

[Component Name]

Component Seal

Privacy Impact Assessment
for the
[System Name]

Issued by:

[Senior Component Official for Privacy (if designated, otherwise the component privacy point of contact)]

Reviewed by: Luke J. McCormack, Chief Information Officer, Department of Justice

Approved by: Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [Component to insert date of PIA approval]

(September 2012 DOJ PIA Form)

THIS PAGE IS FOR INTERNAL ROUTING PURPOSES AND DOCUMENTATION OF APPROVALS. UPON FINAL APPROVAL, COMPONENTS SHOULD REMOVE THIS PAGE PRIOR TO PUBLICATION OF THE PIA

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) posted at <http://www.justice.gov/opcl/pia.htm>.]

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

- (a) the purpose that the records and/or system are designed to serve;
- (b) the way the system operates to achieve the purpose(s);
- (c) the type of information collected, maintained, used, or disseminated by the system;
- (d) who has access to information in the system;
- (e) how information in the system is retrieved by the user;
- (f) how information is transmitted to and from the system;
- (g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
- (h) whether it is a general support system, major application, or other type of system.

The response should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

[]

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers											
Social Security				Alien Registration				Financial account			
Taxpayer ID				Driver's license				Financial transaction			

Identifying numbers					
Employee ID			Passport		
File/case ID			Credit card		
Other identifying numbers (specify):					

General personal data					
Name			Date of birth		
Maiden name			Place of birth		
Alias			Home address		
Gender			Telephone number		
Age			Email address		
Race/ethnicity			Education		
Other general personal data (specify):					

Work-related data					
Occupation			Telephone number		
Job title			Email address		
Work address			Business associates		
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints			Photos		
Palm prints			Scars, marks, tattoos		
Voice recording/signatures			Vascular scan		
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID			Date/time of access		
IP address			Queries run		
Other system/audit data (specify):					

Other information (specify)					

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person	<input type="checkbox"/>	Hard copy: mail/fax	<input type="checkbox"/>	Online	<input type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):	<input type="checkbox"/>				

Government sources					
Within the Component	<input type="checkbox"/>	Other DOJ components	<input type="checkbox"/>	Other federal entities	<input type="checkbox"/>
State, local, tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):	<input type="checkbox"/>				

Non-government sources					
Members of the public	<input type="checkbox"/>	Public media, internet	<input type="checkbox"/>	Private sector	<input type="checkbox"/>
Commercial data brokers	<input type="checkbox"/>				
Other (specify):	<input type="checkbox"/>				

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please 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. Please describe the choices that the component 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.)

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose

<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>	For civil enforcement activities
<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>	For administrative matters
<input type="checkbox"/>	To conduct analysis concerning subjects of investigative or other interest	<input type="checkbox"/>	To promote information sharing initiatives
<input type="checkbox"/>	To conduct analysis to identify previously unknown areas of note, concern, or pattern.	<input type="checkbox"/>	For administering human resources programs
<input type="checkbox"/>	For litigation		
<input type="checkbox"/>	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority	Citation/Reference
<input type="checkbox"/> Statute	
<input type="checkbox"/> Executive Order	
<input type="checkbox"/> Federal Regulation	
<input type="checkbox"/> Memorandum of Understanding/agreement	
<input type="checkbox"/> Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component 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.)

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component				
DOJ components				
Federal entities				
State, local, tribal gov't entities				
Public				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

<input type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.		
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:	
<input type="checkbox"/>	No, notice is not provided.	Specify why not:	

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

<input type="checkbox"/>	Yes, individuals have the opportunity to decline to provide information.	Specify how:	
<input type="checkbox"/>	No, individuals do not have the opportunity to decline to provide information.	Specify why not:	

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:	
<input type="checkbox"/>	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not:	

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

| |

Section 6: Information Security

6.1 Indicate all that apply.

		The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation:
		If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
		A security risk assessment has been conducted.
		Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify:
		Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:
		Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information:
		Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.
		Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.
		The following training is required for authorized users to access or receive information in the system:
		General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
		Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

| |

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

		Yes, and this system is covered by an existing system of records notice.
		Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system:

	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

| |