PRIVACY IMPACT ASSESSMENT

Global Foreign Affairs Compensation System PIA

1. Contact Information

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

2. System Information

(a) October 2022
(b) Name of system: Global Foreign Affairs Compensation System
(c) System acronym: GFACS
(d) Bureau: Bureau of the Comptroller and Global Financial Services (CGFS)
(e) iMatrix Asset ID Number: 5441
(f) Child systems (if applicable) and iMatrix Asset ID Number:
(g)

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial reauthorization

(h) Explanation of modification (if applicable):

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b)
☒ Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

GFACS is the Department of State's (Department) global pay system for employee payroll and annuity pay processing. The system calculates payments for all Civil and Foreign Service personnel, Locally Employed (LE) staff at embassies, consulates, and

missions abroad, and Foreign Service Annuitants. Hereafter, all will be addressed as Payee.

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

The elements of PII collected are:

- Name
- Personal Address
- Social Security Number (SSN)
- Date of Birth
- Individual Financial Institution – banking
- Individual Financial Information - net/gross pay and withholdings
- Individual Legal Information - garnishment information
- Individual Benefit Information – health and life insurance which includes an individual's SSN
- Work e-mail
- Work title

(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. 4041 (Administration);
42 U.S.C. 653 (Federal Parent Locator Service);
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, etc.)?

☒Yes, provide:

- SORN Name and Number:
  Personnel Payroll Records, STATE-30

- 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 Office 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 (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):

- Disposition Authority Number:
  DAA-GRS-2016-0015-0007 (GRS 2.4, item 061)

- Length of time the information is retained in the system:
  Temporary. Destroy when 3 years old or after Government Accountability Office (GAO) audit, whichever comes sooner, but longer retention is authorized if required for business use. (Supersedes GRS 2, item 22c)

- Type of information retained in the system:
  Payroll system reports providing fiscal information on agency payroll. Records produced in administering and operating payroll functions of a general nature and not linked to an individual employee's pay.

(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) On what other entities above is PII maintained in the system?

☒ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☐ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary? ☒Yes ☐No ☐N/A

- 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)

(d) How is the PII collected?

The sources of the PII are:

- The Payee's human resource (HR) files contained in the Global Talent Management's (GTM) system Global Employee Management System (GEMS). Theses HR files can include the SF-50 (Notification of Personnel Action Form), JF-0062 (Personal Services Contracting Action Form), Form 212 Allotment Form, and the DS-1992 (Allotment of Pay/Prior Service Credit Application). The HR files are transferred electronically, via system-to-system data file transfer, from GEMS into GFACS.
- Information can be provided by the Payee through OPM's Employee Express or Annuitant Express systems which is transferred to GFACS via electronic interface.

The following PII 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, Thrift Savings Plan (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 Memorandums of Understanding (MOUs) and Interconnection Security Agreements (ISAs) with these Federal Agencies to process data files sent and received.

(e) 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.

(f) What process is used to determine if the PII is accurate?

All PII collected from a Payee is verified for accuracy by HR Specialists and Pay Technicians when cross checking the payee's identification and banking documents against GEMS. There is an inter-system validation process that ensures the data in GFACS matches GEMS.

The Payee has the ability to view their personal information via Employee Express, Annuitant Express, and HROnline (a child system of GEMS). HROnline provides the self-service functionality for GEMS data to be presented to the employee. If the Payee notices inaccuracies they can request changes through both the HR and Payroll offices, if necessary.

(g)

Yes, the information is current. All Payee information is verified by Pay Technicians prior to the respective pay dates when the pay is calculated.

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

(h) 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.

(i) How was the minimization of PII in the system considered?

The PII captured and stored in GFACS is limited to the necessary data required to process pay to include disbursement, taxation, and authorized deductions.

(a) What is/are the intended use(s) for the PII?

The PII in GFACS is used to assist HR Specialist and Pay Technicians in identifying a payee in order to process their pay including disbursement, taxation, and deductions.

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

Yes, the use of the PII is relevant to the purpose for which the system was designed. GFACS is the Department's global pay system for employee payroll and annuity pay processing. The PII in this system is used to process accurate payments to eligible Payees.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

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

(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

(d) If the system will use test data, will it include real PII?

☐ Yes ☐ No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

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

Internal: The information is shared with the Global Talent Management (GTM/EX) on a routine and ad hoc basis as directed by the senior-level department management.

External: 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.

American Employees and Annuitants

- Data are shared with Federal disbursing offices to provide payment.
- The Internal Revenue Service (IRS) and the Social Security Administration (SSA), which are sent tax and withholding data.

The Office of Personnel Management (OPM), which receives benefit deductions, including life and health insurance, and the total record of pay types in the Federal Government (formally referred to as the Civil Service Retirement System and the Federal Employees Retirement System).

Locally Employed (LE) staff

- Department posts are provided extracts of social security contributions for the Department's foreign national employees in select countries.

(b) What information will be shared?

Internal: The following information is shared with GTM/EX:

- Personnel Data - SSN, name, personal 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 which includes a Payee's SSN

External: The following American and Annuitant information is shared with the entities listed in 6(a):

- 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 which includes a Payee's SSN

The following Locally Employed (LE) staff information is shared with the entities listed in 6(a):

- Personnel Data - name, address
- 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?

Internal: 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.

External: 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?

Internal: Any GFACS data shared internally is transferred by secure transmission via the Secure Hypertext Internet File Transfer System (SHIFTS), a transmission method that securely transmits electronic files through an encrypted tunnel. This encryption is approved by the Federal Government as defined in Federal Information Processing Standard (FIPS) 140-2.

External: Any GFACS data shared externally to U.S. government agencies is transferred by secure transmission via a commercial-off-the-self (COTS) software called Connect Direct that is a Department purchased product.

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

Internal: Memorandums of Understanding (MOUs) 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. Also, access to SHIFTS is restricted to OpenNet and users are designated by the data owners.

External: The Department has MOUs and Interconnection Security Agreements (ISAs) with other government 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. There are inherit safeguards with Connect Direct along with its access controls.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Yes, notice is provided to the subject at the point of collection. 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 (mentioned in 4d), contain Privacy Act Statements, alerting the record subject of the collection and use of personal information before beginning ingested into GFACS. There is also notice provided to the Payee in OPM's Employee Express or Annuitant Express systems.

Notice is also provided to individuals whose personal information is collected in GFACS through the publication of System of Records Notice (SORN), State-30, Personnel Payroll Records.

(b)

☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

Payees do not provide their information in GFACS and are not able to directly access their information in the system. The information collected will be ingested into Department systems used to process their pay. Consent is given by the Payee when they sign HR forms upon being hired by the Department of State. 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.

(c) What procedures allow record subjects to gain access to their information?

Payees are not able to directly access their information in GFACS. The Payee has the ability to view their personal information via Employee Express, Annuitant Express, and HROnline (a child system of GEMS). the individual has to have an established user account on Employee and Annuitant Express to access.

Payees who would like access to their information 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.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Payees are not able to directly access their information in GFACS but if they notice inaccurate or erroneous information, they can update select information in the systems that feed to it.

Payees who have reason to believe that their information is incorrect should also 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.

(e) By what means are record subjects 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. Notice is also provided to individuals whose personal information is collected in GFACS through the publication of System of Records Notice (SORN), State-30, Personnel Payroll Records.

8. Security Controls

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

The information is secured from threats outside the application via inherent security controls on the Department's internal network (OpenNet) in addition to the access controls which are based upon the user's job function. GFACS is also a single sign on system using a user's OpenNet credentials.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

- Administrator role: Privilege to run processes through the process scheduler and install new software within the software configuration management process. This role has access to all PII in the system.
- GFACS HR role: Privilege to view and update Payee personnel data and view payment information. This role has access to all PII in the system.
- GFACS Financial role: Privilege to view and update Payee payment data and view some personnel information. This role has access to all PII in the system.
- ISSO role: Has privilege to view, add, and remove users, assign roles and privileges. This role has no access to PII.

(c)

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.

GFACS is a single sign on system using a user's OpenNet credentials.

(d) How is access to data in the system determined for each role identified above?

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. Roles are determined by the position occupied by the user and/or a request from the supervisor. No role request can be granted if the Segregation of Duties document is violated.

- Administrator role: Has access to the entire system to include all hardware, software, and data.
- GFACS HR role: Has access to view and change personnel/biographical data but view only for payroll data. This only requires limited access for these individuals.

- GFACS Financial role: Has access to view and change payroll data but view only for personnel/biographical data. This only requires limited access for these individuals.
- ISSO role: Has access to add and remove users, assign roles and privileges but no access to PII data.
-

(e)

Activity within the system is audited via audit tables in the database. The Administrator Role 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.

(f) 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.

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

Orientation of new employees is routinely conducted to address system access and privacy issues. The annual Cybersecurity Awareness Training (PS800) course, which contains a privacy component, and the biennial PII training course (PA318 – Protecting Personal Identifiable Information), offered by FSI, are mandatory. The ISSO conducts periodic briefings and re-certifications of user IDs and passwords.