PEACE CORPS PRIVACY IMPACT ASSESSMENT

Peace Corps System Name and Acronym: Gov Time and Attendance Application (GovTA)

Managing Office: Office of Human Resources (OHR)

PIA Approval date: October 20, 2023

1. Is this a new or revised electronic information system? If revised, describe revisions.

GovTA is a new information system. It is replacing WebTA, which performs the same functions as WebTA.

If any question does not apply, state not applicable (N/A) and explain why.

2. Identify who the Personally Identifiable Information (PII) is collected from:

- ☐ Members of the public, including Peace Corps Volunteer applicants and interns
- ☑ Federal employees/federal contractors/Peace Corps Volunteers
- ☐ Both members of the public and Peace Corps personnel

3. Legal Authority. Cite the legal authorities that permit and authorize the collection of this information by this IT system.

The Peace Corps Act (22 U.S.C. 2501 et seq.), as amended; Executive Order 9397, as amended, Numbering System for Federal Accounts Relating to Individual Persons.

4. Purpose. Explain the purpose of the system (e.g., nature and source).

The GovTA application (GovTA) is a web-based time and attendance (T&A) application specially designed and developed by the Ultimate Kronos Group (UKG) for United States Department of Agriculture(USDA) National Finance Center (NFC) and its customers to meet the T&A reporting requirements for Federal department and agencies and their employees. Peace Corps employees use GovTA to record their time and leave. The users log into GovTA to record arrival and departure times. The recorded time goes to the user's supervisor for approval. GovTA tracks the work

schedule, leave, donated leave, overtime, and the onsite and telework hours worked for all Peace Corps (PC) federal staff members. It can also provide statistical information related to the Agency's telework and remote workforce. GovTA allows the individual to submit electronic leave requests, donate leave, and validate their time and attendance online. Supervisors review, approve, decline, and validate the timesheets, leave requests, and other requests related to time and attendance for employees under their supervision.

Sources of information can be found at multiple user levels. OHR creates the employee's unique user profile upon entry into the Agency. OHR uses information from the form OF-0306, "Declaration of Federal Employment," to include the individual's Social Security number (SSN). The SSN is necessary to complete payroll functions, and properly identify the individual for contributions to Social Security and other financial requirements. Individuals with official access are also sources of information: the employee makes entries for work and leave time in his/her online profile; the Supervisor reviews and verifies the employee's timecard; the Timekeeper reviews the employee's bi-weekly record and supports the employee and Supervisor; the Master Timekeeper (HR Payroll employee) can take action when an error occurs or an adjustment is needed; the Master Supervisor (HR Payroll employee) can perform when the employee's supervisor is not available. The System Administrator (HR payroll employee) performs the Volunteer Leave Transfer Program, reporting and systemic reviews/audits. Authorized OHR personnel use the individual's unique user ID to pull records or information related to that individual.

5. List all forms of Personally Identifiable Information (PII) that is collected, maintained, or disseminated.

The PII that is collected includes the employee's profile which includes first name, last name, SSN, partial SSN, unique user ID, unique password, and any protected health information typed in by the employee in the notes section. The employee may provide additional PII details in notes for leave requests and related to hours earned.

6. Why is PII being collected (e.g., to determine eligibility)? Does the IT system collect PII directly from individuals, or from another system?

The information is collected in order to prepare the individual's payroll. It also accounts for leave earned and used, identifies work time and leave categories, and serves as a system of record for employee leave approvals, denials, and incorporates leave transfer to a gaining agency. The designated OHR Timekeeper manually inputs the individual employee's PII, such as the first name, last name, and SSN into GovTA to create the new employee profile. Employee information can be loaded to GovTA through the bi-directional feed between the Agency and USDA's NFC. However, the Peace Corps OHR manually adds employees' profiles into GovTA. An individual employee may contact the OHR Timekeeper or representative to request correction if the user profile PII is incorrect.

7. Sharing and Disclosure.

a. Will the PII from this system be shared with another agency? If yes, list the agency, all types of PII that is shared, and why this is shared outside our agency.

Yes, the information is shared with USDA -National Finance Center (NFC), the Peace Corps' Payroll provider. The information is used to update the NFC system, and the Employee Personal Page, which is also supported by USDA.

b. Is the sharing pursuant to a Memorandum of Understanding, Computer Matching Agreement (CMA), or other type of approved sharing agreement with another agency?

Yes. NFC is a Shared Service Provider for Financial Management Services and Human Resources Management Services. NFC is an Office of Personnel Management-certified Human Resources Shared Service Center. There is an Inter-agency agreement between Peace Corps and NFC signed on July 11, 2022.

8. Notice of the collection of information.

a. Do individuals have the opportunity to object or to consent to the particular use of their PII prior to collection?

☐ Yes ☑ No

b. If "Yes," describe the Privacy Act Statement (PAS) or notice provided to the individual prior to collection of his or her information. If "No," state the reason why individuals cannot give or withhold their consent. Identify if this is not applicable because information is obtained from an existing information system or source.

The individuals are not able to object or consent to the particular use of their PII prior to the collection because OHR collects and inputs the individual's PII in order to prepare the individual's payroll. This is required to process the federal payroll activities. OHR enters an individual's name and SSN into GovTA upon entry of employment or appointment. The individual submits biweekly entries to fulfil federal payroll and time and attendance requirements.

c. List any Peace Corps form(s) or federal form(s) used to collect PII for this system. Each PC form must have a Privacy Act Statement.

OF-0306: Declaration of Federal Employment.

d. Provide the OMB Control number and the agency number for the collection if this collection is covered by the Paperwork Reduction Act (PRA).

OMB No. 3206-0182.

9. Security.

a. What administrative, technical, and physical security safeguards/controls are in place to protect the PII?

The privacy risks associated with this IT system are unauthorized access, unauthorized disclosure of PII, and the risk that a user may enter incorrect information. Peace Corps and the hosting facility (USDA/NFC) have administrative, technical, and physical security controls in place to mitigate these risks. Peace Corps has a service level agreement and interagency agreement with NFC that define the agreed-upon services provided by the U.S. Department of Agriculture (USDA), Office of the Chief Financial Officer, National Finance Center (NFC) for hosting the GovTA system. Additionally, it identifies the customer's responsibilities required to ensure successful operations. The physical controls are not outlined in this document. This is an authorized system hosted and managed by USDA/NFC that has undergone a security review and authorization of administrative, technical, and physical security safeguards and controls on an annual basis.

Administrative Controls: One of the security controls includes administrative controls. Access controls to GovTA require different authorized levels of roles and responsibilities. This is managed through a set of privileges granted only by the system administrator based upon role and group levels. Elevated roles and access privileges are assigned to individuals who have the need to know to fulfill time and attendance responsibilities. Authorized users are trained in the proper handling of personally identifiable information and their official responsibilities under the Privacy Act and Peace Corps security controls and technical governance for the rules of behavior. Access to GovTA can only be via PC network. GovTA uses role-based access and user ID/Password to protect access to data. Employees have access only to their own records; supervisors have access only to employees they supervise.

Technical Controls: The system also has several technical controls. GovTA has access controls and user account authentication mechanisms to secure the information. Access to the system requires the use of a user ID and password. USDA also utilizes an eAuthetication system that allows PC users to create an eAuthetication (eAuth) account. This eAuth account is created after the user has been verified and the account credential have been linked to the USDA eAuthetication system. A user must have undergone background and security clearance and gained approval before accessing the PC network. Users can then access GovTA after authorization via the PC network. IT Security will provide access after the individual reads and signs the PC Rules of Behavior and completes all the mandatory training. HR personnel will create the user profile, and a temporary password will be sent to the user to gain access to GovTA and create a new unique password based on the PC password requirements. Information is encrypted using Secure Socket Layer (SSL) protocol, and HTPPS is used for all web access to GovTA.

Physical Control: The GovTA is hosted by USDA . The hosting agency server location meets physical security requirements.

b. Has a system security plan been completed for the information system?

Yes, a System Security Plan is in place. It was completed on October 2, 2023.

10. Privacy Act System of Records. Identify the System of Record Notice (SORN) that covers this IT system, or state if a SORN will be created under the Privacy Act, 5 U.S.C. 552a.

PC-6, Employee Pay and Leave Records.

11. Records Retention and Disposition. Identify the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system, or for the records maintained in the system, as well as the record retention instructions.

Records are scheduled to be retained and disposed of in accordance with NARA's GRS 2.4, item 030 (Disposition Authority: DAA-GRS-2019-0004-0002). The record disposition is temporary. The agency is required to destroy the records after three years.