

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



**Privacy Impact Assessment  
for the  
MicroPact Background Investigation Tracking System / Employee  
Relations & Labor Relations System (BITS/ERLR)**

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

**CATRINA PURVIS**

Digitally signed by CATRINA PURVIS  
Date: 2020.08.31 13:20:41 -04'00'

05/17/2020

---

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

Date

## U.S. Department of Commerce Privacy Impact Assessment USPTO BITS/ERLR

**Unique Project Identifier: [2396] PTOC-009-00**

### **Introduction: System Description**

- a) *Whether it is a general support system, major application, or other type of system*  
BITS/ERLR is a major application system.
- b) *System location*  
BITS/ERLR system is located at 44470 Chilum Place Bldg 1, Ashburn, VA 20147.  
BITS/ERLR has an alternate hot site located at data center located at 180 Peachtree Street, Atlanta, GA at an Equinox Atlanta Data Center.
- c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*  
The BITS/ERLR applications are hosted by the MicroPact SaaS. NSI and ESS – RBAC facilitates the communication between USPTO and MicroPact
- d) *The way the system operates to achieve the purpose(s) identified in Section 4*  
BITS USPTO adjudicators, who are contractor and employee specialists, access the application through a web-based portal to create, update, track and monitor the status of personnel background investigations. Access to the web portal is restricted to USPTO personnel within the intranet and received authorization.  
ERLR administrators, managers, specialists and employees are able to access the application through a web-based portal to input case data, events and dates. Manage the sharing of records and documents between assigned staff and internal organizations using business rule workflow. Access to the web portal is restricted to USPTO personnel within the intranet and who have received authorization.
- e) *How information in the system is retrieved by the user*  
USPTO OHR staff access the system via the USPTO intranet and web-based portal. Users are able to retrieve and transmit information from the systems after authenticating.
- f) *How information is transmitted to and from the system*  
Users access the BITS and ERLR systems via the USPTO intranet and a web-based portal hosted by the MicroPact SaaS. The transmission of information is facilitated by an encrypted communication between USPTO and MicroPact.
- g) *Any information sharing conducted by the system*  
Information is shared within the bureau based on business need and requests. Information is shared with supporting federal agencies and DOC when requested.
- h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*  
Executive Orders 10450, 13526; 5 U.S.C. 301 and 7531–7533; 15 U.S.C. 1501 et seq.; 28 U.S.C. 533–535; 44 U.S.C. 3101; Executive Orders 9397, as amended by 13478, 10450, 10577, 10865, 12968, and 13470; Section 2, Civil Service Act of 1883; Public Laws 82–298 and 92–261; Title 5, U.S.C., sections 1303, 1304, 3301, 7301, and 9101; Title 22, U.S.C., section 2519; Title 42 U.S.C. sections 1874(b)(3), 2165, and 2201; Title 50 U.S.C. section 435b(e); Title 51, U.S.C., section 20132; Title 5 CFR sections 731, 732 and 736; Homeland

Security Presidential Directive 12 (HSPD 12), OMB Circular No. A-130; E.O. 12107; E.O. 13164; 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987.

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

The FIPS 199 security impact category for the 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.)

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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.

### **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.)

<b>Identifying Numbers (IN)</b>					
a. Social Security*	<input checked="" type="checkbox"/>	e. File/Case ID	<input checked="" type="checkbox"/>	i. Credit Card	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: At this time, there is no way for avoiding the collection and processing of SSNs by the system. This info is necessary for the system users to conduct the background investigation tracking.					

### **General Personal Data (GPD)**

a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input checked="" type="checkbox"/>	m. Religion	<input type="checkbox"/>
b. Maiden Name	<input checked="" type="checkbox"/>	h. Place of Birth	<input checked="" type="checkbox"/>	n. Financial Information	<input type="checkbox"/>
c. Alias	<input checked="" type="checkbox"/>	i. Home Address	<input type="checkbox"/>	o. Medical Information	<input type="checkbox"/>
d. Gender	<input checked="" type="checkbox"/>	j. Telephone Number	<input type="checkbox"/>	p. Military Service	<input type="checkbox"/>
e. Age	<input checked="" type="checkbox"/>	k. Email Address	<input checked="" type="checkbox"/>	q. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input checked="" type="checkbox"/>	l. Education	<input type="checkbox"/>	r. Mother's Maiden Name	<input type="checkbox"/>
s. Other general personal data (specify):					

<b>Work-Related Data (WRD)</b>					
a. Occupation	<input checked="" type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>	g. Salary	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input checked="" type="checkbox"/>	h. Work History	<input type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input type="checkbox"/>		
i. Other work-related data (specify):					

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

<b>System Administration/Audit Data (SAAD)</b>					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input checked="" type="checkbox"/>
g. Other system administration/audit data (specify): Account logon events, Account management, Directory Service Access, Logon Events, Object Access, Policy Change, Privileged Use, Process Tracking, System Events					

<b>Other Information (specify)</b>					

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

<b>Directly from Individual about Whom the Information Pertains</b>					
In Person	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input checked="" type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify):					

<b>Government Sources</b>					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input checked="" type="checkbox"/>	Other Federal Agencies	<input checked="" type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources			
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>
Third Party Website or Application	<input type="checkbox"/>		
Other (specify):			

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

USPTO OHR admin's/specialists have the ability to modify user information and work with employees, contractors and volunteers to validate the accuracy of the information. The data is stored within a database and data is backed-up continually.
--

2.4 Is the information covered by the Paperwork Reduction Act?

<input checked="" type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. #3206-0005 and #3206-0261
<input type="checkbox"/>	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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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.)

<b>Purpose</b>			
To determine eligibility	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input checked="" type="checkbox"/>	For criminal law enforcement activities	<input checked="" type="checkbox"/>
For civil enforcement activities	<input checked="" type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	
For web measurement and customization technologies (single-session )	<input type="checkbox"/>	For web measurement and customization technologies (multi-session )	<input type="checkbox"/>
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).

For BITS - The U.S. Patent & Trademark Office (USPTO) must ensure that only trustworthy individuals are hired to work in national security or public trust positions. The primary means for determining whether an individual is trustworthy is the background investigation, authorized by Executive Order 10450 and 5 C.F.R. Parts 731, 732, and 736. Periodic investigations are conducted at least once every 5 years on individuals who occupy Public Trust Positions as well as those individuals who have access to classified (national security positions). The background investigation is not an evaluation of the subject's character, but is instead a determination of the likelihood that a particular person will adhere to all security requirements in the future. In addition, Homeland Security Presidential Directive 12 (hereinafter HSPD-12) requires a standardized form of official identification for both government employees and contractors. The directive establishes minimum government-wide background investigation requirements for entry on duty and states that official identification cards should be issued only to those individuals with certain pre-employment background checks completed and that the validity of these checks must be updated or verified every five (5) years for employees and contractors. The HSPD-12 directive will expand the USPTO's oversight responsibilities to include monitoring identification card recertification for all employees and contractors, and checking hiring practices for contractors who are investigated and hired locally.

For ERLR - The information will be used to document, track and manage the flow of ER and LR cases more efficiently. Both organizations will use the same system, and they will be able to control the sharing of records and documents among them in accordance with the business rules defined in relevant workflows. The system will automatically generate template letters, and reports for upcoming events, and reports can be shared between ER to LR as approved by the relevant Human Resource (HR) business area or Human Resource Senior Management. The systems pull PII from the database to automatically generate these files and reports.

- 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.)

Nation states are the predominant threat to the systems privacy and data leakage. USPTO has implemented NIST security controls (encryption, access control, auditing) and selected a FedRAMP authorized cloud provider to reduce the risk. Mandatory IT Awareness and role-based training are required for staff that have access to the system and address how to handle, retain and dispose of data. Contract terms between the cloud provider and USPTO provide guidance on how data should be handled, retained and disposed.

## **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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.

<input checked="" type="checkbox"/>	<p>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:</p> <p>The BITS system is connected with OPM/NBIB.</p> <p>For ERLR - HR data is resident within the National Finance Center (NFC). NFC data is fed to the USPTO's Enterprise Data Warehouse. – USPTO System administrators then upload a flat file from the Enterprise Data Warehouse into the Employee Relations / Labor Relations system. There is no direct connection between the two systems – it requires human intervention to upload this data.</p> <p>Encryption and access controls are used to prevent PII/BII leakage.</p>
<input type="checkbox"/>	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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
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.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	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: <a href="https://www.uspto.gov/privacy-policy">https:// www.uspto.gov/privacy-policy</a>	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: BITS: All information requested is provided on a voluntary basis. USPTO as part of the U.S Government is authorized to ask for this information under Executive Orders 10450 and 10577. As such the information is required in order to conduct
-------------------------------------	---	---

		adequate background investigation to be considered for employment with the USPTO. Declining to provide the information would result in not being considered for employment.
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: ERLR: PII that is processed or stored by ERLR is pulled from internal USPTO personnel records. This information is needed for case management, and individuals cannot decline having this information input in to the system.

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

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: BITS: All information requested is provided on a voluntary basis. USPTO as part of the U.S Government is authorized to ask for this information under Executive Orders 10450 and 10577. Social Security Number (SSN) is needed in order to keep records accurate, because other people may have the same name and birth date. The executive Order 9397 also asks Federal Agencies to use SSN to help identify individuals in agency records. The information is required in order to conduct adequate background investigation to be considered for employment with the USPTO.  ERLR: PII processed or stored by ERLR is pulled from internal USPTO personnel records and individuals cannot consent to a particular use within ERLR.

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

<input type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For BITS - Individuals do not have access to review their PII. They can however, reach out to the security office to review to update any PII/BII information.  For ERLR - Employees cannot view or update information.

**Section 8: Administrative and Technological Controls**

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

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Application, System and Security logs are used to track and record access to PII/BII.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 5/23/2019 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	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).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	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).*

Automated operational controls include securing all hardware associated with BITS/ERLR in the MicroPact Data Center. The Data Center is controlled by access card entry and all use of the card is audited through the access system to restrict access to the servers, their Operating Systems and databases. In addition, physical access points to the MicroPact Data Center are controlled by physical locking mechanisms including separate door locks, an alarm control contact monitored twenty-four (24) hours a day by ADT, a motion detector at each door and hallway and a video camera at each hallway.

Contingency planning has been prepared for the data. Backups are performed on the processing databases. All backup tapes that contain PII or information covered under the Privacy Act are encrypted with FIPS 140-2 compliant algorithms by the MicroPact Database Administration Team.

Technical controls: Information is also secured through the application itself, by only allowing authorized users access to the application and to data to which they have access and privilege. Also the information system controls attacks and unauthorized attempts on the application and database through strict logins, AV protection, and through firewalls.

--

## **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 <i>(list all that apply)</i> :
<input checked="" type="checkbox"/>	COMMERCE/PAT-TM-24: Background Investigations Employees Personnel Files not covered by Notices of Other Agencies – COMMERCE/DEPT-18. OPM Central 9 – Personnel Investigations Records OPM/GOVT – 3 – Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	BITS: Personnel Security Investigative Reports (GRS 5.6, 170) Personnel Security and Access Clearance Records (GRS 5.6, 180-181) Index to the Personnel Security Case Files (GRS 5.6, 190)
<input checked="" type="checkbox"/>	ERLR: NARA GRS Schedule 2.3: Employee Relations Records, Item 060, Administrative Grievances, Disciplinary, and Adverse Action Files; Item 050, Labor Management Relations Agreement Negotiations Records.
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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.)*

<b>Disposal</b>			
Shredding	<input checked="" type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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 as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Name, SSN, DOB, POB
<input type="checkbox"/>	Quantity of PII	Provide explanation:
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The presence of employee SSNs, DOB, POB, and Name in the BITS system alone are sensitive PII, and in combination, could result in potential harm to individuals if not used in accordance with their intended use. For ERLR - Use of PII and work / system audit data in combination for tracking and reporting of employee and labor relations cases.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: The BITS acts as an electronic personnel security folder for each person, tracking data related, but not limited to, investigations, clearances and adjudications. For ERLR, because the information containing PII must be transmitted outside of the USPTO environment, there is an added

		need to ensure the confidentiality of information during transmission.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: Based on the data fields input in to the BITS system, USPTO must protect the PII of each individual in accordance with the Privacy Act of 1974.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Because the information containing PII must be transmitted outside of the USPTO environment there is an added need to ensure the confidentiality of information during transmission.
<input type="checkbox"/>	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.)

Nation states and adversarial entities are the predominant threats to the information collected and its privacy. Security controls following FedRAMP and NIST guidance were implemented to deter and prevent threats to privacy.

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

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.