

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



**Privacy Impact Assessment  
for the  
MicroPact Background Investigation Tracking System (BITS)**

Reviewed by: John B. Owens II, 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 D. Purvis**

Digitally signed by Katrina D. Purvis  
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open  
Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US  
Date: 2017.05.05 17:35:09 -04'00'

---

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

Date

## U.S. Department of Commerce Privacy Impact Assessment USPTO MicroPact Background Investigation Tracking System (BITS)

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

### **Introduction: System Description**

*(a) a general description of the information in the system*

The MicroPact Background Investigation and Tracking system (BITS) suite of Web-based applications. MicroPact provides a fully managed support infrastructure service including: supporting hardware and software, secure computing facilities, Internet gateway communications security, system administration, and system and application security services.

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

BITS is an Application information system, and provides a personnel background investigation security tracking system for the USPTO. The system tracks a number of candidate types (employees, contractors, volunteers etc.) and their current personnel security details. The BITS acts as an electronic personnel security folder for each person, tracking data related, but not limited to, investigations, clearances and adjudications.

*(c) any information sharing conducted by the system*

The information will primarily stay within the USPTO Office of Security and Safety and is shared with properly credentialed background investigators who are conducting the background investigation and employees from the OHR's Employee Relations Division who conduct suitability adjudication on USPTO employees. It will also be shared with other federal agency security offices that require the 'passing' of USPTO background investigative data for USPTO personnel visiting or attending meetings, conferences, and/or briefings at other federal agencies.

*(d) a citation of the legal authority to collect PII and/or BII*

The system of records has been created under the Privacy Act, 5 U.S.C 522a and is published as "COMMERCE/PAT-TM-24: Background Investigations". According to the system or records notice, the legal authorities for collecting the PII and/or BII that are collected by USPTO and subsequently processed in the MicroPact BITS system are: *Executive Orders 10450, 11478, 12065; 5 U.S.C. 301 and 7531-7533; 15U.S.C. 1501 et seq.; 28 U.S.C. 533-535; 44 U.S.C. 3101; and Equal Employment Act of 1972. 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, 2201, and 2455; Title 50 U.S.C. section 435b(e); Title 5 CFR sections 731, 732 and 736; Homeland Security Presidential Directive 12 (HSPD 12) and OMB Circular No. A-130.*

*(e) the Federal Information Processing Standard (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.)*
- 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	<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):					

**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*	<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): Last, First and Middle initial, DOB, POB, Dual Citizenship, Position Title, Position Designation, Employee/Contractor, Name of Contracting Co., if applicable, type of background investigation (BI), status of BI, BI Case Number, OPM Issue Code and adjudicative determination					
Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: The system tracks a number of candidate types (employees, contractors, volunteers etc.) and their current personnel security details. The BITS acts as an electronic personnel security folder for each person, tracking data related, but not limited to, investigations, clearances and adjudications.					
*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: At this time, there is no way for avoiding the collection and processing of SSNs by the system. This IN 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 type="checkbox"/>	j. Telephone Number	<input type="checkbox"/>	p. Military Service	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	k. Email Address	<input type="checkbox"/>	q. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input 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 type="checkbox"/>	g. Salary	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input type="checkbox"/>	h. Work History	<input type="checkbox"/>
c. Work Address	<input 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 type="checkbox"/>	c. Date/Time of Access	<input type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input type="checkbox"/>	d. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

<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 type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

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

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

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

<b>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</b>			
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.)*

<b>Activities</b>			
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 type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
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).

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. To ensure 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.

**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"/>

<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 type="checkbox"/>	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:
<input checked="" 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 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: _____.	
<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 type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an	Specify why not: All information requested is provided on a

	opportunity to decline to provide PII/BII.	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.
--	--	--

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: 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. As such the information is required in order to conduct adequate background investigation to be considered for employment with the USPTO.

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: Individuals do not have access to review their PII information. They can however, reach out to the security office to review to update any PII/BII 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:
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>May 23, 2016</u> <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 (POAM).
<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.

Automated operational controls include securing all hardware associated with BITS 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 is controlled by physical locking mechanism 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.”

<input checked="" type="checkbox"/>	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> ):  “COMMERCE/PAT-TM-24: Background Investigations”
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .

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

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: Personnel Security Clearance Files (GRS 18, 22a-b) Personnel Security Clearance Status Files (GRS 18, 23)
<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 type="checkbox"/>
Degaussing	<input checked="" type="checkbox"/>	Deleting	<input 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.

<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.
<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.
<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 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.

12.2 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.