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

Privacy Impact Assessment
for the
Integrative Workplace Management System (IWMS)

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

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.02.16 10:09:40 -05'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Integrative Workplace Management System (IWMS)

Unique Project Identifier: EBPL-PFM-02-00

<u>Introduction</u>: System Description

Provide a brief description of the information system.

Integrative Workplace Management System (IWMS) is a Software-as-a-Service (SaaS) cloud-based system. IWMS leverages International Business Management Corporation (IBM) Maximo & TRIRIGA SAAS (Maximo/IBM TRIRIGA) to provide USPTO with a facilities and space management solution. IWMS utilizes the IBM TRIRIGA SaaS portion of the Cloud Service Provider's (CSP's) product offering.

IBM TRIRIGA features an intuitive interface to provide quick and easy access to key facilities information that USPTO requires to ensure facilities are well managed and utilization is clearly understood to prevent extraneous leasing costs. Through this tool, USPTO employees and contractors can:

- Upload Automated Computer-Aided Design (AutoCAD) drawings of USPTO facilities' floor plans with information such as allocation for offices, hoteling spaces, conference and work rooms;
- Create move scenarios to optimize available space and report on utilization;
- Capture and analyze space utilization in USPTO facilities and report on real-time and planned changes;
- Track lease information and costs;
- Access property information to ensure routine and planned maintenance, capital improvement and lease management needs;
- Maintain archive of AutoCAD floor plans and provide search capabilities;
- Dynamically search for employees' assigned office/work space, if they have one assigned within the USPTO facilities.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
IWMS is a Software-as-a-Service system.

(b) System location
IWMS production environment resides on IBM's primary data hosting facility and federal cloud infrastructure located in Richardson, Texas.

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

Network and Security Infrastructure System (NSI): NSI facilitates the communicates, secure access, protective services, and network infrastructure support for all USPTO systems and applications. IWMS leverages NSI to connect externally via secure connection to the cloud service provider, IBM.

USPTO Enterprise Data Warehouse (EDW): EDW is the subsystem of Information Delivery Product (IDP), provides access to integrated USPTO data to support the decision-making activities of managers and analysts in the USPTO's business areas as needed to achieve business goals. It helps USPTO managers and analysts to answer a variety of strategic and tactical business questions using quantitative enterprise business information. For the purposes of facilities management, EDW's data provides information that allows business users to evaluate space requirements based on telework status, office organization and other considerations such as supervisory requirements. IWMS collects PII from this system.

Enterprise Windows Servers (EWS): EWS is an infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions, such as Microsoft (MS) Mail Relay servers. IWMS will connect to USPTO's MS Mail Relay servers for email notifications.

Identity, Credential, and Access Management Identity as-a-Service (ICAM-IDaaS): ICAMIDaaS provides consolidated access management across applications and API based on single sign-on. Identity and access management is provided by OKTA, a cloud-based solution, which uses Universal Directory to create and manage users and groups**.**

(d) The way the system operates to achieve the purpose(s) identified in Section 4
IWMS collects and transmits Employee PII data, such as Enterprise User ID, federal employee names, and work email, work address, etc. IWMS collects square footage, geographic location data of USPTO facilities.

(e) How information in the system is retrieved by the user
IWMS employs multi-factor authentication via OKTA Single Sign On (SSO) to access the SaaS product, IBM TRIRIGA. OKTA will be integrated with Active Directory (AD) to perform user identifier management. IWMS Administrators use their USPTO Single Sign On (SSO) credentials linked to Security Assertion Mark-up Language (SAML). IWMS users will have roles assigned and will be able to access the data required for their jobs. IPSec tunneling will be utilized for bi-directional communication between the FedRAMP SAAS system and USPTO.

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

IWMS uses a cloud-based application, IBM TRIRIGA, that is hosted by IBM's cloud infrastructure, IBM SoftLayer. The implementation will provide site to site IPSEC/VPN tunneling that USPTO will use for bidirectional communication with IBM TRIRIGA to secure data transfer, email communication, and authentication.

System PII is leveraged from EDW. IWMS only collects Employee ID/User ID, work email, and employee name necessary for proper system functionality to provide general users with space management requests within USPTO facilities.

(g) Any information sharing
IWMS will only share reports internally to better understand and plan USPTO facility usage.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
DAO 217-21 Space Allowance and Management Program
EO 13327 Federal Real Property Asset Management
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
IWMS is categorized as a Moderate system.

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.

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:					

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. 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	□	e. Work Email Address	☒	i. Business Associates	□
b. Job Title	☒	f. Salary	□	j. Proprietary or Business Information	□
c. Work Address	☒	g. Work History	□	k. Procurement/contracting records	□
d. Work Telephone Number	□	h. Employment Performance Ratings or other Performance Information	□		
l. Other work-related data (specify): USPTO employees' assigned office/work space, if they have one assigned within the USPTO facilities					

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	☒	c. Date/Time of Access	☒	e. ID Files Accessed	□
b. IP Address	□	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	□
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): N/A					

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

IWMS is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application. The accuracy of the information is ensured by another system, EDW. Individuals are able to review and update their personal information within EDW; IWMS will then collect data directly from EDW.

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): Click or tap here to enter text.			

☒	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).

The information in this system is about federal employees and contractors and is used for administrative matters.

Administratively, IWMS processes and transmits data, such as Enterprise User ID, federal employee names, and work email, work address, etc. in order to denote the user that is reserving or designing facility space within USPTO's campus. IWMS also collects square footage, geographic location data of USPTO facilities in order for USPTO employees to reserve facility space across USPTO campus. The presence of any of the PII identified in section 2.1 could be from a federal employee/contractor.

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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within IWMS could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through USPTO enterprise system in which IWMS pulls data from, and all personnel who access the data must first authenticate to IWMS at which time an audit trail is generated by the Cloud Service Provider (CSP) SIEM. Logging reports are reviewed by the system Information System Security Officer (ISSO) and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

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. (*add system interconnections)

☒	Yes, this IT system connects with or receives infomation 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: Yes, this IT system connects with or receives infomation 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: IWMS interconnects with the following systems: - EDW - ICAM-IDAAS - NSI - EDW 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 account. The USPTO monitors in real-time all activities and events within the servers storing the potential PII data. Selected USPTO personnel review audit logs received on a regular basis and alert 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: https://www.uspto.gov/privacy-policy	
☐	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:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals do not have the opportunity to decline to provide PII/BII from IWMS, as the information is obtained from EDW.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The PII/BII maintained in this system is required to ensure the integrity of the system.

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:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: The individual can not update their information directly in IWMS because the users' PII is obtained from EDW.

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 (employees and contractors) 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: PII is monitored via audit logs
☒	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.
☒	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 5 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 information system and it has been detemined 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 DOC 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).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST and FedRAMP requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

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). (*review w Privacy)*

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, number, and link. *(list all that apply)*: 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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: GRS 5.1, item 010: Administrative records maintained in any agency office. Temporary. Destroy when business use ceases. GRS 3.2:030, System Access Records (systems not requiring special accountability for access). Temporary. Destroy when business use ceases. GRS 3.2:031, System Access Records (systems requiring special accountability for access). Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
☐	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 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.
□	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.)*

☒	Identifiability	Provide explanation: Employee name within system – Low impact; no other PII/BII.
☒	Quantity of PII	Provide explanation: Five (5) PII data points per person that is a USPTO employee or contractor which would be around 10,000 employees.
☒	Data Field Sensitivity	Provide explanation: System data fields such as user ID, employee name, work email, and employee office location has little relevance outside the context of use.
☒	Context of Use	Provide explanation: IWMS only collects USPTO employee, user work-related info.
☒	Obligation to Protect Confidentiality	Provide explanation: NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 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) and the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: IWMS is a SaaS-based system hosted by the Cloud Service Provider (CSP). PII is not shared externally of USPTO. Active Directory credentials, VPN, and SSO is utilized before the user accesses the system.
□	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 PII in this system poses a low risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the Cloud Service Provider's (CSP) infrastructure and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. The CSP monitors, in real-time, all activities and events within the servers storing the potential PII data and USPTO system personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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.