Version Number: 01-2020

U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Impact Assessment
for the
Time and Attendance System (TAS)

Reviewed by: Henry J. Holcombe, 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

Lisa Martin for Dr. Jennifer Goode 12/08/2021

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Time and Attendance System (TAS)

Unique Project Identifier: PTOC-045-00

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

The Time and Attendance System (TAS) is an Application information system. The purpose of the TAS is to support the Human Resources business functions within the United States Patent and Trademark Office (USPTO). TAS supports all activities associated with the recruitment and management of USPTO personnel. TAS provides the following capabilities:

- Allows USPTO employees Time and Attendance (T&A) information to be entered, verified, electronically certified and collected for transmission via PTONet, GDC Integration, Inc. (GDCI), and OHRNet to the Department of Agriculture's National Finance Center's (NFC) personnel/payroll system.
- A broad range of data processing and management capabilities including specialized features, capabilities to provide the Office of Security & Safety the ability to track and manage data.
- Rapid dissemination of emergency notifications to targeted USPTO personnel working on campus and/or remotely.

TAS allows the USPTO T&A information to be entered, verified, and electronically certified. The information is then collected for transmission to the NFC's personnel/payroll system in accordance with existing policies and procedures.

TAS provides the following functionality:

- Provide a Web based intranet interface for all USPTO employees
- Allow the automated entry, saving and storing of T&A data on a 24-hour per day/7 days per week availability (except during maintenance)
- Generate and send e-mail messages and task information using USPTO email addresses
- Gather information for the PTO Leave Donor Program

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

(b) System location
TAS is a cloud-based services platform hosted by GDCI.

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

GDC Integration, Inc. (GDCI): GDCI hosts TAS where T&A information may be entered, verified, electronically certified and collected for transmission to the Department of Agriculture's National Finance Center's (NFC) personnel/payroll system.

National Finance Center (NFC): NFC is the Department of Agriculture's personnel/payroll system which receives T&A information from USPTO via GDCI.

Enterprise Data Warehouse (EDW): EDW is a USPTO system providing access to integrated USPTO data through various tools in support of not only reporting and visualizing but also analytics used in decision-making across USPTO.

Network and Security Infrastructure (NSI): The NSI is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.

Enterprise Software Services (ESS): ESS provides Enterprise Directory Services, Role-Based Access Control System, Email as a Service, PTO Exchange Services, Symantec Endpoint Protection, Enterprise SharePoint Services, etc.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
TAS collects and maintains USPTO employee Social Security Numbers (SSNs) to transmit and to process pay. TAS is a T&A application specifically designed to meet the time, attendance and leave reporting requirements as defined by the Office of Personnel Management (OPM) for Federal Departments and/or Agencies, and Federal employees. TAS allows USPTO employees to record, track, validate and certify their T&A. This data is transmitted to our payroll provider to complete payroll and personal transactions. TAS collects and maintains USPTO employee SSNs to process bi-weekly payments for USPTO employees. The system also stores personal leave balances, T&A information and some employee related information.

(e) How information in the system is retrieved by the user
TAS is a web-based automated SaaS used by USPTO employees to gather, validate, process, and manage employee T&A data. TAS is hosted at GDCI's private cloud. Using desktop workstations, employees will access TAS from the USPTO web browsers on the USPTO intranet. The employee's supervisory certifying official will render online approval for the T&A recordings.

(f) How information is transmitted to and from the system
The information is transmitted to and from the TAS system using end-to-end secure transport layer protocols. USPTO will implement IPSec VPN tunnels between USPTO and GDCI that all Time Attendance data will be gone through the IPSec tunnels traffic between USPTO and GDCI sites.

(g) Any information sharing conducted by the system
The information is shared with NFC's automated personnel/payroll processing system.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
The information is collected for the purpose of Federal and Federal contract employment under sections 1302, 3301, 3304, 3328, and 8716 of title 5; Executive Order 9397, as amended; and U.S. Code and Federal Continuity Directive-1 (FCD-1). Section 1104 of title 5 allows OPM to delegate personnel management functions to other Federal agencies.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
The FIPS-199 security impact category identified for TAS system is Moderate.

Section 1: Status of the Information System

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

☒ 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 (version 01-2015).
☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

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*	☒	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: TAS collects and maintains USPTO employee SSNs to process personal leave balances, T&A information, employee information, and position description. The T&A information are shared with NFC for payroll process using SSN for identification. TAS utilizes SSNs to ensure each employee is associated to a unique identifier and allows for accurate processing of payroll transactions.					

General Personal Data (GPD)					
a. Name	☒	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. Physical Characteristics	☐
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	☐	e. Work Email Address	☒	i. Business Associates	☐
b. Job Title	☒	f. Salary	☐	j. Proprietary or Business Information	☐
c. Work Address	☐	g. Work History	☐		
d. Work Telephone Number	☐	h. Employment Performance Ratings or other Performance Information	☐		
k. Other work-related data (specify): work schedule.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☒
b. IP Address	☒	d. 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	☒
Telephone	☐	Email	☐		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☐	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.

USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and as expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. In addition, NSI provides additional automated transmission and monitoring mechanisms to ensure that PII/BII information is protected and not breached by external entities. Information is collected from the users directly and collected data is used for decision making only.

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.
☒	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):			

☒	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):			

☒	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	☒
For administrative matters	☒	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).

TAS collects, maintains, or disseminates PII about DOC employees. The types of information collected, maintained, used or disseminated by the system includes, for example, employee SSNs to process pay using personal leave balances, T&A information & employee information used to maintain the human resources files. The T&A information is shared with NFC for payroll process using SSN as primary identification.

5.2 Describe any potential threats to privacy 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.)

The scope of potential threat to privacy includes internal USPTO employees (insider threats) and GDCI privileged users. GDCI implements security and management controls to prevent the inappropriate disclosure of sensitive information.

USPTO has also identified and evaluated potential threats to PII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility and integrity of information. Users are provided one-on-one, weekly, and monthly training. All users have access restriction or permissions based on the built-in security controls of the system. Furthermore, the system has the ability to password protect any sensitive data for added protection. Data retention is managed automatically using IQ Archivist in accordance with records management retention policy. System access to PII/BII data is limited to a restricted set of users.

Management controls are utilized to prevent the inappropriate disclosure of sensitive information including Annual Security Awareness Training which is mandatory for all TAS users. It includes training modules on understanding privacy responsibilities and procedures and other information such as defining PII and how it should be protected. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the GDCI and expected by users. GDCI implements automatic purging of information, as applicable, by means of deletion and/or shredding. In addition, GDCI provides additional automated transmission and monitoring mechanisms to ensure that PII information is protected and not breached by any other unauthorized entities.

Technical Controls:

- TAS is protected externally and internally using Checkpoint Firewall gateways. The TAS Web Applications are additionally protected using Barracuda Web Application Firewall for web-proxy traffic and routing.
- Sensitive information transmitted to or from any external or internal destination is encrypted by TLS 1.2 or later at the transport layer, or through the use of an encrypted VPN tunnel. Microsoft SQL Server forces encryption on all incoming connections.
- The primary purpose of a Protected Distribution System is to deter or prevent physical access to communication lines carrying national security information. GDCI-TAS does not currently store, process, or transmit national security information. Nevertheless, the network components facilitating communication between the GDCI-TAS information systems are either A) Virtual or B) Contained within a locked network cabinet accessible only to authorized personnel and secured within a hardened data center. Any sensitive

information being transmitted outside of this environment is done so via a secure network protocol such as TLS 1.2 and/or secured via AES-256 file encryption.

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	☒	☒	☒
DOC bureaus	☐	☐	☐
Federal agencies	☐	☒	☐
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?

☐	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.

☒	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: • Enterprise Software Services (ESS) • GDC Integration, Inc. (GDCI) • National Finance Center (NFC) GDCI provides facilities and hardware in support of the TAS services with security features controlled by GDCI at the Infrastructure level. GDCI is responsible for the application delivery layers including: infrastructure (e.g., hardware and software that comprise the infrastructure); and service management process. (e.g., the operation and management of the infrastructure and the system and software engineering lifecycles). USPTO relies on GDCI to manage the cloud infrastructure including the network, data storage, system resources, data centers, security, reliability, and supporting hardware and software.

	The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved an authorized accounts. The USPTO monitors in real-time all activities and events within the servers storing the potential PII data and a subset of USPTO C3 personnel review audit logs received on a regular bases and alert the ISSO and or the appropriate personnel when inappropriate or unusual activity is identified. Access is restricted on a "need to know" basis, and there is utilization of Active Directory security groups to segregate users in accordance with their functions.
☐	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	☒
Contractors	☒		
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.)*

☒	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	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: See Appendix A.	
☐	Yes, notice is provided by other means.	Specify how:
☐	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: Applicants can decline to provide their information during onboarding. However, in doing so, the agency and federal government would not be able to process their payroll.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: Applicants can consent to provide their information during onboarding. However, in doing so, the agency and federal government would not be able to process their payroll.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: USPTO employees have the opportunity to review and update their personal information online through NFC's Employee Personal Page application or the Department of Treasury's HR Connect system. Employees may also visit the USPTO's Office of Human Resources (OHR) department for additional assistance.
☐	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.)*

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (GDCI and USPTO employees) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Unauthorized access, suspicious system log behavior and log failures are audited by GDCI and reported to the appropriate USPTO personnel to troubleshoot and help remediate any potential issues.
☒	The information is secured in accordance with 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.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	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).
☒	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish ownership rights over data including PII/BII.

☒	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).*

In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4, the GDCI-TAS FedRAMP System Security & Privacy Plan (SSPP) addresses the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. GDCI provides facilities and hardware in support of the TAS services with security features controlled by GDCI at the Infrastructure level. GDCI is responsible for the application delivery layers including: infrastructure (e.g., hardware and software that comprise the infrastructure); and service management process. (e.g., the operation and management of the infrastructure and the system and software engineering lifecycles). USPTO relies on GDCI to manage the cloud infrastructure including the network, data storage, system resources, data centers, security, reliability, and supporting hardware and software. All access has role-based restrictions and individuals with access privileges undergo vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The Executive Correspondence Specialist (ECS) must approve access to the system. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. The data is encrypted in transit and at rest. Additionally, TAS is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels.

Section 9: Privacy Act

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

☒	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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: **TAS:** An existing system of records notice covers the information residing in the SaaS Application: COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons.
☐	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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: GRS 2.4- Items 010, 030, 040, 060 and 061
☐	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:
☒	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	☒	Overwriting	☐
Degaussing	☐	Deleting	☒
Other (specify):			

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

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.
☒	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 levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: TAS collects, maintains, or disseminates PII about DOC employees. The types of information collected, maintained, used or disseminated by the system include for

		example, SSNs, name, job title, etc. Alone, or when combined, this large data set uniquely and directly identifies individuals. If the information is inappropriately accessed, used, or disclosed, potential harm could result to the subject individuals and or the organization.
☒	Quantity of PII	Provide explanation: The number of records generated bi-weekly is approimately 13, 000. This time data is sent to NFC. Such large numbers of individual PII would result in a serious or substantial number of individuals affected by loss, theft, or compromise.
☒	Data Field Sensitivity	Provide explanation: The types of identifying numbers such as SSN and employee ID, for example make these data fields alone or in combination directly usable in other contexts and make the individual or organization vulnerable to harms such as identity theft, embarrassment, and loss of trust or cost.
☒	Context of Use	Provide explanation: TAS collects and maintains USPTO employee SSNs to process pay using personal leave balances, T&A information & employee information. Disclosure of the PII itself may result in serious harm to the individual or organization.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected, USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974 and USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. These government-wide privacy laws, regulations and mandates that have been put in place to protect the individual and the organization, lower the PII Confidentiality Impact rating.
☒	Access to and Location of PII	Provide explanation: Access to TAS is only to privileged users. TAS is a FEdRamp approved cloud-based services platform hosted by GDCI. All the recommended NIST controls including Physical and Environmental controls are in place. Access via the web requires passing the GDCI Firewall-DMZ-Firewall-Security Module, Application Authentication and Database.
☐	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 scope of potential threat to privacy includes internal USPTO employees (insider threats) and GDCI privileged users.

Management controls are utilized by GDCI and USPTO to prevent the inappropriate disclosure of sensitive information including Annual Security Awareness Training which is mandatory for all GDCI and USPTO employees. It includes training modules on understanding privacy responsibilities and procedures and other information such as defining PII and how it should be protected.

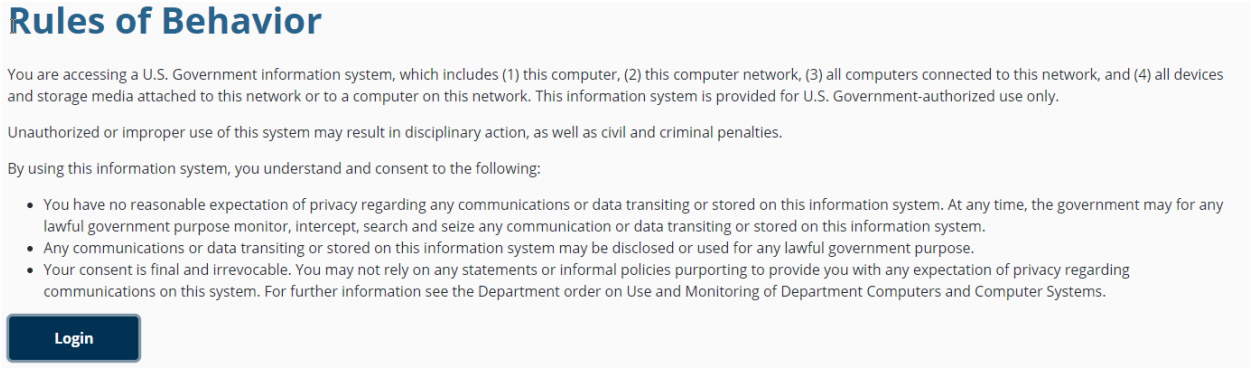
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	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.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.

Appendix A: USPTO Privacy Act Statement



Rules of Behavior

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

- You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system.
- Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.
- Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system. For further information see the Department order on Use and Monitoring of Department Computers and Computer Systems.

Login