Waiver Review System (WRS)
Privacy Impact Assessment

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

a. Date PIA was completed: September 8, 2009

b. Name of system: Waiver Review System

c. System acronym: WRS

d. IT Asset Baseline (ITAB) number: 415

e. System description (Briefly describe scope, purpose, and major functions):

The Waiver Review System (WRS) is designed to support the Bureau of Consular Affairs, Visa Office, Legal Waiver Division (CA/VO/L/W). WRS is an information system used to track the application and adjudication process of exchange visitors, with J Visas seeking to waive the two-year foreign residency requirement 212(e) of the Immigration and Nationality Act. WRS consists of two additional subsystems: the J Visa Waiver Online (JWOL) and Internet Status Check System (ISCS).

The JWOL web site allows exchange visitors desiring 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 for a waiver recommendation. The exchange visitor or representative controls the data entry to ensure an error-free submission. The JWOL creates a bar-coded document that will facilitate processing by the Waiver Review Division. Any applicant (exchange visitor) who has a Waiver Review Case Number can use the ISCS website to check the status of their case. 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.

f. Reason for performing PIA:

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

g. Explanation of modification (if applicable): N/A

h. Date of previous PIA (if applicable): May 2007

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

WRS primarily collects data on foreign nationals as part of the J visa waiver application process. As such, the information provided by the applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

Because J visa waiver applicants themselves are not U.S. persons (that is, U.S. citizens or legal permanent residents), they are not covered by the provisions of the Privacy Act. However, a WRS record may include PII about persons representing the J visa waiver applicant who are US citizens or legal permanent residents.

This PII data on U.S. citizens may include the following: Attorney, Representative, and/or Organization Name, address and phone number, fax number, and email address. The source of information is the exchange visitor or representative (e.g., attorney) completing the form on the visitors behalf.

b. How is the information collected?

The information is collected in the J Visa Waiver Recommendation Application on the JWOL web site.

c. Why is the information collected and maintained?

To allow a J-1 exchange visitor ("EV") to request a waiver of the two-year home country requirement.

d. How will the information be checked for accuracy?

Information is checked for accuracy during processing by the Waiver Review Division.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)
- Mutual Educational and Cultural Exchange Act of 1961

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Due to strict security controls that are required to be in place before operation of the system, no identified privacy risks are associated with this system. The controls are subject to rigorous testing and formal certification and accreditation (C&A). Authority to operate is authorized by the Chief Information Officer (CIO) for the Department of State. Security controls are reviewed annually and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application. Only authorized users with a need to know are granted access to WRS.

4. Uses of the Information

a. Describe all uses of the information.

Waiver officers use the information managed by WRS to:

- Notify applicants on receipt of documentation;
- Determine what documentation remains outstanding; and
- Completes the case, when all required documentation has been submitted, by rendering a favorable or not favorable waiver recommendation.

b. What types of methods are used to analyze the data? What new information may be produced?

As part of the waiver recommendation process, WRS interfaces with the Consular Lookout and Support System (CLASS) to perform name checks and with the Consular Consolidated Database (CCD) to associate waiver information to visa information. The result of the name check request (hit or no hit) is used in making a waiver recommendation that can be one of the following:

- Favorable
- Not Favorable
- Subject
- Not Subject
- Inactive
- Withdrawn
- Ineligible
- Favorable
- Unfavorable

In addition, WRS generates a variety of reports for statistical and management purposes.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

WRS does not use commercial, publicly available, or information from other Federal agency databases.

d. Are contractors involved in the uses of the PII?

WRS is a government-owned system. Government personnel are primary users of WRS. Contractors are involved with the design and development of the system. All users are required to pass annual computer security/privacy training and to sign non-disclosure and rules of behavior agreements.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

User access to information is restricted according to job responsibilities and requires managerial level approvals. 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. The Department of State's Consular Consolidated Database is used to maintain user accounts and user roles for the WRS application. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

5. Retention

a. How long is information retained?

Record retention varies depending upon the type of record. Files of closed cases are disposed of in accordance with published Department of State record schedules as approved the National Archives and Records Administration (NARA).

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with published Department of State record schedules as approved the National Archives and Records Administration.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

WRS information is shared with Department of State Adjudicators who are the individuals responsible for processing a waiver application; typically, the Waiver Review Officer.

In addition, WRS interfaces with the Consular Lookout and Support System (CLASS) to perform name checks and the Consular Consolidated Database (CCD) to associate waiver information with visa information.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

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. All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. Access to electronic files is protected by passwords and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Access to information is controlled by application access controls. User training at the application level is delivered annually in accordance with internal Department of State regulations.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Waiver recommendations are forwarded to the Department of Homeland Security (DHS) Citizenship and Immigration Service (CIS) for a final decision. While the Waiver Review Division is responsible for issuing recommendations, DHS has the final authority to approve or deny waiver requests.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

WRS data is replicated to the Consular Consolidated Database (CCD). From CCD, the recommendation letter is forwarded to Customs and Immigrant Service (CIS) Computer Linked Automated Information Management System, Version 3 (CLAIMS-3) and CLAIMS-4 via a CCD web service call. CLAIMS supports the functions required for the receipt and adjudication of applications and petitions for immigration benefits.

Each data sharing arrangement with federal agency partners is covered by a written agreement in the form of a Memorandum of Understanding (MOU) or exchange of letters as well as technical documentation including an interface control document and interagency security agreement. Data is sent through encrypted lines.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

WRS information is shared with U.S. government agencies with a statutory requirement and in accordance with confidentiality requirements under INA section 222(f). Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly adhered to in order to ensure any risk is addressed through the user-authorization process.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

- Visa Records State -39

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

The information provided by the J visa waiver applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

The J Visa Waiver Recommendation application form provides a statement that the Department of State assures will not:

- Obtain personal identifying information about you, unless you choose to provide such information; and
- Share any information it receives with any outside parties, except for authorized law enforcement investigations, or as otherwise required by law.

Also, notice is provided in the System of Records Notice (SORN) Visa Records, State-39.

b. Do individuals have the opportunity and/or right to decline to provide information?

Information is given voluntarily by the applicants or his/her representative.

Individuals who voluntarily apply for a waiver must supply all the requested information and may not decline to provide part or all the information required, if they wish services.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Applicants may decline to provide information; otherwise, they have no right to limit the use of the information (consistent with the system's disclosed purposes and uses).

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The information provided by the applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

The information provided on the form and in the SORN regarding visa records fully explain how the information may be used by the Department and how it is protected.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

The information in WRS is considered a visa record subject to confidentiality requirements under INA 222(f).

If individuals believe there is incorrect information regarding the record of their waiver cases, they are instructed to contact VO Public Inquiries at (202) 663-1225, and are given the opportunity to submit amended information.

WRS information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a), and individuals may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have

been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

To the extent information in WRS may be Privacy Act-covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements. Therefore, this category of privacy risk is appropriately mitigated in WRS.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to WRS is limited to authorized Department of State users that have a justified need for the information in order to perform official duties. To access the system, authorized users must be an authorized user of the Department of State' unclassified network. Access to WRS requires a unique user account assigned by a Certifying Authority. Each authorized user must sign a user access agreement before being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

User access to information is restricted according to job responsibilities and requires managerial level approvals. 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. The Department of State's Consular Consolidated Database (CCD) application is used to maintain user accounts and user roles for the WRS application. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

Internet based users of ISCS and JWOL only have access to these systems for the purpose of completing a J Visa Waiver Recommendation Application or checking the status of their application once their application has been assigned a Case Number. These users are presented with a Computer Fraud and Abuse Act Notice and Privacy Act Notice that they must take explicit action to accept prior to using these

systems. These notices outline the expected use of these systems and how they are subject to monitoring.

b. What privacy orientation or training for the system is provided authorized users?

Users internal to the Department must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training.

Internet based users must read and accept the Computer Fraud and Abuse Act Notice and Privacy Act Notice that outline the expected use of these systems and how they are subject to monitoring prior to being granted access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Access control lists, which define who can access the system and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. (An audit trail provides a record of all functions authorized users perform--or may attempt to perform.)

11. Technologies

a. What technologies are used in the system that involves privacy risk?

WRS does not employ any technology known to elevate privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Since WRS does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be at the very minimum satisfactory in this application.

12. Security

a. What is the security certification and accreditation (C&A) status of the system?

Department of State operates WRS and subsystems ISCS and JWOL, in accordance with information security requirements and procedures required by federal law and policy. To ensure information is appropriately safeguarded and protected, the Department of State has conducted a risk assessment of the system to identify appropriate security controls to protect against risk and implemented controls. Department of State performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, WRS and subsystems ISCS and JWOL were certified and accredited for 36 months to expire on May 31, 2010.

13. Certifying Officials' Signatures

_____

Kirit Amin, System Owner

_____

David Husar, System Manager

_____

Don Lyles, Information Security Manager

Email the completed PIA in MSWord format to "PIA Team". Upon signing, please send this signature page to the same group email box in the form of a scanned PDF, or send as paper via interoffice mail to the Privacy Office "A/ISS/IPS/PRV".

_____

TO BE COMPLETED BY THE PRIVACY OFFICE

Reviewer: _____ Approver: _____