GFMS PIA

1. Contact Information

PIA Completed By:	System Owner:
Name: Samuel Bisbey Title: Systems Manager Organization: CGFS/GFMS Phone: 703-875-5987 Email: BisbeySW@state.gov	Name: Dawn M. Parrish Title: Deputy Director Organization: CGFS/GFMS Phone: 703-875-6912 Email: ParrishD2@state.gov
Program Manager: Name: Jamie McCullough Title: Director Organization: CGFS/GFMS Phone: 703-875-4977 Email: McCulloughJL@state.gov	**IT Security Manager:** Name: Monique Lanier Title: Systems Accountant Organization: CGFS/GFSS Phone: 703-875-5974 Email: LanierMN@state.gov
A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services	

2. System Information

(a) **Name of system**: Global Financial Management System

(b) **Bureau**: Comptroller and Global Financial Services (CGFS)

(c) **System acronym**: GFMS

(d) **iMatrix Asset ID Number**: 928

(e) **Reason for performing PIA**:

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

(f) **Explanation of modification (if applicable):**

The purpose of this change is to comply with NIST Special Publication 800-53 Revision 4, AC-2, Account Management, (j) Review accounts for compliance with account management requirements according to organization-defined frequency; and with Department policies 12 FAM 623.1 and 12 FAH-10 H-112.1-3. GFMS, Data Warehouse (DW) and Central Contractor Registry Connector (CCRC) user account data needing verification will be gathered by a script executed in the GFMS overnight cycle (to be executed weekly if manual; daily if automated). Six output data files will be provided to myData to

populate the verification form. Data will be output to a shared folder, from which the myData team will load the data into myData.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

_X__ Yes ____ No

(b) What is the security Assessment and Authorization (A&A) status of the system?

GFMS has an Authorization-To-Operate (ATO) that expires on February 29, 2020.

(c) Describe the purpose of the system:

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; processes vendor payments; records general ledger entries; generates reports to Department of Treasury, Internal Revenue Service (IRS) and the Office of Management and Budget (OMB); 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.

There is also a Data Warehouse component of GFMS that provides supplemental reporting. This is a multi-tiered web-based application that uses SAP's Business Objects 3.1 software. It reports on processed data received from GFMS. Global Business Intelligence (Global BI) is the new business intelligence platform for the CGFS Bureau that will eventually replace the GFMS Data Warehouse. It is an implementation of an SAP HANA appliance with a Business Objects application platform, providing reports, dashboards, and analytics based on data aggregated from multiple financial systems both internal and external to CGFS. Migration of Data Warehouse reporting to Global BI will begin in Spring 2018.

(d) Describe the PII that the system collects, uses, maintains, or disseminates:

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 (TIN); 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), Foreign Service Nationals (FSN) Pay, Global Foreign Affairs Compensation System (GFACS) – Locally Employed (LE) and GFACS – Annuitants. 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.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

Specific legal authorities and/or agreements that allow the information to be collected include:

- Federal Manager's Financial Integrity Act of 1982
- Federal Financial Management Improvement Act (FFMIA) of 1996
- Debt Collection Act of 1982 and 1996
- Federal Funding Accountability and Transparency Act (FFATA) of 2006 and 2008
- Chief Financial Officers Act of 1990

1. 31 U.S.C. 3512 –This is the law that includes the Federal Manager's Financial Integrity Act of 1982.
2. 26 U.S.C. 6103 - Tax Returns and return information
3. 5 U.S.C. 5514 - Installment deduction for indebtedness to the United States (e.g. Withholding pay for items such as Child Support)
4. 5 U.S.C. 301 - The head of an Executive department or military department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
Yes __X__ If yes, provide:

- **SORN Name and Number:** State-73, Global Financial Management System
- **SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):** July 15, 2008

No ___ If a SORN is not required, explain how the information is retrieved without a personal identifier.

(g) **Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?** Yes ___ No __X__

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) **Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?** Yes __X__ No _____
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:
- **Schedule number (e.g., (XX-587-XX-XXX)):** DAA-GRS-2013-0003-0001
- **Type of information retained in the system:** Financial Management
- **Length of time the information is retained in the system:** Six years

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☐ Members of the Public

☒ U.S. Government employees/Contractor employees

☒ Other (Vendors)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
Yes __X__ No ____

- If yes, under what authorization?

Specific legal authorities and/or agreements that allow the information to be collected include:

- Federal Manager's Financial Integrity Act of 1982
- Federal Financial Management Improvement Act (FFMIA) of 1996
- Debt Collection Act of 1982 and 1996
- Chief Financial Officers Act of 1990

(c) How is the information collected?

GFMS collects or maintains information from GFACS payroll systems. Information from these systems is collected directly from the individuals. Staff hired domestically use the IRS Employees' Withholding Allowance Certificate (W-4) and equivalent forms for state withholdings. Locally Employed Staff (LES) utilize the JF-0162 Personal Services Contracting Action form.

Vendors input their information into CCR, or information is collected by FMO or designated financial staff using the Automated Clearing House (ACH) Vendor/Miscellaneous Payment Enrollment Form (SF-3881).

(d) What process is used to determine if the information is accurate?

The financial management officer certifies the transaction for accuracy before submitting data on a payment request for DoS.

The Bureau of the Comptroller and Global Financial Services (CGFS) verifies vendor/corporate information for accuracy. Various automated techniques are used including check digits* on SSN numbers plus random audits. In addition, the vendor maintenance process has a series of edits that check for duplicates, valid codes, and completeness of vendor attribute fields as they are entered into the system.

* A "check digit" ensures that data was delivered and was not manipulated from the time it was written until the time it was opened by the recipient.

(e) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Yes. Employees and contractors will provide updated information as necessary in order to ensure they receive authorized payments. If there are changes to be made, employees and contractors recertify their information to continue receiving payments.

(f) Does the system use information from commercial sources? Is the information publicly available?

No, the system does not use information from commercial sources or publicly available information.

(g) Is notice provided to the individual prior to the collection of his or her information?

Yes, notice is provided to the individual at the point of collection.

(h) **Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?** Yes __X__ No ____

- If yes, how do individuals grant consent?

This information is voluntary but is required in order to process payroll payment, reimbursement and benefits. Individuals grant consent in writing by providing the necessary information on applicable forms such as the IRS W-4 and JF-0162 (Personal Services Contracting Action). Any form that requires PII has been vetted by the Department and provides a Privacy Act Statement when applicable.

- If no, why are individuals not allowed to provide consent?

(i) How did privacy concerns influence the determination of what information would be collected by the system?

Only information required by the Department of Treasury and the IRS is collected. This is to ensure that employees and vendors can receive payments as authorized and proper tax withholding is collected and reported. In this way, the minimum amount of PII is collected.

5. Use of information

(a) The intended use(s) for the information is/are:

GFMS collects and maintains only information that is required for financial transactions. The employee's ID, address and bank routing information are required for employee reimbursements. TIN, corporate address, and bank routing/account are required for electronic fund transfer payments; telephone numbers and equal employment opportunity code classifications are used for IRS form 1099 tax reporting. The information is essential for accurate payment processing and establishment of accounts receivable, accounts payable, cash receipts, treasury and tax reporting.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes

(c) **Does the system analyze the information stored in it?** Yes ___ No __X__

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? Yes ___ No ___

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? Yes ____ No ____

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Information is shared internally with Bureaus whose users have been approved to see information that relates to their job duties. However Bureau users do not have access to PII such as social security numbers or banking information. Externally, information is shared with the Department of Treasury and the IRS.

(b) What information will be shared?

Internal use is by registered GFMS users who are cleared government employees or contractors with work-related responsibility for GFMS. GFMS users are granted role-based security profiles that restrict access only to the types of information needed to perform their job functions. Bureau users have access to financial information based on their security profiles but do not have access to PII.

Externally, information is shared with the Department of Treasury to issue authorized payments to companies and individuals or to issue authorized reimbursement payments to employees. Information is also shared with the Internal Revenue Service and companies or individuals who have received qualifying payments during the tax year as recipients of IRS-1099 reporting.

(c) The purpose for sharing the information is:

Information is shared with the Department of Treasury to issue authorized payments to companies and individuals or to issue authorized reimbursement payments to employees. Information regarding employee income is shared with the IRS and state taxing authorities as legally required. State also provides the IRS with 1099 information (vendor payments for the calendar year).

Information is shared with the Bureaus so that they may properly manage their authorized funding. Bureaus must manage spending versus budgeted amounts. They also need to approve and verify status of payments to individuals and vendors.

(d) The information to be shared is transmitted or disclosed by what methods?

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

(e) What safeguards are in place for each internal or external sharing arrangement?

GFMS is accessed by authorized bureaus and posts by secure transmission methods permitted under DoS policy for handling and transmission of sensitive but unclassified information.

There are Memorandum of Understandings (MOUs) and Internnection Security Agreements (ISAs) in place with Treasury/Financial Management Service (FMS), Carlson-Wagonlit Government Travel, Inc. (CWGT), GSA-Federal Acquisition Service and the Charleston Financial Services Center.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Internal sharing occurs only to registered GFMS users who are cleared government employees or contractors with work-related responsibility for GFMS. Risks to privacy are mitigated by

providing only those reports associated with the person's permissions that are established by their supervisor and in conjunction with the ISSO. GFMS users within the Bureaus do not have access to PII.

Only information required by the Department of Treasury and the IRS is collected. This is to ensure that employees and vendors can receive payments as authorized without collecting any unnecessary information from vendors and employees. Data sharing to Treasury and IRS are based on regularly scheduled events that are controlled via job scheduling which invoke the secure transport software for file delivery.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals who wish to gain access to or amend records pertaining to them in State-73 should write to the Director, Office of Information Programs and Services, A/GIS/IPS, SA–2, Department of State, 515 22nd Street, NW, Washington, DC 20522–8100.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information? Yes__X__ No _____

If yes, explain the procedures.

Individuals who wish to gain access to or amend records pertaining to them should write to the Director, Office of Information Programs and Services, A/GIS/IPS, SA–2, Department of State, 515 22nd Street, NW, Washington, DC 20522–8100

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Procedures are published in State-73 to inform individuals how to inquire about the existence of records about them.

8. Security Controls

(a) How is the information in the system secured?

The GFMS system is secured by the OpenNet configuration of VPN (Virtual Private Network) lines which encrypt transactions traversing the OpenNet and by role based access and privileges for users. We are currently working with IRM and the other Bureaus to identify an enterprise solution for data at rest encryption for the OpenNet.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Access to GFMS is limited to authorized DoS government and contractor employees 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 GFMS requires a user account assigned by CGFS.

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).

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Activity by authorized users is monitored, logged, and audited in accordance with US Department of State Diplomatic Security configuration guidelines at the database and server level. The system and database administrators in CGFS are the only users with direct access to the database for the purpose of performing maintenance. All rights to information and functionality within GFMS are enforced by user profiles according to the principles of least privilege and separation of duties. All access to GFMS is logged by the operating system and/or the application, depending on the activities being performed.

(d) Explain the privacy training provided to authorized users of the system.

Every user must attend a security briefing, which also includes information regarding the Privacy Act of 1974, prior to receiving access to the DoS networks and getting a badge for facility access. Users must complete initial and annual cybersecurity awareness training. The training consists of computer security awareness to include the proper handling of PII. The course PA459 - Protecting Personally Idenfiable Information - is also mandatory for all Department employees.

(e) **Are any security controls such as encryption, strong authentication procedures, or other controls in place to make the information unusable to unauthorized users?** Yes __X__ No ____

If yes, please explain.

Security controls to make information unusable to unauthorized users include:

- **Restricted GFMS Access**
  A potential user must fill out an access request form with his/her supervisor's consent.

- **To maintain access, annual training required**

Every user must attend a security briefing to receive access to the DoS networks. Subsequently, all GFMS users must complete annual cybersecurity and privacy training to maintain their GFMS access.

- **Roles & Permissions within the GFMS application**
  All rights to information and functionality within GFMS are enforced by user profiles to limit access according to the principles of least privilege and separation of duties.

- **GFMS has single sign on**
  GFMS users will not be able to log onto another user's GFMS account while logged onto the DoS network under their credentials.

(f) How were the security measures above influenced by the type of information collected?
Sensitive information is required to be collected. The security measures were designed to minimize privacy risks without hampering necessary business operations of the State Department.

9. Data Access

(a) Who has access to data in the system?

Access to GFMS is limited to authorized DoS government and contractor employees who have a need for access to the system. All users maintain a security clearance level at least commensurate with public trust positions.

(b) Access to data in the system is determined by:

The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? Yes __X__ No ____

(d) Will all users have access to all data in the system or will user access be restricted? Please explain.

User access is restricted. GFMS users may only access data to which they have a valid business requirement to access. All rights to information and functionality within GFMS are enforced by user profiles according to the principles of least privilege and separation of duties.

(e) **What controls are in place to prevent the misuse (i.e. unauthorized browsing) of data by users having access to the data?**

Activity by authorized users is monitored, logged, and audited in accordance with US Department of State Diplomatic Security configuration guidelines at the database and server level. The system and database administrators are located in CGFS and are the only users with direct access to the database for the purpose of performing maintenance. All rights to information and functionality within GFMS are enforced by user profiles according to the principles of least privilege and separation of duties. All access to GFMS is logged by the operating system and/or the application, depending on the activities being performed.