# GFACS PIA

## 1. Contact Information

**A/GIS Deputy Assistant Secretary**
Bureau of Administration
Global Information Services

## 2. System Information

(a) Name of system: Global Foreign Affairs Compensation System

(b) Bureau: Bureau of the Comptroller and Global Financial Services (CGFS)

(c) System acronym: GFACS

(d) iMatrix Asset ID Number: 5441

(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): Oracle and Windows upgrades

## 3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The GFACS Authority to Operate (ATO) expires November 2019.

(c) Describe the purpose of the system:
GFACS is the Department's global pay system for employee payroll and annuity pay processing. The application calculates payments for all Civil and Foreign Service personnel, the Foreign Nationals at the embassies, consulates and missions abroad and Foreign Service Annuitants hereafter known as Payee.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
The elements of PII collected are:

- Name
- Address

- SSN
- Date of Birth
- Individual Financial Institution - banking
- Individual Financial Information - net/gross pay and withholdings
- Individual Legal Information - garnishment information

Other information collected by the pay system from State Department Payees are marital status, beneficiaries, tax exemptions, bank information, bond information, and union dues information.

The source of this information is the Payee's Human Resources (HR) files contained in the Global Employee Management System (GEMS), information provided by the Payee through OPM's Employee Express or Annuitant Express systems, and information provided directly to the department by the Payee.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
22 U.S.C. 2651a (Organization of the Department of State);
22 U.S.C. 3921 (Management of Service);
5 U.S.C. 301 (Management of the Department of State);
22 U.S.C. 4042 (Maintenance of the Foreign Service Retirement and Disability Fund);
42 U.S.C. 653 (the Personal Responsibility and Work Opportunity Reconciliation Act of 1996);
Executive Order 11491, as amended (Labor-management Relations in the Federal Service);
5 U.S.C. 5501-5584 (Pay Administration); and
31 U.S.C. 901-903 (Agency Chief Financial Officer's Act).

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:

- SORN Name and Number: STATE-30, Personnel Payroll Records
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): February 11, 1998

☐No, 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

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 ☐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)): A-05-013-04
- Length of time the information is retained in the system: Destroy after 3 years.
- Type of information retained in the system:
  Information needed to calculate payments and historical Payee payments

## 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 (people who are not U.S. Citizens or LPRs) - Annuitants

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

- If yes, under what authorization?
22 U.S.C. 4042 (Maintenance of the Foreign Service Retirement and Disability Fund);
42 U.S.C. 653 (the Personal Responsibility and Work Opportunity Reconciliation Act of 1996);
Executive Order 11491, as amended (Labor-management Relations in the Federal Service);
5 U.S.C. 5501-5584 (Pay Administration); and
31 U.S.C. 901-903 (Agency Chief Financial Officer's Act)

(c) How is the information collected?
Information is collected by HR from the employee upon hiring or the annuitant upon retirement and from their personnel and payroll records. This information is obtained by HR via:

- SF 50 – Personnel Action Form
- JF62 – PSC Employee Actions Form
- Form 212 Allotment Form
- DS 1992 Allotment Form

The necessary data needed to pay a Payee is transferred electronically, via system to system data file transfer, from the HR system (GEMS) into GFACS.

The following information is provided to GFACS electronically, via secure file transfer protocol (FTP), as needed by Federal agencies and/or third party sources:

- Office of Personnel Management (OPM) – federal employee health benefits, TSP contribution changes
- National Finance Center/USDA (NFC) – federal employee health benefits pay
- Long Term Care Partners – Long-term care insurance, dental and vision insurance
- AFSPA (American Foreign Service Protective Association) – Information collected includes Union dues for the individual employee or annuitant
- Federal Employees Education Assistance Fund (FEEA) Child Care Subsidy Data Import

The Department of State has MOUs (Memorandums of Understanding) and ISAs (Interconnection Security Agreements) with these other Federal Agencies to process data files sent and received.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

Click here to enter text.

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

All information collected from a Payee in GEMS and GFACS is verified for accuracy by HR Specialists and Pay Technicians using the payee's identification and banking documents and crosschecking the information between the two systems. The Payee has the ability to view their personal information via HR Online, Employee Express and Annuitant Express. The Payee can request changes through both the HR and Payroll offices, if necessary.

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

All Payee information is verified by pay technicians prior to the respective pay dates when the pay is calculated.

An electronic file from the Social Security Administration (SSA), is received monthly, is compared with GFACS data to identify Social Security Numbers of deceased Payees.

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

No commercial information is used in GFACS, nor is the information publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?
Notice is provided to individuals whose personal information is collected in GFACS through the publication of System of Records Notice (SORN), State- 30, Personnel Payroll Records. Most of the forms used to collect information, from the Internal Revenue Service (IRS) (i.e. the W-4 and W-4P forms) or the Department of State, contain Privacy Act statements, alerting the record subject of the collection and use of personal information.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?
Consent is given by the Payee when hired by the Department of State when they sign the employment agreement. All information collected in GFACS is necessary to process payments for the Payees. Failure to provide this information could result in the inability to process the payment.
- If no, why are individuals not allowed to provide consent?
Click here to enter text.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
This system collects the absolute minimum amount of Personally Identifiable Information required to solely satisfy the functionality of this system.

## 5. Use of information

(a) What is/are the intended use(s) for the information?
The information in this system is used to calculate and process accurate payments to eligible Payees and provide mandated reporting to government entities.

(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

If yes:

(1) What types of methods are used to analyze the information?
Payee payment reports are produced as part of the normal pay cycle to verify the accuracy of payments.

(2) Does the analysis result in new information?
Each quarter, payment and tax withholding information is generated and provided to the IRS and a variety of state and local tax authorities, per regulations. The Office of the Legal Advisor also verifies garnishment 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.

The information is shared within the Department with the HR bureau (HR/EX) on a routine basis and ad hoc as directed by the senior-level department management.

The information from GFACS is shared outside of the Department of State with:

- Federal, state, city, and foreign government agencies that are issued tax reports and other mandated information that is required for evaluation and oversight of federal personnel management.
- Data is shared with Federal disbursing offices to provide payment.
- The Internal Revenue Service and the Social Security Administration, which are sent tax and withholding data.
- The Office of Personnel Management, which receives the total record of the Civil Service Retirement System and the Federal Employees Retirement System, benefit deductions, including life and health insurance.
- For Foreign National employees only – extracts of social security contributions for State Department foreign national employees in select countries such as France would provide the Country (France) with the social security contributions made on behalf of the French Foreign Nationals who are the Department of State employees supporting the embassy, consulate or mission abroad

(b) What information will be shared?

The following information is shared with all entities listed in 6(a), including the HR bureau (HR/EX):

- Personnel Data - SSN, name, address
- Individual Financial Institution - banking information
- Individual Financial Information - net/gross pay and withholdings
- Individual Legal Information - garnishment information
- Individual Benefit Information – health and life insurance

(c) What is the purpose for sharing the information?

The information is shared to verify and manage payments to the Payee and to other entities, such as insurance companies, on behalf of the Payee.

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

Any GFACS data shared internally or externally is transferred by secure transmission via Connect Direct, a software product used to securely transfer electronic files between agencies.

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

External sharing - The Department of State has MOUs (Memorandums Of Understanding) and ISAs (Interconnection Security Agreements) with other Federal Agencies, to process data files sent and received, which describe data and safeguards to data during transfer and at rest in the application data base.

Internal sharing – MOU's are written and signed by senior management within the department that describe the data and safeguards to data during transfer and at rest in the application database.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
There is always a concern of collecting PII that is not needed for the system to complete the function and disclosure of PII to individuals that do not have a need to know.

All needed PII is identified in the SORN. It is stored and maintained in accordance with established Departmental PII standards. Use and disclosure is only with respect to the performance of duties related to the maintenance and processing of Payee records or in compliance with other federal, state or local tax authorities. The potential risk of sharing PII is mitigated through the use of secure transmission methods and established data safeguards in and MOU/MOA.

## 7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Select information is available to the Payee via the OPM Annuitant or Employee Express websites if the individual has established a user account on that site.
Payees who have reason to believe that their information is incorrect should contact the Managing Director of Global Compensation at 1969 Dyess Ave. Charleston, SC, 29405 or via e-mail at PayHelp@state.gov.

Payees may also contact the Department via HR Shared Services by phone at 866-300-7419 or via e-mail at HRSC@state.gov

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.
Select information is available to the Payee via the OPM Annuitant or Employee Express websites if the individual has established a user account on that site.
Payees who have reason to believe that their information is incorrect should contact the Managing Director of Global Compensation at 1969 Dyess Ave. Charleston, SC, 29405 or via e-mail at PayHelp@state.gov.

Payees may also contact the Department via HR Shared Services by phone at 866-300-7419 or via e-mail at HRSC@state.gov
If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
Payees are notified of the procedures to correct their information by HR Services via email, postal mail, online websites, and/or payee statements.

## 8. Security Controls

(a) How is the information in the system secured?
The information is secured via the application through use of access controls based upon the user's job function. The information is secured from threats outside the application via security controls on the department's internal network (OpenNet) and by Transparent Data Encryption (TDE) functionality on the database.

(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.

GFACS is a single sign on system using a user's OpenNet credentials. Application specific user security profiles are established by the office of the Managing Director of Global Compensation, documented in the segregation of duties guide, and granted by the CGFS Information System Security Officer (ISSO). These security roles define the specific types of data an individual user can access and actions that a user can perform within the system in effort to prevent fraud and error.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
Activity within the system is audited via audit tables in the database. The system administrator has the capability of printing audit reports for data changes through the GFACS Audit and Monitoring Report module for periodic review.

GFACS provides trigger-based auditing functionality. This function allows GFACS to monitor changes to PII and sensitive data. This level of auditing maintains the integrity of the data by providing proactive security measures. GFACS takes advantage of Oracle database triggers and the audit and/or notification is triggered when a user makes a change to a specified field that is being monitored.

(d) Explain the privacy training provided to authorized users of the system.
Orientation of new employees is routinely conducted to address system access and privacy issues. Annual Cybersecurity Awareness Training, which contains a privacy component, and one-time PII training, PA 459 offered by FSI, are mandatory. The ISSO conducts periodic briefings and re-certifications of user IDs and passwords.

(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 ☐No
If yes, please explain.
GFACS will not allow access to anyone who does not authenticate via single sign-on using the department's Active Directory (LDAP) and has the appropriate role granted to their user account. The database is protected by Oracle's Transparent Data Encryption that is an approved FIPS 140-2 compliant encryption algorithm.

(f) How were the security measures above influenced by the type of information collected?
This application was assessed as a moderate level system and the data is protected in accordance with the regulations that apply to a moderate level system.

## 9. Data Access

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

Administrator Roles: Allows access to run processes through the process scheduler and install new software within the software configuration management process.

GFACS HR Roles: Allows access to view and update Payee personnel data and view payment information.

GFACS Financial Roles: Allows access to view and update Payee payment data and view some personnel information

(b) How is access to data in the system determined?

Established business processes are used to define the roles that are required by the system to maintain data integrity, accuracy, and confidentiality. Assignment of the roles is based on the user's job function. This process is accomplished using one of the GFACS System Access Request forms. This form must be signed by the designated office director/supervisor, the prospective end user, and counter signed by the ISSO.

Once a form has been approved, the access request is forwarded to the ISSO who establishes or changes the user in the GFACS Security tables, assigning them the appropriate GFACS Security Role.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No
The procedures for granting or changing access to users in GFACS are documented in a Quality Work Instruction (QWI) found in the GFSC Knowledge Base on OpenNet.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
User access is restricted to different subsets of the data defined as part of an individual's Departmental job responsibilities.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
Security controls were established during GFACS implementation that segregated data access to roles necessary to perform specific business functions. Users that have a business need to see specific data are assigned to specific roles.