PRIVACY IMPACT ASSESSMENT

Waiver Review System (WRS)

1. Contact Information

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

2. System Information

(a) Name of system: Waiver Review System

(b) Bureau: Consular Affairs

(c) System acronym: WRS

(d) iMatrix Asset ID Number: 415

(e) Reason for performing PIA:

☐ New system (as a consolidated boundary)

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

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?

This system is undergoing a reauthorization and is expected to receive an Authorization to Operate (ATO) in Spring 2018.

(c) Describe the purpose of the system:

This system is used to track the status of applications for exchange visitors with J Visas who seek to waive the two-year foreign residency requirement (212(e) of the Immigration and Nationality Act), including processing waiver requests and making waiver recommendations to USCIS. WRS includes two subsystems: the J Visa Waiver Online (JWOL) and Internet Status Check System (ISCS).

-The JWOL web site allows exchange visitors who seek a waiver of 212(e) to reserve a case number and begin the paperwork for their request to the Department of State Waiver Review Division. Data entry is controlled to ensure an error-free submission. The JWOL creates a bar-coded, hard copy only form that the applicant mails in for processing by the Waiver Review Division. When the form is initially processed, the applicant is provided with a Waiver Review Case Number via return mail.

-Any applicant (exchange visitor) who has a Waiver Review Case Number from JWOL can use the ISCS website to check the status of his/her case after it has been scanned/processed by WRS. The case number from JWOL will scan but nothing will display until WRS scans or processes it. The ISCS provides two text fields offering the status of the two most recent actions on the case and the date the information was retrieved. No personally identifiable information (PII) is collected, processed, or retained by ISCS.

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

Foreign Nationals: names, birthdates, phone, address, email, ID number

US citizens/LPR: Information for the applicants: their attorney, representatives, and/or organizations; specifically name, address and phone number, and email address. [DS Form 3035]

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

- 5 U.S.C. 552a, Privacy Act of 1974, as amended
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State);
- 8 U.S.C. 1151-1363a (Title II of the Immigration and Nationality Act of 1952, as amended)
- 22 C.F.R. Parts 40-42, and 46 (Visas)
- 22 U.S.C. 2651a (Organization of the Department of State);
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996, PL 104-208, Div. C, September 30, 1996
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PL 107–56, October 26, 2001
- Enhanced Border Security and Visa Entry Reform Act of 2002, PL 107-174, May 14, 2002

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

☒ Yes, provide:

- State-39, Visa Records; October 25, 2012
- State-26, Passport Records; March 24, 2015
- State-05, Overseas Citizens Service Records, September 8, 2016
- State-77, Country Clearance Records, October 3, 2011

WRS

☐No, explain how the information is retrieved without a personal identifier.

(g)Do the existing SORNs 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)):
- Length of time the information is retained in the system:
  Retention depends on the type of record in the listed schedules. Specific information may be obtained from: http://infoaccess.state.gov/recordsmgt/recdispsched.asp.
- Type of information retained in the system: Information relating to appointments, the Diversity Visa Lottery, J Visa waivers, and tracking visa applications

  A-14-001-26 Visa- Waiver Review System: Cut off at final determination. Destroy 11 years after cut off.
  B-09-002-04a Non-Immigrant Visas – Issuances (Cut off at end of calendar year when issued. Destroy 25 years after issuance.
  B-09-002-39a Non-immigrant Visa Computer –Assisted Processing System: After 1 year, archive a copy of log files, data, and reports onto a disk, tape, CD, or other electronic media (to allow records to be used in future fraud investigations). Verify copy, then destroy/delete on-line reports.
  B-09-002-40a Diversity Visa Applicant Control System (DVACS): Destroy when active use ceases.

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 (are US citizens or aliens lawfully admitted for permanent residence)

☐U.S. Government/Federal employees or Contractor employees

☒Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐Yes

☒No --- None of these systems collect SSNs

- If yes, under what authorization?

(b) How is the information collected?

The information is collected from applicants who use the J Visa Waiver Recommendation Application on the JWOL web site.

(c) 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.

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

Accuracy of the information provided on the forms is the responsibility of the applicant. Applicant information is vetted during the normal course of waiver request processing.

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

Ensuring the information provided on the forms remains current is the responsibility of the applicant upon submission of the waiver request. Applicant information is also vetted in the normal course of waiver request processing to check that the information is current.

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

These systems do not use commercial information, publicly available information or information from other Federal agency databases.

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

Both the JWOL and ISCS websites display a Privacy Act Statement (PAS) and a Computer Fraud and Abuse Act Statement prior to data being collected, thereby notifying individuals of why their information is being collected and how it will be used.

(h) 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? (Security Control: IP-1)

Consent is by OPT-IN – Individuals see the screen with the PAS and Computer Fraud and Abuse Statement and must click to Agree before data may be entered. Individuals may decline to enter the information; however, if the mandatory fields are not filled in, the individual may not be provided the service he/she is seeking.

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

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

The PII items listed in Question 3d are 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. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function for which it was intended.

5. Use of information

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

The intended use for the information is to assist with tracking the status of applications for exchange visitors with J Visas who seek to waive the two-year foreign residency requirement (212(e) of the Immigration and Nationality Act).

(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 information is used according to the system's purpose.

(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?
The system does not analyze information
(2) Does the analysis result in new information? ☐Yes ☒No

(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.

Internally, the information is shared with the Consular Consolidated Database (CCD) and Consular Shared Tables (CST), which is bi-directional. There is no external sharing.

(b) What information will be shared?

WRS shares the name, address, phone number, and email address of exchange visitors with J Visas who seek to waive the two-year foreign residency requirement.

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

Information is shared to cross check data, such as names and visa application numbers residing in the CCD and the CST, in order to adjudicate and process waivers. CCD subsequently provides the waiver recommendations to the Department of Homeland Security Citizenship and Immigration Service (CIS).

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

The information is shared using Department of State approved Information System Connection Ports, Protocols and Services.

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

Internal sharing requires a connection agreement and OpenNet users with privileged role based access to manage the connection.

(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:

a. Accidental disclosure of information to non-authorized parties
b. Deliberate disclosure/theft of information regardless whether the motivation was monetary, personal or other.

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.

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

- 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.

- Strict access control based on roles and responsibilities, authorization and need-to-know

- System authorization and accreditation process along with continuous monitoring. Security controls are implemented for management, operational, and technical functions 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?

Waiver applicants can enter their case numbers provided upon completion of their initial application to check their status and information entered in the system.

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

☒Yes ☐No

If yes, explain the procedures.
During the adjudication process applicants can correct information during their interview and/ or by responding to a letter being notified that a correction is needed.

If no, explain why not.

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

Individuals are notified of the procedures to correct records in these systems by a variety of methods:
(1) Instructions on application forms and web pages (or link to instructions)
(2) Upon completion of their waiver application on the J Visa Online site.
(3) During their interview
(4) Being notified by letter that a correction is needed

Each method contains information on how to amend records and who/what office to communicate with as well as contact information.

8. Security Controls

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

The system 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.

Applications are configured according to the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable 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.

(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, persons must be authorized users of the Department of State's unclassified network which requires a background investigation and an application approved by the supervisor and 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 (PIV)/Common Access Card (CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

A system use notification ("warning banner") is displayed before logon is permitted and informs the user of system use and restrictions with every login. Users are required to read and actively click a button indicating understanding and agreement before logon can be completed. Users must first authenticate to OpenNet using their Department of State One Badge (PIV Card) via the above process. The user can then proceed to logon to the CCD Web Portal using their CCD credentials (User Name, User Password and User Location). Once logged on to CCD, the user can click the Waiver Review System from the menu to launch.

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 that are to be restricted. 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?

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with Department of State Security Configuration Guides, conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and Federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with Department of State Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with Department of State Security Configuration Guides, auditing is 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 audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

Operating System-Level auditing is set in accordance with the Department of State Security Configuration Guide. The Operating System (OS) interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. In addition to the security log, the system log and application logs provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

(d) **Explain the privacy training provided to the authorized users of the system.**
In accordance with Department of State computer security policies, mandatory annual security/privacy training is required for all authorized users, including security training and regular refresher training. Annually, each user must complete the Cyber Security Awareness Training and pass the PA-459 course, entitled "Protecting Personally Identifiable Information." The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree in writing to the rules and to 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.
To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. All data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Information is destroyed when no longer needed. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) How were the security measures above influenced by the type of information collected?
Because of the potentially adverse consequences to organizations or individuals whose PII has been breached or exposed to unauthorized users, which may include inconvenience, distress, or damage to standing or reputation, financial loss, harm to Department programs or the public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violations, the security measures listed above were implemented to secure the data in the system.

9. Data Access

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

System Administrators, Web Administrators, Database Administrators, and WRS OpenNet Users have access to data in the system based on their prescribed roles and requirements.

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

Access is determined based on duties to be performed, which are approved by the supervisor. Access is role based and 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

Information is documented in the System Security Plan. The Plan includes information regarding system access to data.

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

Users other than administrators will not have access to all data in the system. 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.

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

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

-Separation of duties is implemented

-Least Privileges are restrictive rights/privileges or accesses users need 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.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN).