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: December 16, 2009

(b) Name of system: Web Post Administrative Software Suite Explorer

(c) System acronym: WebPASS

(d) IT Asset Baseline (ITAB number): 744

(e) System description:

WebPASS Explorer ("WebPASS") is a suite of business applications used by overseas posts to administer a variety of internal activities. Some but not all applications under WebPASS collect and maintain personally identifiable information (PII) about post employees, their family members, and visitors. WebPASS is web-enabled and operates within the confines of OpenNet, the Department's sensitive but unclassified (SBU) network.

The main application is Web Post Personnel (Web.PS), which is a database of the American employees (AEs), their dependents, and Locally Employed Staff (LES). Whereas the official record for an AE employee is maintained in Washington, DC, the Web.PS database supports local personnel-related tasks. Its LES-related features support personnel actions for LES staff directly hired at the post such as intake, assignments, transfers, grade increases, and terminations.

After an AE or LES staff is established in Web.PS, some of their basic identifiers (e.g., name, employee type, office) may be pulled electronically into other WebPASS applications that support separate functions such as motor pool operations, residency in government-held real property, and distribution of pharmaceutical medications.

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To bring PIA into conformance with latest Department PIA guidance

(g) Explanation of modification: Not applicable

(h) Date of previous PIA: December 1, 2007

3. Characterization of the Information

The system:

☐ does NOT contain PII.

☒ does contain PII.

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

Categories of Record Subjects. WebPASS collects and maintains PII about four categories of record subjects:

- AEs assigned to the post: AEs comprise U.S. citizens assigned to an overseas post in the Senior Foreign Service, the Foreign Service, or the Civil Service; eligible family members of an AE who are also employed at the post; and U.S. citizens employed under Personal Services Agreements (PSAs).
- Dependents of AEs: Family members of AE employees who are not also employed at the post, but who are otherwise eligible for certain post services.
- LES staff employed at the post: LES employees are persons employed at a post who are not AEs. An LES may be a direct hire foreign national non-U.S. citizen (who is also not a family member of an AE); an ordinary resident U.S. citizen legally living and working in the host country; a Personal Services Contractor (PSC); or a person hired under a PSA who is also not an AE.
- Temporary visitors to the post: This category may include, but not be limited to, Federal employees of other government agencies, contractors, private sector business persons, and individuals who are part of a Congressional delegation or a delegation of their staffs.

Sources of Information. During the period of time a record subject is associated with a post, he or she is a direct source for their own PII that is collected and maintained in WebPASS. Other Department IT systems that are considered authoritative sources for personnel-related data for AE employees may also be used to establish or update an individual's record in WebPASS.

PII Collected About AE Employees. The following categories of PII, either linked or linkable, are collected and maintained about each AE:

- The basic personal identifiers of name and Social Security Number (SSN) are required elements and are the indices for regular retrieval of the AE's record. In addition, the individual's sex is a required element.

- Details about travel documents (e.g., passport number, dates of issuance and expiration) are collected to process travel messages pertaining to the AE.

- Information about the AE's language skills, education, and specialized training.

- Bi-weekly time-and-attendance reports for compensation and leave.

- The following kinds of information about an AE may be optionally collected:

    - Other personal details including birth date, place of birth, state of legal residence, marital status, diplomatic title, number of dependents, and number of dependents living at the post.

    - Work-related contact information (e.g., location on post, telephone numbers, email addresses).

    - Information about the AE's employment status in relation to the post (e.g., type of appointment, tenure, assignment, tour, work schedule).

    - Information about the AE's compensation (e.g., pay plan, grade, class, step, salary, and payroll office ID number).

    - Information about the post privileges granted to the AE.

    - Information about where the AE or a related family member is located or can be contacted, including a contact's name, relationship of the contact to the AE, and the address, telephone numbers, and email address of the contact.

    - Health-related information about the AE or their dependents, but limited to allergies, current medications, and medications dispensed by the post.

PII Collected About AE Family Members. The following categories of PII, either linked or linkable, are collected and maintained about each dependent of an AE:

- The dependent's name, sex, and relationship to the AE are required elements. Details about travel documents issued in the dependent's name (e.g., type, number, expiration date) are also required elements.

- The following kinds of information about an AE's dependent may be optionally collected:

    - The birth date of the dependent and facts related to the dependent's schooling status.

- Information about where the dependent is located or can be contacted, including contact's name, relationship to the dependent, and the residential address, telephone numbers, and email address of the contact.

- Health-related information about the dependent, but limited to allergies, current medications, and medications dispensed to the dependent by the post.

PII Collected About LES Employees. The following elements of PII, either linked or linkable, are collected and maintained for each LES employee:

- The surname of the LES is a required element and functions as the index for regular retrieval of the individual's record. In addition, the following information is collected:

  - LES's birth date, sex, and citizenship.

  - Information about the LES's compensation (e.g., compensation plan, step, salary, contract, agreement, payroll office ID number).

  - Bi-weekly time-and-attendance reports for compensation and leave.

  - If applicable, information about participation by the LES in a retirement savings program designed to provide benefits upon separation to LES employees.

  - Information about the LES's language skills, education, and specialized training.

  - For each dependent of an LES, the dependent's name, sex, birth date, and relationship to the LES.

- The following elements about an LES may be optionally collected:

  - Other personal details including marital status, place of birth, country of origin, citizenship of birth, alien number, permanent resident alien status, third-country national status, and number of dependents.

  - If the LES is a U.S. citizen, their SSN.

  - Information about the LES's employment status in relation to the post (e.g., type of appointment, tenure, assignment, tour, work schedule).

  - Dates and facts related to events in the LES's employment (e.g., hire date, security certification date, medical examination date, milestone dates, award dates).

  - Information about certain documents or credentials held by the LES related to medical examinations, security clearances, passports, visas, post identification cards, vehicle licenses, and vehicular accidents.

  - Work-related contact information (e.g., location on post, telephone numbers, email addresses).

- Information about where the LES or a related family member is located or can be contacted, including contact's name, relationship of the contact to the LES, and the address, telephone numbers, and email address of the contact.

PII Collected About Temporary Visitors. The following elements of PII are collected and maintained for each visitor:

- The full name of the visitor, their expected arrival and departure dates, and their security clearance level.

- As applicable, the visitor's parent agency, company, country, and contract number.

- Optionally, information about access-controlled areas of the post to be visited, the sponsor of the visit, any local event related to the visit, job position and description, work contact information, passport information, and nationality.

b. How is the information collected?

Most PII in WebPASS is collected directly from the record subject (from paper forms completed by the record subject or from documents the record subject presents) by an authorized task worker at the post. In some cases, PII may be copied into WebPASS electronically from other Department IT systems that are considered authoritative sources for the data. In other cases, PII may be transcribed from hard copy outputs from other Department IT systems into WebPASS.

c. Why is the information collected and maintained?

By Department policy, posts are authorized to maintain duplicate copies of personnel records of all categories of U.S. citizen employees to facilitate post personnel administration. The following mission-related functions are supported by WebPASS records maintained at a post:

- Personnel and position management functions that are inherently local in nature, including time and attendance reporting.

- Management and distribution of pharmacy medications and supplies that may be administered to AE staff and their dependents as a service provided by the post.

- Record-keeping and tasks related to official visitors to the post.

- Assignment and tracking of occupancy in residential units of U.S. government real property, including records of primary occupants and tandem occupants.

- Motor pool vehicle registration and maintenance, and record-keeping pertinent to motor pool driver safety and accidents.

- Collection of cost of living survey data used by the Department to calculate post salary allowances. Post employees are surveyed about local retail outlets used, the percentage of goods purchased locally at post or military commissaries, from catalogues, the internet, or brought to the post at government expense.

- Procurement of goods and services, and assignment of non-expendable property.

d. How will the information be checked for accuracy?

The interactive interfaces of WebPASS applications employ field-specific and contextual edits to avoid transcription errors during data entry. As much as possible, personal data elements already maintained in WebPASS are used to pre-fill records as they are created in other WebPASS applications to reduce duplicate data entry and chance of error. Other Department IT systems that are considered authoritative sources are referenced in the course of maintaining WebPASS data, and consequently provide an additional safeguard for the correction of WebPASS data inaccuracies.

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

22 U.S.C. 2581 (General Authority of Secretary of State); 22 U.S.C. Chapter 52 (Foreign Service); 31 U.S.C. 901–903 (Agency Chief Financial Officers); and the Federal Financial Management Improvement Act of 1996 provide a statutory basis for the collection and maintenance of PII in WebPASS.

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

The most sensitive unique identifier in WebPASS is the record subject's SSN, which is stored in Web.PS. After its first entry into Web.PS, the SSN is not displayed in any interactive interface available to post task workers who have basic user access privileges. Marginal risk exists that routine authorized uses of WebPASS, or data inaccuracies in WebPASS, might render an adverse determination against the record subject, or deny the individual a right, benefit, or privilege of the government, or otherwise cause them harm.

4. Uses of the Information

a. Describe all uses of the information.

The principle uses of WebPASS are to support the administration of several regular activities common to all overseas posts. Whereas the official record for an AE employee is maintained in Washington, WebPASS supports personnel-related tasks that are inherently more suitable to be administered locally, including time and attendance reporting, providing post privileges, and accommodating official visitors. Its LES component supports personnel tasks about LES staff directly hired at the post such as intake, assignments, transfers, grade increases, and terminations. After an AE or LES staff is established in WebPASS for the purposes of personnel and position management, some of their basic identifiers (e.g., name, employee type, office) may be pulled electronically into other component WebPASS applications that support functions such as motor pool operations, residency in government-held real property, and distribution of pharmaceutical medications to AEs and their dependents. A separate component application supports information needs related to official visits to the post.

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

No analytical methods involving pattern-based queries, searches, matches, or other analyses of multiple databases of PII are used in WebPASS. The only subject-based queries are related to the authorized uses described in paragraphs 3.c. and 4.a. WebPASS data is periodically transmitted to domestic Department offices by all posts to support the Department needs described in paragraph 6.

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

These sources of information are not used in WebPASS.

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

Contract employees at some posts and in domestic Department offices may be given authorized access to WebPASS as part of their official duties, working under the supervision of Department employees. WebPASS data is not otherwise disclosed or handled by contractors.

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.

The limited nature of PII elements in WebPASS creates negligible risk that the information may be used for other than the intended purposes. Limitations on the use of WebPASS are sufficiently regulated by user access agreements, security and privacy awareness training, and system use notifications ("warning banners") specific to WebPASS, as well as more broadly by comparable controls adjunct to the Department SBU network under which WebPASS operates.

5. Retention

a. How long is information retained?

The information entered in WebPASS is covered by various official foreign records disposition schedules, which carry different retentions:

- Records of AE staff maintained in WebPASS for the purpose of facilitating post personnel administration are destroyed one year after the AE's transfer from the post or separation from the Department.
- Records of LES staff maintained in WebPASS for the purpose of facilitating post personnel administration are considered "temporary" and separate from the Official Personnel Folder (OPF) maintained about the individual. The electronic records are destroyed after transfer of the paper OPF to a gaining post or another federal agency, or retirement of the OPF to the Department personnel records branch upon the separation or death of the individual.

- Time and attendance records are destroyed after six years.
- Records related to the health of, or pharmacy services provided to, employees or their dependents are destroyed after six years.
- Records related to an individual's use of post privileges are destroyed one year after departure from the post.
- Visitor records are destroyed after one year.

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

Because of the limited PII in the records, the privacy risk related to retention (i.e., data accuracy degradation over time) is negligible. The records are retained in accordance with foreign records disposition schedules, which reduce the risk of retention beyond what is officially accorded the records by the schedules.

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 PII in WebPASS is used primarily to satisfy local operations at each overseas post. The PII at each post is not accessible by WebPASS users located at other posts. PII in WebPASS is shared with domestic Department offices as follows:

- Data are transmitted daily to a Post Personnel Consolidated Data Base (PSCDB) located in Washington, DC. The PSCDB is used by the Bureau of Human Resources to satisfy the need for aggregate reports of personnel, position, and staffing information; to assist posts on specific personnel-related issues; and to support the Executive Branch initiative for a "Right-Sized Overseas Presence."
- Time and attendance data are transmitted from the WebPASS at each post bi-weekly to the Consolidated American Payroll Processing System (CAPPS) in Charleston, SC, or the Foreign Service National Payroll System (FSN-Pay) in Bangkok, Thailand.
- PII related to use of U.S government owned and leased real property is periodically transmitted from the WebPASS system at each post to the Office of Overseas Building Operations in Washington, DC, for use in the Department-wide real property management program.

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

All information is shared by secure network transmission methods permitted under Department policy for the handling and transmission of SBU information.

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

Because of the limited disclosure of the PII in WebPASS, privacy risk from internal sharing is negligible. Access by internal Department users who are authorized to access PII in WebPASS in the performance of their official duties is regulated and monitored by the controls on use and access described in paragraphs 4 and 10.

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?

No PII in WebPASS that can be used to uniquely distinguish an individual is shared with persons or entities outside the Department of State.

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

Not applicable.

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

Not applicable.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

☐ does NOT contain information covered by the Privacy Act.

Depending on its specific use or uses, PII collected and maintained in WebPASS is subject to the provisions of the Privacy Act, and is described in the following Privacy Act systems of records:

- State-24, Medical Records
- State-25, Overseas Records
- State-30, Personnel Payroll Records
- State-31, Human Resources Records
- State-36, Security Records

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

Forms may be used at a post for the purpose of collecting PII directly from the record subject. When the PII captured on such a form is subject to the provisions of the Privacy Act, the form contains a Privacy Act statement for the benefit of the record subject that is compliant with section e(3) of the Act.

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

Only a few elements of PII in WebPASS are mandatory and are always requested of record subjects. The mandatory elements vary for each category of record subject, and are described in paragraph 3. The provision of these mandatory elements by a record subject is a basic condition of employment with the federal government. Other elements of PII are optional in nature and a record subject has the opportunity to decline providing them; however, personnel-related services to the individual or their dependents at the post may be hampered by their doing so.

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?

These opportunities are not generally available in WebPASS because of the nature of the functions served by the system and because provision of the PII by the record subject is a basic condition of employment in the federal government.

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.

No privacy risk results from the extent to which WebPASS does or does not offer options to record subjects in providing their PII storage and maintenance in WebPASS.

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?

Because the PII collected and maintained in WebPASS is subject to the Privacy Act, formal procedures for notification and redress exist and are described in the applicable Privacy Act system of records listed in this PIA.

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

This category of privacy risk is appropriately mitigated by the publication of formal notification and redress procedures in the applicable Privacy Act system of records.

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?

All hard copy records are maintained in restricted areas within posts and domestic Department offices having authorized access to WebPASS. Access to electronic records is password-protected. To access the system, the individual must first be an authorized user of the Department's SBU computer network. Access privileges are assigned by a system administrator having a privileged computer account based on the principles of separation of duties, least privilege, and need-to-know. Authorized users maintain a security clearance level at least commensurate with public trust positions.

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

All personnel accessing WebPASS receive security awareness briefings administered by the Bureau of Diplomatic Security and local post management.

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.

Safeguards for access are commensurate with the confidentiality level of PII in WebPASS, and reduce related privacy risk to a negligible level.

11. Technologies

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

WebPASS does not incorporate technologies that elevate privacy risk. At each location where WebPASS is operated, the computer platform upon which it resides is configured to provide only essential capabilities; to specifically prohibit or restrict the use of unnecessary functions or services; and to otherwise comply with the principle of least functionality.

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

This category of privacy risk is negligible.

12. Security

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

The Department of State operates WebPASS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. The last authorization to operate WebPASS in accordance with federal law was issued on June 24, 2009.