Version Number: 01-2020

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

Privacy Threshold Analysis
for the
Time and Attendance System (TAS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Time and Attendance System (TAS)

Unique Project Identifier: PTOC-045-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description system (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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). The TAS supports all activities associated with the recruitment and management of USPTO personnel. The 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, 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 United States Patent and Trademark Office (USPTO) time and attendance 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 GDC Integration Inc.

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 purpose that the system is designed to serve

TAS is a SaaS solution developed by GDCI and it is a Time & Attendance 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.

e) The way the system operates to achieve the purpose

TAS allows USPTO employees to record, track, validate and certify their time and attendance. This data is transmitted to our payroll provider to complete payroll and personal transactions. TAS collects and maintains USPTO employee Social Security numbers to process bi-weekly payments for USPTO employees. The system also stores personal leave balances, time and attendance information, and some employee related information.

f) A general description of the type of information collected, maintained, use, or disseminated by the system

TAS receives personnel data files from the current HRMS HRConnect and Enterprise Data Warehouse (EDW). Additionally, the Program, Project and Activity (PPA) codes are sent to the system via files from EDW.

g) Identify individuals who have access to information on the system

Assigned employees and supervisors who have access to the system for leave requests and completion of time cards. In addition, there are specific roles within OHR that access the solution – timekeeper, master timekeeper, and master supervisor, including contractors.

h) How information in the system is retrieved by the user

TAS is a web-based automated SaaS used by United States Patent and Trademark Office (USPTO) employees to gather, validate, process, and manage employee time and attendance 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 Time and Attendance (TA) recordings.

i) 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.

Questionnaire:

1. What is the status of this information system?

☒ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-	☐	e. New Public Access	☐	h. Internal Flow or	☐

Anonymous				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. *Continue to answer questions and complete certification.*

☐ 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 or 01-2017). *Continue to answer questions and complete certification.*

☐ 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 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☒ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☐ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

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

☒ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☒ DOC employees
- ☐ Contractors working on behalf of DOC
- ☐ Other Federal Government personnel
- ☐ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☒ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
TAS SaaS collects and maintains USPTO employee Social Security Numbers (SSN) to transmit to NFC and process pay for USPTO employees. Personal leave balances, time and attendance (T&A) information & employee information is transmitted to NFC for payroll processing. The T&A related details are transmitted to 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.
Provide the legal authority which permits the collection of SSNs, including truncated form.
PII information is initially collected during the employment application process and is further used by and contained within TAS to process time and attendance data. The Office of Personnel Management (OPM) is authorized to request PII information for the purpose of Federal employment and Federal contract employment under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U.S. Code. Section 1104 of title 5 allows OPM to delegate personnel management functions to other Federal agencies. Executive Order 9397, as amended, also provided authority for the collection of SSNs.

☐ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☒ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☐ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the **Time and Attendance System (TAS)** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the **Time and Attendance System (TAS)** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Colleen Sheehan Office: Office of the Chief Administrative Officer (OCAO) Phone: (571) 272-8246 Email: Colleen.Sheehan@uspto.gov Signature: Users, Sheehan, Colleen Digitally signed by Users, Sheehan, Colleen Date: 2021.09.30 09:13:46 -04'00' Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: DON R Watson Digitally signed by DON R Watson Date: 2021.09.30 11:38:01 -04'00' Date signed: _____
Privacy Act Officer Name: John (Ricou) Heaton Office: Office of General Law (O/GL) Phone: (571) 270-7420 Email: Ricou.Heaton@upsto.gov Signature: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2021.09.29 10:27:13 -04'00' Date signed: _____	**Bureau Chief Privacy Officer and Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Deborah Stephens Digitally signed by Deborah Stephens Date: 2021.09.30 11:51:48 -04'00' Date signed: _____
Co-Authorizing Official Name: Frederick Steckler Office: Office of the Chief Administrative Officer (OCAO) Phone: (571) 272-9600 Email: Frederick.Steckler@uspto.gov Signature: Users, Steckler, Frederick W. Digitally signed by Users, Steckler, Frederick W. Date: 2021.10.20 15:26:27 -04'00' Date signed: _____	