U.S. Department of Commerce
Office of Human Resources Management (OHRM)

Privacy Impact Assessment for GovTA (OS-GovTA)

Reviewed by: Tahira Murphy, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Tahira Murphy for Charles Cutshall 5/18/2023

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of Human Resource Management (OHRM) / GovTA

Unique Project Identifier: GovTA OS-GovTA

Introduction: System Description

Provide a brief description of the information system.

GovTA is an automated commercial-off-the-shelf (COTS) Time and Attendance system from Ultimate Kronos Group (UKG) that utilizes a web interface to an Oracle Time & Attendance database to record time and attendance data for Department of Commerce (DOC) employees. Time and Attendance data is sent to the National Finance Center (NFC) on a bi-weekly basis.

NIST/Census Commerce Business Solutions (CBS) - The National Institute of Standards and Technology (NIST) uses a supplemental file from GovTA to obtain a labor/cost estimate, and Census uses it to validate accounting against CBS valid accounts as well as with an interface to import Decennial Census payroll data.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

Office of Human Resources Management (OHRM) is responsible for planning, developing, administering, and evaluating the human resources management programs of the Department. This enables DOC to acquire and manage a dedicated, diverse, motivated, and highly qualified workforce to accomplish its mission and achieve its goals, while ensuring compliance with pertinent Federal, Office of Personnel Management (OPM), Office of Management and Budget (OMB), and Department of Labor, policy, and administrative mandates.

- GovTA is Kronos Proprietary software is used to record DOC employee's time and attendance data. Employees enter their own time and attendance data. The data is transmitted bi-weekly to NFC for employee pay processing.

(b) System location

The system is hosted by AWS GovCloud and managed by Lentech, Inc.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

NIST/Census CBS - NIST uses a supplemental file from GovTA to obtain a labor/cost estimate, and Census uses it to validate accounting against CBS valid accounts as well as

with an interface to import Decennial Census payroll data. The National Oceanic and Atmospheric Administration (NOAA) loads time-sheet data from files sent from ships. The NFC Payroll System - GovTA collects bi-weekly payroll data from this input to create and transmit a payroll time and attendance file to NFC, the payroll processor at the U.S. Department of Agriculture (USDA). This is a Secure File Transfer Protocol (SFTP) transmission configured and monitored by a GovTA Administrator, with password maintenance and access provided by NFC.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

GovTA is a timekeeping system that stores personal identifying information (PII) for the purposes of passing information to the NFC Payroll system. The system collects data daily from user input. This input consists of Work Data, Leave Data and Dollar Transaction Data.

Work Data consists of weekly (and ultimately, bi-weekly pay period) input of daily labor descriptive data related to daily work duties. A daily occurrence consists of a transaction code describing the nature of the work duty, an accounting code for where the financial system will charge this time and the actual time worked. It is also possible to include a clock time range worked within each workday. There may be multiple occurrences of work data in each pay period, and multiple occurrences of work data in each day.

Leave Data includes weekly (ultimately, bi-weekly pay period) input of daily time off and time off award data, a transaction code describing the type of leave being taken, an account code to trigger the correct charge-back in downstream financial systems and actual time taken as leave. There may be multiple occurrences of work data in each pay period, and multiple occurrences of leave data in each day.

Dollar Transactions include employee requests for reimbursement related to work-incurred expenses. This includes a transaction code describing the type of expense incurred, an accounting code to charge this expense and the actual expense amount requested.
This data is collected, maintained, and used for payroll generation via downstream system, ad-hoc research and reporting and leave-related reporting and tracking.

Each user can be assigned a variety of roles that allow varying levels of data access. These permissions range from basic employee-related time and leave entry to Master User and Administrator, who can see and manipulate much larger data populations and affect system administration-type changes to system operational parameters and functions.

GovTA collects bi-weekly payroll data from this input to create and transmit a payroll time and attendance file to NFC, the payroll processor at USDA. This is a SFTP transmission configured and monitored by a GovTA Administrator, with password maintenance and

access provided by NFC. CENSUS and NIST extract a version of this payroll file via a vendor provided custom process and upload it to downstream financial systems for budget analysis.

CENSUS receives remote input from GovTA to timesheets via a vendor provided custom interface from a system called WebFRED. The remote users do not have direct access to GovTA's timesheet entry and maintenance functions, so this system replaces it to the extent that the remote offices need it to. This remote system also has assigned and restricted access and is limited to timesheet and code- related maintenance.

(e) *How information in the system is retrieved by the user*

CENSUS receives remote input from GovTA to timesheets via a vendor provided custom interface from a system called WebFRED. The remote users do not have direct access to GovTA's timesheet entry and maintenance functions, so this system replaces it to the extent that the remote offices need it to. This remote system also has assigned and restricted access and is limited to timesheet and code-related maintenance.

All other departmental users can print reports containing only data that is allowed by their role within all GovTA. It is the responsibility of the users to handle printed media in accordance with established policies/procedures/rules of behavior and governmental record retention regulations of their bureau and DOC. Users can download information, again based on their assigned user role within GovTA. In terms of removable media, it is the user's responsibility to handle digital media in accordance with established policies/procedures/rules of behavior and governmental record retention regulations of their bureau and DOC.

(f) *How information is transmitted to and from the system*

Information is transmitted across approved encryption protocols such as hypertext transfer protocol secure (HTTPS), Secure Shell (SSH), and SFTP. Sensitive data transmissions are encrypted according to NIST 800-18, Federal Information Processing Standards (FIPS) 186, Digital Signature Standard and FIPS 186-6, and Secure Hash Standard issued by NIST when necessary.

(g) *Any information sharing*

GovTA data is transmitted bi-weekly to NFC for DOC employees pay processing.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

Includes the following, with all revisions and amendments: 5 United States Code (U.S.C.) 301; 44 U.S.C. 3101; Executive Office (E.O.) 12107, E.O. 131614, 41U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999, DAO 202-430 (performance management system), DAO 205-16 management of electronic records.

The authority to deliver, maintain, and approve Department-wide and bureau-specific automated human resources systems and serve as the focal point for the collection and reporting of human resources information within DOC is delegated to OHRM. This authority is identified by Departmental Organization Order (DOO) 20-8, Director for Human Resources Management, Section 4.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The FIPS 199 for GovTA is categorized as Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_X_ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: SSN is used to ensure accurate employee reporting and is a required unique identifier for NFC.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	X
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

Information required by GovTA is provided by the employee during start of employment. Users can review and update their information when gaining access to GovTA.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.

X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

GovTA is used to track DOC employee's hours; so, each employee can be paid and compensated accordingly.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

GovTA data needs to be retained for 6 years. After this time, the data will be processed through existing DOC or Federal mandated data shredding and disposal processes or archived and placed in appropriate secure archival storage. Related training is held as part of annual DOC security training. Please see this web page: https://connection.commerce.gov/reference-and-other-resources/annual- cybersecurity-awareness-training. There is a potential for insider threat. Employees acting with privileged access in GovTA, including the following credentials: Timekeeper, Supervisor, Administrator, HR Admin, Master Timekeeper, and Master Supervisor, are "classified" as "positions of trust." They receive GovTA's Roles and Responsibilities document. Each role higher than "employee" (personal timesheet entry only) has certain permissions allowing for the job associated with it to be completed successfully. When an employee is assigned to one of these roles, their supervisor will evaluate their permissions and assign access on a need-to-know basis. They are in a position of trust and are expected to perform quality control based upon their specific role. All information containing PII or elements of information that can be used to identify

individuals must be emailed as required using Kiteworks secure email. User access to the various permissions in GovTA is audited per DOC policy. Please see this bulletin: https://www.commerce.gov/sites/default/files/2018-12/hr-bulletin-FY15-196.pdf.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		
DOC bureaus	X		
Federal agencies		X	
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: NFC Payroll System - GovTA collects bi-weekly payroll data from this input to create and transmit a payroll time and attendance file to NFC, the payroll processor at USDA. This is a secure SFTP transmission configured and monitored by a GovTA Administrator, with password maintenance and access provided by NFC. WebFRED- CENSUS receives remote input from GovTA to timesheets via a vendor provided custom interface from a system called WebFRED. The remote users do not have direct access to GovTA's timesheet entry and maintenance functions, so this system replaces it to the extent that the remote offices need it to. This remote system also has assigned and restricted access and is limited to timesheet and code- related maintenance.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://docgovta.commerce.gov/govta.	
X	Yes, notice is provided by other means.	Specify how: Once users are logged in to GovTA, they get the message "The data in this system is Privacy Act protected, thus users must obey all agency policies regarding the protection of the data. Privacy Act data must never be shared with anyone who does not have a work-related need to know."
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals are not given an opportunity to give consent after the initial HR hiring process. If they declined to provide PII, employees would not receive employment and/or receive paychecks.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals are not given an opportunity to give consent after the initial HR hiring process. If they declined to provide PII, employees would not receive employment and/or receive paychecks.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals can review and update their PII within their GovTA profile.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Reports can be generated to show who has access to areas with PII and if those items have been accessed.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☒ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report (SAR) has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
X	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The PII data used in GovTA, is NFC data, provided by the Office of Human Resources Management. All PII information is transferred in a secure fashion. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for any anomalies. To guard against the interception of communication over the Internet, GovTA uses the Transport Layer Security (TLS) protocol which encrypts communications between users' web browsers and the web server. Data that flows between the web server and the database server is secured through encrypted communication.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

_X_ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: The applications are covered by the system of records notice (SORN) COMMERCE/DEPT–1 Attendance, Leave, and Payroll Records of Employees and Certain Other Persons, COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: The retention period for these records is guided by the General Records Schedules (GRS), which are issued by the National Archives and Records Administration (NARA) to provide disposition authorization for records common to several or all agencies of the Federal Government. In accordance with GRS 2.4, item 030, and GRS 2.2, item 010, electronic versions of records scheduled for disposal may be deleted at the expiration of the retention period authorized by the GRS for the equivalent paper copies or when no longer needed, whichever is later.
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Specific individuals can be identified.
X	Quantity of PII	Provide explanation: The PII contained in the various systems is collected from all Commerce Employees.
X	Data Field Sensitivity	Provide explanation: Data collected contains various PII including SSN.
X	Context of Use	Provide explanation: Data is used to collect time and attendance for DOC employees.
X	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act of 1974 (5 USC 552a) and OMB Memorandum provide the obligation to the US Government to protect this information.
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The potential threat to this system is an insider threat. However, contractors are required to take the Annual Cyber Security Awareness Training. They prove they have completed it by signing the certificate that is available electronically online at the end of the course only after successfully completing this course. All users are required to sign the Rules of Behavior, which outline the data protection requirements, prior to being granted access to the application, annually, and whenever the rules have been updated.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: Application and data are stored in the cloud using Amazon Web Services (AWS) GovCloud environment.
	No, the conduct of this PIA does not result in any required technology changes.