Appendix B. PIA Template

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: April 15, 2009

(b) Name of system: Recruitment System

(c) System acronym: RECRUIT

(d) IT Asset Baseline (ITAB) number: 493

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

RECRUIT allows personnel in DS/MGT/HRM's Recruitment Office to manage and track employment application data for Foreign Service Agents, Diplomatic Couriers, Security Engineering Officers, and Security Technical Specialists during the recruitment process.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable):

(h) Date of previous PIA (if applicable): 2008

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?

RECRUIT contains employment applications data such as:

- Name
- Gender
- Race
- POB
- DOB
- SSN
- Address (Home/Work)
- Phone Number (Mobile/Home/Work)

- E-Mail Address (Personal/Professional)
- Educational History
- Job Experience
- Military Status
- Citizenship
- Spouse Info
- Security Clearance Information

A large majority of the data collected is considered privacy data. Data is commonly collected from Form DS-1950, Application for Employment, which applicants are required to complete.

b. How is the information collected?

An individual applying for a position within the Department of State using Form DS-1950 supplies the Department with his or her personal information which is used in evaluating his or her qualifications.

c. Why is the information collected and maintained?

The information collected and maintained through RECRUIT is used to track candidates in the employment process who have applied for DS specific Foreign Service positions.

d. How will the information be checked for accuracy?

The agency or source providing the information is responsible for verifying accuracy. Specific methodologies for verification employed by DS include, among other things, maintaining the system as a live feed, allowing the information to be updated/edited at any time, and cross-referencing information with the DS/MGT/HRM analyst or surrogates

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

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to RECRUIT, are as follows:

- Pub.L. 99-399(Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended;
- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the sharing of Terrorism Information to Protect Americans).

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

RECRUIT collects the minimum amount of personally identifiable information necessary to track candidates in the employment process who have applied for DS specific positions in the Foreign Service.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National

Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The information collected is used to determine if the knowledge, skills and abilities an individual possesses qualifies him or her for a position in the Foreign Service. The PII will be used to verify citizenship, military service, and to conduct an investigation to determine employment suitability. The social security number is used to verify identify.

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

Analysis of the information is limited to non-subject-based statistical Information, such as the applications in a particular status (i.e. received, working, approved, or mailed) on an aggregate cycle (i.e., Monthly, Quarterly, Yearly, etc.); number of inquires, number of responses, and etc. Furthermore, no new information is derived.

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

The system does not use any commercial information, publicly available information, or information from other Federal agency databases. All of the information in the system is supplied by the applicants.

d. Is the system a contractor used and owned system?

RECRUIT is a U.S. Government owned system primarily designed and developed by contractors. All contractors have abided to regulatory guidelines and have signed and follow DS's Rules of Behavior.

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.

RECRUIT is a government owned system supported by contract employees, who support U.S. Government employees in their maintenance of the system.

Contractors and Government employees, who support and use RECRUIT, are subjected to a background investigation of the files of certain U.S. Government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. Contractors involved in the development and/or maintenance of RECRUIT hardware or software must have at least a SECRET-Level Security Clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11.

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

The retention of data collected by RECRUIT adds a higher risk due to the volume of data which is maintained by the system. In an attempt to mitigate this risk, the Department of State has implemented numerous management, operational, and technical security controls in order to protect the information in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments; physical and environmental protection; encryption; access control; personnel security identification and authentication; contingency planning; media handling; configuration management; boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software); and audit reports.

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?

The information submitted to RECRUIT by potential employees is shared between Human Resources offices within the Department of State. The information which is shared between the Departments is limited to only what is necessary in order to track the progress of the potential employee's candidacy into a position with the Department of State.

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

The information is hand carried from one Human Resources offices to the other by a Human Resource employee who has been trained on the handling procedures consistent with information of this level of sensitivity.

Moreover, numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with internal sharing and disclosure including, but not limited to annual security training, separation of duties, least privilege and personnel screening.

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

Unauthorized and/or unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse or elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plan text), and over an

un-trusted communications link can also pose a significant risk. Numerous management and operational and technical controls are in place to reduce and mitigate the risks associated with unauthorized external sharing and unintentional disclosure including, but not limited to formal memoranda of agreement/Understandings (MOA/MOU); services level agreements (SLA); annual security training; separation of duties; least privilege; and personnel screening.

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?

The information collected by RECRUIT is not shared with any bureaus outside of DS/MGT/HRM's Recruitment Office.

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

The information collected by RECRUIT is not shared with anyone outside of the Department of State.

RECRUIT is monitored and guided by the inherited security controls of the OpenNet. Controls built into the OpenNet General Support System (GSS), including routers and Network Intrusion Detection System (NIDS), provide network level controls that limit the risk of unauthorized access from all IP segments, to include patch management, configuration management, and segregation of duties.

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

The information RECRUIT collects is not shared with any external organizations; therefore, there is no heightened privacy risk from external sharing.

Unauthorized and/or unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text), and over an un-trusted communications link can also pose a significant risk. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associated with unauthorized external sharing and unintentional disclosure including, but not limited to formal memoranda of agreement/understandings (MOA/MOU); service level agreements (SLA); annual security training; separation of duties; least privilege; and personnel screening.

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): Security Records, STATE-36

☐ does NOT contain information covered by the Privacy Act.

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

Notice of the purpose, use and authority for collection of information submitted are available on a Privacy Act Statement on the Form DS-1950 and are described in the System of Records Notices titled STATE-36.

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

Providing information on the application is voluntary; however, the application will not be processed if an individual fails to disclose any information (including SSN). Before divulging information via the telephone (Land-Line, Mobile, or Internet), the individual is informed of the Privacy Act statement, whereby the acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use and authority for collection of information submitted are also described in the system of records notice STATE-36.

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?

No, the system would not be able to process the application or utilized the system for its intended purpose.

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 notice offered is reasonable and adequate in relation to the system's purposes and uses.

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?

RECRUIT contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport 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.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

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?

Users must first authenticate to OpenNet, which utilizes Windows authentication. System authorization is based upon role-based control and session management. An end user is only granted access rights once he/she has authenticated to OpenNet. All actions performed within the system are audited by controls configured for the operating system and database. Each update to the database is logged and available as an audit trail.

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 RECRUIT components, for changes to the DoS mandated security controls.

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

All 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.

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.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system and at what privilege level, are regularly reviewed; inactive accounts are promptly terminated. 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 the particular functions a particular user performed--or attempted to perform--on an information system.)

11. Technologies

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

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes; continuous monitoring; checking the national vulnerability database (NVD); and following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the safeguards implemented to mitigate the risk to any Information Technology. RECRUIT has been designed to minimize risk to privacy data. Please refer to 11(b) for further information.

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

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational, and technical controls in place to mitigate these risks. Applying security patches and hot-fixes; continuous monitoring; checking the national vulnerability database (NVD); following and implementing sound federal, state, local; and Department and bureau policies and procedures are only a few of safeguards implemented to mitigate the risks to any information technology (IT).

12. Security

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

The RECRUIT application system was accredited for three years in May 2007.