Version Number: 02-2018

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

Privacy Impact Assessment
for the
Corporate Administrative Office System (CAOS)

Reviewed by: David Chiles, Bureau Chief Privacy Officer (Acting)

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

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce,
ou=Office of the Secretary, cn=CATRINA PURVIS,
0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.09.28 18:32:26 -04'00'

09/07/2018

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Corporate Administrative Office System (CAOS)

Unique Project Identifier: PTOC-005-000

<u>Introduction</u>: System Description

(a) A general description of the information in the system:

The Corporate Administrative Office System (CAOS) is an Application information system. The purpose of the CAOS is to support the Human Resources business functions within the United States Patent and Trademark Office (USPTO). The CAOS is composed of three (3) Automated Information Systems (AISs) that provide the following capabilities:

- Allows USPTO employees' Time and Attendance information to be entered, verified, electronically certified and collected for transmission via PTONet 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.

The CAOS consists of the following three (3) subsystems:

WebTA 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.

WebTA 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

ENS is a network-based emergency notification system which provides rapid dissemination of emergency messages to USPTO personnel. It enables the Office of Security to provide emergency information and instructions agency-wide or to a targeted building and, when beneficial, to receive feedback through responses to the message. Through an audible alert and visual desktop popup text message. It is a rapid and effective means of notifying the entire USPTO community (10,000+ employee workstations) in less than 5 minutes so they may react quickly in an emergency. This includes those working from a remote location (teleworking) as well as those on campus.

- The ENS uses an alert management COTS software to provide a scalable central solution for Network Alerts emergency notification systems.
- It is widely used by several federal agencies including the Department of Defense, US Coast Guard, Department of Energy and Department of Veteran's Affairs.
- The USPTO Office of Security can issue pre-scripted or ad hoc messages from any web browser enabled computer with access to the USPTO network (as well as via VPN).
- Agency ENS administrators can create, manage, and send alerts to any computer using a standard web browser. Alerts can be designated for targeted recipients by specific department or location.
- The Office of Security can track alerts, which are maintained in an audit trail that shows exactly which personnel received and acknowledged each alert.

COOP-WB is a replacement of the existing Continuity of Operations Plan Work Book (COOP-WB) with a more efficient electronic, web-based solution, accessible to other COOP-WB representatives. In addition to being a simpler and less time-consuming method for Business Unit COOP-WB managers and assistants to complete and maintain their portion of the overall USPTO COOP-WB/Plan, the data contained in the work is accessible/retrievable for inclusion in reports that improve the agency's ability to reconstitute following an emergency or disaster.

COOP-WB uses the COTS software from Sustainable Planner, which greatly reduce the amount of time agency continuity personnel spends completing the Business Continuity and Contingency Plan (BCCP) and workbooks and provides reports that are vastly superior to the manual outputs possible from existing documents. USPTO should be able to rapidly generate a list of downstream impacts to/from any pinpointed failure, whether those failures occur in an automated information system or in a particular building. This should provide critical data/information to the agency during a continuity event and could decrease the amount of time to return the agency to full operational status.

RSP is be used by employees to view, through a user interface, their badge in/badge out and log in/log out details. The information that is contained within the Record Sharing Platform system enables a user to verify the information that is being entered into the USPTO webTA time reporting system. RSP is not a system of records.

RSP contains the following key features:

1) Employee View that shows totals and detailed badge in/badge out and log in/log out information,
2) Manager View that allows a manager to query and view employee totals along with detailed badge in/badge out and log in/log out information,
3) Business Administrator View that provides enhanced reporting through expanded selection criteria along with Manager Delegation authority,
4) Manager Delegation View that provides the ability to designate another manager to perform their RSP reporting responsibilities while they are out of the office, and

5) Technical Admin reviews and validates RSP daily refresh services.

(b) A description of a typical transaction conducted on the system:

WebTA: Allows USPTO employees to record, track, validate and certify their time and attendance. Complete payroll and personal transactions including Statements of Earnings and Leave, quick service payments, final salary payments for indebted employees, payments to the estate of a deceased employee, view and print a USPTO employee's W-2, and Wage and Tax Statement data.

COOP-WB: Allows authorized emergency management personnel and COOP Business Unit managers and assistants to input Continuity of Operation information such as business impacts, line of succession, critical IT applications and processes, staff/employee personal information, and more.

ENS: The USPTO Emergency Notification System (ENS) provides rapid dissemination of emergency messages to USPTO personnel and contractors via desktop notifications on and mail messages to USPTO email accounts. Also, ENS provides a "Self Service" facility where users may provide additional mean of contact, such as Cell, Home phone or alternate email which will also receive the alert.

RSP is used by employees to view, through a user interface, their badge in/badge out and log in/log out details.

(c) Any information sharing conducted by the system:

WebTA: The information collected is shared with NFC's automated personnel/payroll processing system.

COOP-WB: The information collected is shared internally among agency emergency management personnel, COOP Business Unit managers/assistants, and USPTO Senior Management.

ENS: The information collected is shared internally among agency emergency management personnel.

RSP: Information hosted or collected by RSP is only accessible to individual user and RSP administrators and is not shared with anyone else within USPTO or outside USPTO.

(d) A citation of the legal authority to collect PII and/or BII:

WebTA: PII information is initially collected during the employment application process and is further used by and contained within WebTA to process time and attendance data. The Office of

Personnel Management (OPM) is authorized to request PII information for the purpose of Federal 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.

COOP-WB: The information collected is provided voluntarily and by manual input from emergency management personnel, COOP Business Unit Managers/assistants, and USPTO Senior Management. This information is collected under Federal Continuity Directive-1 (FCD-1), January 2017. It is necessary to collect such information from essential personnel because their roles and responsibilities align to emergency management duties.

ENS: The information collected is provided voluntarily and by manual input from USPTO employees and contractors, emergency management personnel and USPTO Senior Management. This information is collected under Federal Continuity Directive-1 (FCD-1), January 2017. It enables the Office of Security to provide emergency information and instructions agency-wide or to a targeted building and, when beneficial, to receive feedback through responses to the message.

(e) The Federal Information Processing Standard (FIPS) 199 security impact category for the system

WebTA, COOP-WB, ENS and RSP: The Sub-system security impact category is Moderate.

CAOS: The Master System high water-mark security impact category 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.)*

☒ This is an existing information system in which changes do not create new privacy risks. *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-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):					

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*	☒	e. File/Case ID	☐	i. Credit Card	☐
b. Taxpayer ID	☐	f. Driver's License	☐	j. Financial Account	☒
c. Employer ID	☐	g. Passport	☐	k. Financial Transaction	☐
d. Employee ID	☒	h. Alien Registration	☐	l. Vehicle Identifier	☐
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: WebTA collects and maintains USPTO employee Social Security Numbers (SSN) to process personal leave balances, time and attendance (T&A) information, employee information, and position description. The T&A information are transmitted to NFC for payroll process using SSN from both WebTA and NFC for identification.					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished: No, there is no way to avoid future collection of SSN. WebTA 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	☒	g. Date of Birth	☐	m. Religion	☐
b. Maiden Name	☐	h. Place of Birth	☐	n. Financial Information	☐
c. Alias	☒	i. Home Address	☒	o. Medical Information	☐
d. Gender	☐	j. Telephone Number	☒	p. Military Service	☒

e. Age	□	k. Email Address	☒	q. Physical Characteristics	□
f. Race/Ethnicity	□	l. Education	□	r. Mother’s Maiden Name	□
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	☒	d. Telephone Number	☒	g. Salary	□
b. Job Title	☒	e. Email Address	☒	h. Work History	□
c. Work Address	☒	f. Business Associates	□		
i. Other work-related data (specify):					

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 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			
To determine eligibility	☐	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): **WebTA** collects and maintains USPTO employee Social Security numbers to process, personal leave balances; time and attendance information, employee related information, position description and management information. **COOP-WB**, Individual COOP officers in the various major Offices and Business Units within USPTO supply information and requirements supporting emergency Continuity of Operations for the USPTO. COOP-WB collects the necessary staff/employee resource information such as: names, personal home number, personal cell number, and personal email. **ENS** collects and maintains USPTO employee ID, email ID, work and home phone number, work and home			

address which enables the Office of Security to provide emergency information and instructions agency-wide or to a targeted building and, when beneficial, to receive feedback through responses to the message.

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).

WebTA captures employee Social Security Numbers in order to collect, validate, and electronically certify time and attendance information. This information is further collected for secure transmission over the USPTO network to the National Finance Center (NFC) for payroll processing. WebTA collects only USPTO employee information.

The COOP-WB information is to be used only in reporting to the COOP Manager and USPTO Senior Management, and creation of the overall USPTO COOP Workbook. COOP-WB collected information is used to support emergency Continuity of Operations for the USPTO. Both USPTO employee and contractor information is collected from those personnel with emergency Continuity of Operations responsibilities.

ENS collected information enables the Office of Security to provide emergency information and instructions agency-wide or to a targeted building and, when beneficial, to receive feedback through responses to the message. Both USPTO employee and contractor information is originally collected from those personnel at the time of onboarding.

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 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: **WebTA** interconnects with the Department of Agriculture's National Finance Center (NFC) for payroll processing. All data transmissions require credential verification and validation of data prior to transmitting. The data passes through a dedicated interconnection (IPSec VPN tunnel) established with NFC. **COOP-WB** information will be shared internally to the COOP Office and with USPTO Senior Management (via reports and the overall Workbook). COO-WB information is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) system. **ENS** information will be shared internally to the agency emergency management personnel and with USPTO Senior Management. ENS information is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) system.
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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: **CAOS:** https://www.opm.gov/forms/pdf_fill/of0306.pdf and USPTO's internal IT Privacy Policy (*for business use only*).	
☐	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: CAOS: PII data is collected as part of the employment process through OMB Form 3206-0182. Applicants can decline to provide their information, however, in doing so, the agency and federal government would not be able to process their employment application.
☐	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: CAOS: PII data is collected as part of the employment process through OMB Form 3206-0182. General or routine uses of the information collected is disclosed in the Form. Applicants can decline to provide their information, however, in doing so, the agency and federal government would not be able to process their employment application.
☐	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: CAOS: 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 (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:
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 9/03/2017 ☐ 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 (POAM).
☒	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.

In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4, the CAOS System Security Plan (SSP) 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. The SSP is reviewed on an annual basis. In addition, annual assessments and Continuous Monitoring reviews are conducted on the CAOS data. The USPTO Office of Policy and Governance/Cybersecurity Division (OPG/CD) conducts these assessments and reviews based on NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations. The results of these assessments and reviews are documented in the CAOS Security Assessment Package as part of the system's Security Authorization process.

Management Controls

1. USPTO uses the Life Cycle review process to ensure that management controls are in place for CAOS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security Plan. The System Security Plan specifically addresses the management, operational, and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff. Additionally, USPTO develops privacy and PII-related policies and procedures to ensure safe handling, storing, and processing of sensitive data.

Operational Controls

1. Automated operational controls include securing all hardware associated with the CAOS in the USPTO Data Center. The Data Center is controlled by access card entry, and is manned

by a uniformed guard service to restrict access to the servers, their Operating Systems and databases. Contingency planning has been prepared for the data. Backups are performed on the processing databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database UserID; (4) Restricted data display, as required; and (5) Restricted access.

2. Manual procedures shall be followed for handling extracted data containing sensitive PII, which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

a. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
b. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.
c. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
d. Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private Network (VPN).
e. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

Technical Controls

1. CAOS 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. Web communications leverages modern encryption technology such as TLS 1.1/1.2 over HTTPS. Dedicated interconnections offer protection through IPSec VPN tunnels.

Section 9: Privacy Act

9.1 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)*:

	Records contained in these systems do not constitute a new system of records within the meaning of the Privacy Act. The following are existing SORNs: **CAOS:** An existing system of records notice covers the information residing in the database: *COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.* **COOP:** An existing system of records notice covers the information residing in the database.: *COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.* **WebTA**: An existing system of records notice covers the information residing in the database.: *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, a SORN is not being created.

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: USPTO Office of the Chief Administrative Officer Comprehensive Records Schedule 2018: http://ptoweb.uspto.gov/ptointranet/cisd/cio/records_mgmt/docs/Section%208-%20Office%20of%20the%20Chief%20Administrative%20Officer.pdf
☐	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): PII collected by COOP-WB and ENS is disposed when it is no longer valid using above mentioned methods. The PII collected by WebTA is not disposed.			

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.

☐	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: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☒	Quantity of PII	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☒	Data Field Sensitivity	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☒	Context of Use	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☒	Obligation to Protect Confidentiality	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☒	Access to and Location of PII	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
☐	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.