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: 3/09/2010

(b) Name of system: Global Financial Management System

(c) System acronym: GFMS

(d) IT Asset Baseline (ITAB) number: 928

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

Global Financial Management System (GFMS) is a multi-tiered web-based application, based on commercially available software, which provides flexible financial accounting, funds control, management accounting, and financial reporting processes. It maintains the Department of State's spending budget, supports buying of goods and services, vendor payments, records general ledger entries, reports to Department of Treasury and the Office of Management and Budget, verifies data accuracy and properly clears and closes ledgers and journals. GFMS is comprised of subsystems that include budget execution, travel, accounts payable, accounts receivable, planning, automated disbursement, general ledger, annual closing of books, acquisition and delivery of goods, and reporting.

(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): 9/14/2009

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?

GFMS collects or maintains information from sources as listed below:

Employees:

- Name;
- Addresses;
- Phone Number;
- Social Security Number;
- Employee identification number; and
- Bank account and routing number.

Vendors and or Contractors:

- Corporate Name;
- Corporate Address;
- Phone Number;
- DUN;
- Tax identification number; and
- Bank account and routing number.

The sources of information for DoS and other federal agency employees are the Consolidated American Payroll Processing System (CAPPS) and Domestic Account Tracking System (DARTS). The Central Contract Registry (CCR) and Financial Management Officer (FMO) or designated financial staff employees are the sources of information for the vendors and contractors.

b. How is the information collected?

GFMS receives manual batch files via secure file transfer protocol, by DoS e-mail, compact discs and via manual entry. Vendors input their information into CCR or information is collected by FMO or designated financial staff employees using a purchase order agreement form.

c. Why is the information collected and maintained?

GFMS is the official financial management system for the DoS to account for and control appropriated resources and to maintain accounting and financial information associated with the normal operation of U.S. government organizations. The information in this system is used to make authorized payments for goods and services to companies or individuals doing business with the DoS, to make authorized reimbursement payments to an employee, to prepare IRS-1099 tax reports, and to account for individual accounts of debts owed to the DoS or the U.S. Government, in accordance with the Debt Collection Improvement Act of 1996.

d. How will the information be checked for accuracy?

The data provided on a payment request from other than DoS sources is certified by the submitting agency for accuracy. The data provided on Accounts Receivable accounts and cash receipts are verified by the Accounts Receivable Division for accuracy. The vendor is responsible for the accuracy of information in CCR.

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.

GFMS is the official financial management system for the DoS to account for and control appropriated resources and to maintain accounting and financial information associated with the normal operation of U.S. government organizations. Therefore, GFMS collects a significant amount of PII, including employee SSN. Transfer of financial information to the IRS is a statutory requirement, therefore the collection of SSN is part of the minimum amount of PII necessary to complete GFMS' statutory mission.

To mitigate the privacy risk within GFMS, the level of sensitivity of information accessed, processed, stored and transmitted by GFMS is sensitive but unclassified (SBU) and has been categorized as a moderate impact system. GFMS processes privacy data as defined by the Privacy Act of 1974. The employees and contractors working for the DOS have undergone a thorough background security investigation. Access to the Department and its annexes is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals with proper escort. Access to computerized files is under the direct supervision and folders are password protected.

4. Uses of the Information

a. Describe all uses of the information.

Information collected from the public is limited to companies doing business with the DoS and therefore is information about the corporate entity (e.g. Tax Identification Number (TIN); corporate address; Bank Routing/Account for electronic fund transfer (EFT) payments; telephone number; EEOC classification). This is information is required for 1099 tax reporting.

Information collected from DoS employees (e.g. Employee ID (either SSN or FSN ID); address; and Bank Routing information for EFT payments) is information already contained in the CAPPS and/or FSNPay payroll systems and required to make a reimbursement payment to the employee.

Information collected from other systems like DARTS is information about individual accounts receivable like Repatriation Loans, which contains social security numbers, names, addresses, telephone numbers, and loan numbers.

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

GFMS has the capability to identify, locate, and monitor individuals. However, the information is used only to enforce compliance with either tax law and regulations or current published employee practices within the DoS with regards to employee reimbursements. Payment information is collected and compared to previous payments to ensure that duplicate payments are not issued.

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

The DoS uses publicly available information from the CCR system to update their vendor's files.

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

This is a government owned system but contractors are involved in the design and development of the system. All contractors undergo an annual computer security briefing and Privacy Act briefing. All contracts contain approved Federal Acquisition Regulation Privacy Act clauses.

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.

Users have undergone background checks and received training in handling personally identifiable information. Users receive security awareness training annually. Users are restricted to browsing only data that they are authorized to view for official purpose of their duties only.

5. Retention

a. How long is information retained?

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

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 records. Access to electronic records is restricted to authorized personnel 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 the 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?

Receivable, collection, and reference table data are passed between GFMS and DARTS through a two-way interface. DARTS updates GFMS with receivable data, and GFMS returns any rejected receivables back to DARTS through a Rejected Interface. Collections originated in GFMS are transmitted to DARTS through an accepted interface.

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

GFMS exchanges data with DARTS through interfaces that are run at least monthly. This interface, subject to security restrictions, allows for transfer of data, thereby reducing manual data entry.

GFMS is accessed by authorized users by secure transmission methods permitted under DoS policy for handling and transmission of sensitive but unclassified information. Access is enforced by permissions set with the SQL database. User access is controlled by roles as defined in the GFMS and MS SQL database. The system administrator and ISSO are the only employees with direct access to the database.

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

Internal sharing occurs only with registered users who are cleared government employees or contractors with work-related responsibility for GFMS. Risks to privacy are mitigated by sharing only the information associated with the person's 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?

The principal users of this information outside the Department of State are: (1) Department of Treasury to issue authorized payments to companies and individuals or to issue authorized reimbursement payments to employees; and (2) the Internal Revenue Service and companies or individuals who have received qualifying payments during the tax year as recipients of IRS-1099 reporting.

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

The information in shared through a data exchange through GFMS and DARTS. DARTS interfaces with the Department of Treasury Cross-Servicing application. This interface is one-way (output only) from DARTS in the form of a text file. Information to IRS is provided on the IRS 1099.

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

Managers, system administrators, and developers have read access to the data. Only authorized users have read and change access.

Table driven security software defines the access rights and is maintained by the designated Information Systems Security Officer.

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):

Global Financial Management System STATE–73

Volume 73 Number 136

☐ does NOT contain information covered by the Privacy Act.

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

In some instances individuals are made aware of the uses of the information prior to the collection through a Privacy Act Statement located on forms associated with this collection. For the most part, information is not collected directly from the individual therefore the opportunity to provide does not apply. Notice is published in the system of record State-73, Global Financial Management System.

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

Yes, but the information in this system is required to make authorized payments for goods and services to companies or individuals doing business with the Department of State.

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 information in this system is required to make authorized payments for goods and services to companies or individual doing business with the Department of State.

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 mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose 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?

Vendors can review their vendor master file data and report any updates to the DoS or make update in the CCR system. DoS employees have access via a secure employee self-maintenance portal to ensure that their personnel information is accurate and up-to-date. Procedures for notification and redress are published in the system of record State-73, Global Financial Management System and rules published at 22 CFR 171.31.

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?

Internal access to GFMS is limited to authorized staff having a need for the system in the performance of their official duties. All users maintain a least a SECRET security clearance level in order to gain access to the Department's unclassified computer network. To access the records maintained GFMS, the individual must first be an authorized user of the Department's unclassified computer network. Each prospective 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 in order for the individual to perform his or her 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 prior to assigning the individual a logon. 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. The supervisor will assign the level of permission for each user and restrict the data that may be seen and the degree to which data may be modified. Access rights and privileges within GFMS are based on need-to-know, separation of duties, and supervisory requirements.

GFMS system and database administrators are the only users with direct access to GFMS for the purpose of performing maintenance.

GFMS is accessed via OpenNet from Department of State configured workstations. Authorized users must first authenticate to OpenNet using their user ID and password and then authenticate to GFMS using a separate and unique user ID and password. All communication between GFMS and client browsers is routed through an IIS web server tier.

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. The training consists of computer security awareness to include the proper handling of PII.

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. GFMS was Certified and Accredited (C&A) in May 2007. 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?

All technologies in use within GFMS have been approved by the IT/CCB. No technologies commonly considered to elevate privacy risk are employed.

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?

Current ATO expires May 31, 2010.