all guidelines published by Systems Integrity Division, in addition to all Security Configuration Guides published by Diplomatic Security. Adherence to these guides is verified during the system's Assessment and Authorization process.

The CA UMWS uses Transmission Control Protocol/Internet Protocol TCP/IP for data transport across the network. Data in transit is encrypted. The TCP/IP suite consists of multiple layers of protocols that help ensure the integrity of data transmission, including hand-shaking, header checks, and re-sending of data if necessary.

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

The information in UMWS contains PII of U.S. Citizens, Legal Permanent Residents (LPRs) and business information of DoS personnel. Due to the sensitivity of information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing.

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above in paragraph 8(e) are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

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

The following personnel have access to these systems:

Approved UMWS DoS Users - Department of State employees and contractors working domestically and overseas in connection with processing passports; System Administrators and Database Administrators.

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

An individual's job function determines what data can be accessed as approved by the supervisor and the Information Systems Security Officer (ISSO). Access is role based and the user is granted only the role(s) required to perform officially assigned duties.

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

Procedures and controls are documented in the System Security Plan. The Plan includes information and procedures regarding access to data in the CA UMWS.

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

There are three types of CA UMWS user roles: OpenNet Users (Department of State employees and contractors), System Administrators and Database Administrators. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

CA UMWS application Users- Access to CA UMWS is restricted to cleared Department of State direct hire and contractor employees. CA UMWS users are assigned access privileges based on their job functions. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. The UMWS application is used to manage user accounts, passwords, and privileges for passport applications of the systems listed in paragraph 6(a).

The System Administrator- The System Service and Operations Project Manager completes the CA/CST System Administrator Account Request Form. The Project Manager reviews the role and approves, authorizing the account to be established and activated in UMWS. System Administrators have logon identifications associated with their name that allows for user auditing. Administrators are authorized to access the system for the purpose of performing maintenance, troubleshooting technical issues, installing software, and patches. They have logon identifications associated with their name that allows for user auditing.

Database Administrators- UMWS Database Administrators (DBA) are responsible for the daily maintenance, upgrades; patch/hot fix application, backups and configuration, to UMWS. DBA access is controlled by the Integrated Services (IS) team through the use of access control lists (ACLs) as established by the system administrators. DBAs are authenticated using Windows operating system authentication. The ISSO is responsible for reviewing and approving DBA accounts. Database administrators have logon identifications associated with their name that allows for user auditing.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data? CA UMWS information is protected by multiple layers of security controls including:

- Access control policies and access enforcement mechanisms control access to PII.

- Separation of duties is implemented; access is role based as required by policy.

- CA UMWS System & Database Administrators and internal users have access via OpenNet from the Department of State configured workstations. Users must dual factor authenticate utilizing PIV/CAC and PIN to access data. Users are uniquely identified and authenticated before accessing PII and while logged in can be traced to their actions performed.

- Least Privileges are restrictive rights/privileges or accesses of users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

- System and information integrity auditing are implemented to monitor and record unauthorized access/use of information.

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing.