Privacy Impact Assessment (PIA)

1. Contact Information

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

2. System Information

(a) Date PIA was completed: 2/10/2009

(b) Name of system: Foreign Service National Payroll System

(c) System acronym: FSNPay

(d) IT Asset Baseline (ITAB) number: 641

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

FSNPay is a major component of the Department of State (DoS) Payroll System and provides payroll system support to over 49,000 Foreign Service National (FSN) employees in over 180 countries.

FSNPay is server-based and performs bi-weekly payroll processing including payroll calculations, report processing, financial reporting, and preparation/distribution of payments for FSN. Corrective payroll actions and retroactive pay adjustments are also accomplished via appropriate transactions that are processed as a part of the bi-weekly cycle. FSNPay makes payments on behalf of more than 40 other Government Agencies besides DoS, based on each country's local compensation plan. Since each compensation plan has at least two pay scales and one plan has eight pay scales, FSNPay routinely makes payment against 400 or more pay scales.

FSNPay capabilities include:

- Bi-weekly payroll processing
- Payroll calculations
- Report processing
- Financial reporting
- Preparation/distribution of payments and results
- Exception time reporting
- Capture and validate agency-specific project costs

(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): This system was previously reported as not collecting PII data and is now being reported as collecting the PII as the DoS has extended the Act's requirement to all PII-based systems (except NSS) without regard to the kind of record subject and therefore now includes US government employees and contractors.

(h) Date of previous PIA (if applicable): 8/26/2005

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?

Locally engaged staff (LES) at the embassies consulates and missions abroad who are employed by the US Government. LES can include Foreign Nationals and US citizen family members eligible for employment. Information collected from DoS employees and employees of other agencies serving our missions abroad include, name, address, date of birth and other criteria needed to derive payroll in accordance with the local compensation plan of the employee.

b. How is the information collected?

This information is collected from the LES as they enter on duty with the mission abroad from their perspective HR office. The employee completes forms and the HR specialists produce the appropriate data cables containing the information necessary to complete personnel actions in the FSNPay application. The information is transmitted as a cable to the appropriate FSNPay office in Bangkok Thailand or Charleston SC depending on the region of the mission. Once the cable is received by the FSNPay data technician, the data is entered into the FSNPay application.

c. Why is the information collected and maintained?

The information is collected and maintained to process the payroll of the LES according to their local compensation plans and to allow for the disbursement, payment of the payroll to the appropriate individual.

d. How will the information be checked for accuracy?

Various automated techniques are used to ensure the appropriateness of the data entered into FSNPay, additionally the data entered is verified by the Post HR office with the data entry technician supporting the FSNPay application via reports, phone conversations, e-mails and the like.

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

Federal Financial Management Improvement Act (FFMIA) of 1996.

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

Risks are mitigated by collecting the absolute minimum PII required to satisfy the statutory purpose of this system and meet the mission of processing of payroll. Additionally, there are controls through systems security that ensure only those individuals with a need to know are given access to the FSNPay application and it's reports.

4. Uses of the Information

a. Describe all uses of the information.

Payment of payroll, awards and bonuses to the LES of the US missions.

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

FSNPay does not produce new information other than the calculation of compensation for the LES staff.

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

No data is provided to FSNPay that is not directly related to the payroll processing data needed to pay the LES at missions abroad.

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

No. The FSNPay application was developed by the DoS and is maintained and operated by the DoS. There are some support staff at the Charleston GFS that are contractors who are responsible for the maintenance and operation of the application.

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.

Personnel requiring access are required to submit a user agreement form which is approved by management personnel prior to access being granted. The rules of behaviors and controls are placed on user prior to access being granted.

5. Retention

a. How long is information retained?

The retention period for payment, cash receipt and tax data is seven years.

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

Regular backups are performed and recovery procedures are in place for FSNPay. All records containing personal information are maintained in secured file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system

manager. When records have reached their retention period they are immediately retired or destroyed in accordance with National Archive 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?

Information is shared with internal organizations, each bureaus financial section as well as each post's financial and HR sections, primarily in the form of reporting, the Payroll Expenditure report detailing the funding types used to make the payroll of the LES and the 80 report, status of payments report, showing the actual disbursements made by agency and/or post.

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

FSNPay reporting is provided via system security access by authorized users as defined by the Foreign Service Officers at the posts. Secure transmission methods permitted under DoS policy for handling and transmission of sensitive but unclassified information is followed.

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

External sharing occurs only to registered users who are cleared government employees or contractors with work-related responsibility for FSNPay. Risks to privacy are mitigated by providing only those reports associated with the persons permissions that are established by their supervisor and in conjunction with the ISSO.

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?

Information is shared with external organizations primarily in the form of reporting, the Payroll Expenditure Report, specific to the agency, post or bureau that the report is being provided. There are more than 240 missions abroad and 40 other agencies that are serviced by the FSNPay application and disbursements are made by the DoS US Disbursing Officer in payment of their LES payroll. The agencies include Agriculture, Commerce, USAID, IRS and the agencies vary by the mission or post. This information is provided to post agencies to agencies head quarters.

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

FSNPay reporting is accessed by authorized users through secure transmission methods permitted under DoS policy for handling and transmission of sensitive but unclassified information.

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

External sharing occurs only to registered users who are cleared government employees or contractors with work-related responsibilities for RFMS. Risks to privacy are mitigated by providing only those reports associated with the persons permissions that established by their supervisor and in conjunction with the ISSO.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

State 30 Personnel Payroll System

☐ does NOT contain information covered by the Privacy Act.

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

Employee's prior to and as information is collected are informed that the data will be entered into the automated payroll application that will calculate their payroll.

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

No. This information is required in order to process payroll payments and benefits.

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. This information is required in order to process payroll payments and benefits.

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 HR office at post provides guidance to new employees as they are hired which is also the time of collection, a privacy statement is available on forms and the notice is reasonable and adequate in relationship to the system's purpose and use.

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?

Individuals received reporting of their information on personnel actions and if there is a need to amend information the personnel work through their post HR office who then reports the changes required via a personnel action to the FSNPay data entry technician for the modification to be made.

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

There is no risk associated with notification and redress as these are handled as all data exchange is handled between the individual, post HR and authorized users of the FSNPay application. 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?

Access to FSNPay is limited to authorized DoS employees and contractors who have a need for access to the system. All users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to FSNPay requires a user account assigned by Resource Management.

Each authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes rules of behavior describing the individual responsibility to safeguard information and prohibit activities (e.g., curiosity browsing).

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 logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Access to FSNPay is restricted to authorized personnel who are cleared DoS direct hire and contractor employees located within the Charleston and Bangkok Global Financial Service(GFS) centers. The system and database administrators are also located in GFS centers and are the only users with direct access to the database for the purpose of performing maintenance. All rights to information and functionality within FSNPay are enforced by user profiles according to the principles of least privilege and separation of duties. All access to FSNPay is logged by the operating system and/or the application, depending on the activities being performed.

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

Every user must attend a security briefing prior to receiving access to the DoS networks and getting a badge for facility access. This briefing also includes the Privacy Act of 1974. Users must complete initial and annual Cybersecurity Awareness training.

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.

No such residual risk is anticipated. FSNPay was Certified and Accredited (C&A) in May 2005. Residual risks for the application were not identified. Had residual risks been discovered during the C&A process, all risks would have to been reviewed, mitigated,

and accepted by the system owner. This was not the case. The system is accredited for operation in the production environment

11. Technologies

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

There are no Privacy risks associated with this system. All technologies in use with FSNPay have been approved by the IT/CCB and are widely available to all DoS applications.

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

Not applicable.

12. Security

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

The FSNPay authorization expires on May 31, 2009.