

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

**Confidentiality:**  Low  Moderate  High  Undefined

**Integrity:**  Low  Moderate  High  Undefined

**Availability:**  Low  Moderate  High  Undefined

Not applicable – this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

NO

YES **If yes, please provide the date and name or title of the OMB submission:**

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

NO

YES **If yes, please describe the data mining function:**

12. Is this a national security system (as determined by the SecD)?

NO  YES

13. Status of System/ Project:

This is a new system/ project in development. [If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

## II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? MP2 Is a COTS database

b7E

2. Has the system/project undergone any significant changes since April 17, 2003?

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

NO [If no, proceed to next question (II.3).]

YES If yes, indicate which of the following changes were involved (**mark all changes that apply, and provide brief explanation for each marked change**):

A conversion from paper-based records to an electronic system.

A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

A change that results in information in identifiable form being merged, centralized, or matched with other databases.

A new method of authenticating the use of and access to information in identifiable form by members of the public.

A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

A change that results in a new use or disclosure of information in identifiable form.

A change that results in new items of information in identifiable form being added into the system/project.

Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project. The system will be rehosted on VIDAR, a hosting environment for collaborative tools and applications.

Other [**Provide brief explanation**]:

3. Does a PIA for this system/project already exist?

NO  YES

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

NO  YES

[The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1272295-0

Total Deleted Page(s) = 1  
Page 4 ~ b3; b7E;

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(OGC/PCLU Rev. 08/16/2010)

### FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

b3  
b7E

BIKR FBI Unique Asset ID: 2009-047-01-P-115-045-3411

<b>SYSTEM/PROJECT POC</b> Name: Theresa Fretz Program Office: ITB Division: ITSD Phone: 202-324-8447 Room Number: 8977	<b>ALTERNATE POC</b> Name: <input type="text"/> Program Office: CID Division: CID Phone: <input type="text"/> Room Number: 3320	<b>FBI OGC/PCLU POC</b> Name: <input type="text"/> Phone: <input type="text"/> Room Number: JEH, Rm 7350
---	--	---

b6  
b7C

### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Criminal Investigative Division	Signature: <input type="text"/> Date signed: 7/15/11 Name: <input type="text"/> Title: Unit Chief	Signature: <input type="text"/> Date signed: 8/3/11 Name: <input type="text"/> Title: Special Assistant to the Assistant Director
FBIHQ Division: Criminal Investigative Division	Signature: <input type="text"/> Date signed: 8/22/11 Name: <input type="text"/> Title: Assistant Section Chief	Signature: <input type="text"/> Date signed: 8/3/11 Name: <input type="text"/> Title: Special Assistant to the Assistant Director

b6  
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).  
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

**FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:**

PIA is required by the E-Government Act.

PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)?  Yes.  No:

PIA is not required for the following reason(s):

System does not collect, maintain, or disseminate PII.

System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).

Information in the system relates to internal government operations.

System has been previously assessed under an evaluation similar to a PIA.

No significant privacy issues (or privacy issues are unchanged).

Other: This PIA is exceptionally granular in order to provide information and analysis similar to a PIA, which would normally have been conducted if the information in this system was true/accurate, and not solely for backstopping purposes.

Applicable SORN(s): Central Records System, FBI-002

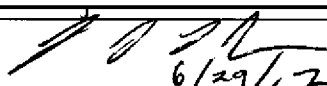
Notify FBI RMD/RIDS per MIOG 190.2.3?  No  Yes--See sample EC on PCLU intranet website here:  
[http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form\\_for\\_miog190-2-3\\_ec.wpd](http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd)

SORN/SORN revision(s) required?  No  Yes :

Prepare/revise/add Privacy Act (e)(3) statements for related forms?  No  Yes :

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

<input type="checkbox"/>	Signature: <input type="checkbox"/>	6/29/12
Privacy and Civil Liberties Unit	Date Signed:	
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: 	6/29/12
	Date Signed:	

b6  
b7c

**I. INFORMATION ABOUT THE SYSTEM / PROJECT**

**1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.**

b3  
b7E

2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

NO

YES [If yes, please continue.]



3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.  
(Check all that apply.)

- The information directly identifies specific individuals.
- The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.
- The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

**If you marked any of the above, proceed to Question 4.**

None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

- NO
- YES The system is designed to pertain predominately to government employees, contractors, or consultants. It would be a very rare instance that it would contain information relating to Confidential Human Sources.

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

- NO. [If no, skip to question 7.]
- YES. [If yes, proceed to the next question.]

6. Does the system/project collect any information directly from the person who is the subject of the information?

- NO [If no, proceed to question 7.]

YES

--

b3  
b7E

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

NO

YES [If yes, proceed to question 7.]

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

NO [The program will need to work with PCLU to develop/implement the necessary form(s).]

YES Identify any forms, paper or electronic, used to request such information from the information subject:

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

NO  YES If yes, check all that apply:

SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

SSNs are necessary to identify FBI personnel in this internal administrative system.

SSNs are important for other reasons. Describe:

The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). Describe: SSNs are masked so that only the last four digits are displayed to the general users. The only personnel with the ability to view the full SSNs are a limited number of administrators.

It is not feasible for the system/project to provide special protection to SSNs. Explain:

8. Is the system operated by a contractor?

No.

Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

     NO    **If no, indicate reason; if C&A is pending, provide anticipated completion date.**

  X   YES    **If yes, please indicate the following, if known:**

**Provide date of last C&A certification/re-certification:**

b3  
b7E

**Confidentiality:**    Low    Moderate   X   High    Undefined

**Integrity:**           Low    Moderate   X   High    Undefined

**Availability:**       Low    Moderate   X   High    Undefined

     Not applicable – this system is only paper-based.

10. Is this system/project the subject of an OMB-300 budget submission?

  X   NO

     YES    **If yes, please provide the date and name or title of the OMB submission:**

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

  X   NO

     YES    **If yes, please describe the data mining function:**

12. Is this a national security system (as determined by the SecD)?

NO  YES

13. Status of System/ Project:

This is a new system/ project in development.

## II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

NO [If no, proceed to next question (II.3).]

YES If yes, indicate which of the following changes were involved (**mark all changes that apply, and provide brief explanation for each marked change**):

A conversion from paper-based records to an electronic system.

A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

A change that results in information in identifiable form being merged, centralized, or matched with other databases.

A new method of authenticating the use of and access to information in identifiable form by members of the public.

A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

A change that results in a new use or disclosure of information in identifiable form.

A change that results in new items of information in identifiable form being added into the system/project.

\_\_\_\_\_ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

\_\_\_\_\_ Other **[Provide brief explanation]:**

3. Does a PIA for this system/project already exist?

\_\_\_\_\_ NO    \_\_\_\_\_ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

\_\_\_ NO    \_\_\_ YES

### FBI PRIVACY THRESHOLD ANALYSIS (PTA)

**NAME OF SYSTEM / PROJECT:** The National Crime Information Center (NCIC) National Instant Criminal Background Check System (NICS) Denied Transaction File (DTF)

**BIKR FBI Unique Asset ID:** \_\_\_\_\_

Derived From: Classified By: Reason: Declassify On:	<b>SYSTEM/PROJECT POC</b> Name: [Redacted] Program Office: LES Section/NCIC Operations and Policy Unit Division: CJS Phone: [Redacted] Room Number: D3-716	<b>FBI OGC/PCLU POC</b> Name: [Redacted] Phone: [Redacted] Room Number: C3-655
--	--	---

b6  
b7C

### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: <i>[Signature]</i> Date signed: <i>11/11/14</i> Name: Michelle S. Klimt Title: Chief, LES Section	Signature: [Redacted] Date signed: <i>9/21/14</i> Name: [Redacted] Title: Supervisory Security Specialist
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6  
b7C

**FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:**

PIA is required by the E-Government Act. *PIA will be done for all recent NCIC changes & this will be included.*

PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)?  Yes.  No

PIA is not required for the following reason(s):

- System does not collect, maintain, or disseminate PII.
- System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- Information in the system relates to internal government operations.
- System has been previously assessed under an evaluation similar to a PIA.
- No significant privacy issues (or privacy issues are unchanged).
- Other:

Applicable SORN(s): NCIC and NICS SORNs

Notify FBI RMD/RIDS per MIOG 190.2.3?  No  Yes--See sample EC on PCLU intranet website here: [http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form\\_for\\_miog190-2-3\\_ec.wpd](http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd)

SORN/SORN revision(s) required?  No  Yes

Prepare/revise/add Privacy Act (e)(3) statements for related forms?  No  Yes:

*If necessary -*

**RECORDS.** The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

Elizabeth Withnell, Unit Chief Privacy and Civil Liberties Unit	Signature: Date Signed:
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: <i>Elizabeth Withnell</i> Date Signed: <i>9/27/12</i>

## I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: (a) name of the system/project, including associated acronyms; (b) structure of the system/project, including interconnections with other projects or systems; (c) purpose of the system/project; (d) nature of the information in the system/project and how it will be used; (e) who will have access to the information in the system/project; (f) and the manner of transmission to all users.

The National Crime Information Center (NCIC) is a computerized information system containing documented criminal justice information that is accessed by name and other descriptive data. The FBI established the NCIC system in 1967 as a service to facilitate the sharing of law enforcement information, and participation now encompasses criminal and noncriminal justice agencies located in the 50 states, the District of Columbia, United States territories and possessions, and select foreign countries. NCIC

[REDACTED]

b7E

The NCIC contains a variety of files of interest to law enforcement, including wanted persons, registered sex offenders, gang members, and missing persons. The NCIC has specific requirements for which agencies may enter records into a file, the necessary data elements for each record, and which agencies may access the file. These requirements vary based on the nature of the NCIC file. [REDACTED]

[REDACTED]

[REDACTED] Access to NCIC files is strictly controlled and audited by both the FBI and the state agencies.

The National Instant Criminal Background Check System (NICS) is a national name check system that is designed to immediately determine if a person is disqualified from receiving or possessing firearms. A person may be disqualified based on one of several federal statutory prohibitors (e.g. a felony conviction, a fugitive from justice, or a misdemeanor crime of domestic violence) or based on various state prohibitors. The NICS queries available records in authorized FBI information systems. [REDACTED]

[REDACTED]

b7E

The purpose of this Privacy Threshold Analysis (PTA) is to describe a new NCIC file, the NICS Denied Transaction File (DTF). This file will make specific information, relating to individuals who have been denied a firearm pursuant to a NICS check available to local, state, tribal, and federal criminal justice agencies for law enforcement purposes. The DTF will serve to warn law enforcement of individuals who have illegally attempted to obtain firearms and provide valuable lead information regarding the location of fugitives and identities of those subject to protection orders. The DTF will include biographic information such as name, date of birth, place of birth, and country of citizenship, as well as social security numbers, and other miscellaneous identification numbers related to the individual. In addition, transaction information such as the date of the NICS denial, state of purchase, and state of residency will be included in the record.



2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality)?

           NO

  X   YES    **[If yes, please continue.]**

3. Please indicate if any of the following characteristics apply to the information in the system about individuals: Bear in mind that log-on information may identify or be linkable to an individual.  
(Check all that apply.)

  X   The information directly identifies specific individuals.

The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

**If you marked any of the above, proceed to Question 4.**

None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly.

4. Does the system/project pertain only to government employees, contractors, or consultants?

NO  YES

5. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

NO. [If no, skip to question 7.]

YES. [If yes, proceed to the next question.]

6. Does the system/project collect any information directly from the person who is the subject of the information?

NO [If no, proceed to question 7.]

YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

NO

YES [If yes, proceed to question 7.]

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

NO [The program will need to work with PCLU to develop/implement the necessary form(s).]

YES Identify any forms, paper or electronic, used to request such information from the information subject:

7. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project? Full SSNs should only be used as identifiers in limited instances.

NO  YES **If yes, check all that apply:** SSNs are not mandatory fields for NCIC files and a search cannot be initiated solely by SSN; however, when a SSN is included in an NCIC inquiry, a search will be performed based on that SSN.

SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

SSNs are necessary to identify FBI personnel in this internal administrative system.

SSNs are important for other reasons. **Describe:** Assistance with the identification of persons for criminal justice purposes.

The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

It is not feasible for the system/project to provide special protection to SSNs. **Explain:**

8. Is the system operated by a contractor?

No.

Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

9. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

NO **If no, indicate reason; if C&A is pending, provide anticipated completion date:**

YES **If yes, please indicate the following, if known:**

Provide date of last C&A certification/re-certification:

Confidentiality:  Low  Moderate  High  Undefined

Integrity:  Low  Moderate  High  Undefined

Availability:  Low  Moderate  High  Undefined

Not applicable – this system is only paper-based.

10. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?

NO

YES If yes, please describe the data mining function:

11. Is this a national security system (as determined by the SecD)?

NO  YES

12. Status of System/ Project:

This is a new system/ project in development.

## II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

NO [If no, proceed to next question (II.3).]

YES If yes, indicate which of the following changes were involved (**mark all changes that apply, and provide brief explanation for each marked change**):

A conversion from paper-based records to an electronic system.

A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed.

(For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

\_\_\_\_\_ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

\_\_\_\_\_ A new method of authenticating the use of and access to information in identifiable form by members of the public.

\_\_\_\_\_ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

\_\_\_\_\_ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

\_\_\_\_\_ A change that results in a new use or disclosure of information in identifiable form.

\_\_\_\_\_ A change that results in new items of information in identifiable form being added into the system/project.

\_\_\_\_\_ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.

\_\_\_\_\_ Other [**Provide brief explanation**]:

3. Does a PIA for this system/project already exist?

\_\_\_\_\_ NO    \_\_\_\_\_ YES

If yes:

a. **Provide date/title of the PIA:**

b. Has the system/project undergone any significant changes since the PIA?

\_\_\_ NO    \_\_\_ YES

### FBI PRIVACY THRESHOLD ANALYSIS (PTA) (Equivalent to the DOJ Initial Privacy Assessment (IPA))

NAME OF SYSTEM / PROJECT: [insert both here and in header next page] [redacted]

Derived From:	<b>SYSTEM/PROJECT POC</b>	<b>FBI OGC/PCLU POC</b>
Classified By:	Name: [redacted]	Name: [redacted]
Reason:	Program Office: NOPU	Phone: [redacted]
Declassify On:	Division:	Room Number: C3-655
	Phone: [redacted]	
	Room Number:	

b7E  
b6  
b7C

#### FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary consonant with Division policy]

	Program Manager (CJIS Division)	Division Privacy Officer
Program Division: [insert division name]	Signature: [redacted] Date signed: 7/27/10 Name: Robert C. Rudge, Jr. Title: Section Chief	Signature: [redacted] Date signed: 7/22/10 Name: [redacted] Title: supervisory security specialist
FBIHQ Division: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6  
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7338).  
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

Upon final FBI approval, FBI OGC/PCLU will distribute as follows:

- 1 - Signed original to file 190-HQ-C1321794 (fwd to JEH 1B204 via PA-520)

Copies (recipients please print/reproduce as needed for Program/Division file(s)):

- 1 - DOJ Office of Privacy and Civil Liberties (via e-mail to [privacy@usdoj.gov](mailto:privacy@usdoj.gov)) (if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)
- 1 - OGC/PCLU intranet
- 1 - PCLU UC
- 1 - PCLU Library
- 1 - PCLU Tickler
- 2 - FBI OCIO / OIPP (JEH 9376, attn: [redacted])
- 1 - FBI SecD/AU (elec. copy: via e-mail to UC [redacted])
- 1 - RMD/RMAU (attn: [redacted])
- 2 - Program Division POC /Privacy Officer
- 2 - FBIHQ Division POC /Privacy Officer

b6  
b7C

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PTA drafter should skip to the next page and continue.]

\_\_\_\_\_ PIA is required by the E-Government Act.

\_\_\_\_\_ PIA is to be completed as a matter of FBI/DOJ discretion.

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? \_\_\_\_\_ Yes \_\_\_\_\_ No (indicate reason):

PIA is not required for the following reason(s):

\_\_\_\_\_ System does not collect, maintain, or disseminate PII.

\_\_\_\_\_ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).

\_\_\_\_\_ Information in the system relates to internal government operations.

\_\_\_\_\_ System has been previously assessed under an evaluation similar to a PIA.

\_\_\_\_\_ No significant privacy issues (or privacy issues are unchanged).

Other (describe): *NOR SORN will be revised to exclude this and other changes and a PIA will be done at that time.*

Applicable SORN(s): *NOT FBI-001*

Notify FBI RMD/RIDS per MIOG 190.2.3?  No \_\_\_\_\_ Yes--See sample EC on PCLU intranet website here:

[http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form\\_for\\_miog190-2-3\\_ec.wpd](http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd)

*Access to records handled via 28 C.F.R. Part 16 C.*

SORN/SORN revision(s) required? \_\_\_\_\_ No  Yes (indicate revisions needed):

*we will revised SORN to encompass this & other changes*

Prepare/revise/add Privacy Act (e)(3) statements for related forms? \_\_\_\_\_ No \_\_\_\_\_ Yes (indicate forms affected):

*N/A*

RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.

Other:

David C. Larson, Deputy General Counsel  
FBI Privacy and Civil Liberties Officer

Signature:

Date Signed:

*[Handwritten Signature]*  
*7/22/2010*

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

## I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes: name of the system/project, including associated acronyms; structure of the system/project, purpose; nature of the information in the system and how it will be used; who will have access to the information in the system and the manner of transmission to all users.

The National Crime Information Center (NCIC) is a computerized information system containing documented criminal justice information that is accessed by name and other descriptive data. The FBI established the NCIC system in 1967 as a service to facilitate the sharing of law enforcement information, and participation now encompasses criminal and noncriminal justice agencies located in the 50 states, the District of Columbia, U.S. territories and possessions, and select foreign countries. NCIC users

[REDACTED]  
[REDACTED] The FBI has issued a Privacy Act system of records notice (SORN) for the NCIC (JUSTICE/FBI-001) (64 F.R. 52343; 66 F.R. 33558; 70 F.R. 7513, 7517; 72 F.R. 3410).

The NCIC is managed and maintained by the FBI's Criminal Justice Information Services (CJIS) Division. The NCIC contains a variety of files of interest to law enforcement, including the Wanted Person File (WPF), one of NCIC's 12 "person" files. This file contains Personally Identifiable Information (PII) on individuals for whom criminal warrants are outstanding, including warrants for juvenile offenders and temporary warrants. The NCIC records are contributed by participating criminal justice agencies. Agencies that enter records are responsible for the accuracy, timeliness, and completeness of those records. The information entered needs to be as complete and accurate as possible to best identify suspects and to eliminate non-suspects. Currently, law enforcement personnel enter the name, date of birth, and physical descriptive information such as race, sex, and age for each wanted person, as well as miscellaneous numbers (to include social security numbers) that may assist in accurate identifications.



[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]



[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

b7E



2. Does the system/project collect, maintain, or disseminate any information about individuals in identifiable form, i.e., is information linked to or linkable to specific individuals (which is the definition of personally identifiable information (PII))?

\_\_\_\_\_ NO [If no, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.]

  X   YES [If yes, please continue.]

3. Does the system/project pertain only to government employees, contractors, or consultants?

  X   NO    \_\_\_\_\_ YES

4. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

\_\_\_\_\_ NO      X   YES

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

5. Are Social Security Numbers (SSNs) collected, maintained or disseminated from the system/project?

\_\_\_\_\_ NO      X   YES    If yes, check all that apply:

  X   SSNs are necessary to establish/confirm the identity of subjects, victims, witnesses or sources in this law enforcement or intelligence activity.

\_\_\_\_\_ SSNs are necessary to identify FBI personnel in this internal administrative system.

  X   SSNs are important for other reasons. **Describe:** Because SSNs are often used as identifiers for driver licenses, they are often requested/accessed by law enforcement personnel to confirm identities.

\_\_\_\_\_ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:**

  X   It is not feasible for the system/project to provide special protection to SSNs. **Explain:** Masking SSNs from law enforcement would be detrimental to the identification of wanted persons. Although SSNs may be entered into the WPF by law enforcement personnel as an optional field.

6. Does the system/project collect any information directly from the person who is the subject of the information?

  X   NO    [If no, proceed to question 7.] The information may be taken directly from the subject by the state or local law enforcement personnel, who then send the records to the NCIC.

\_\_\_\_\_ YES

a. Does the system/project support criminal, CT, or FCI investigations or assessments?

\_\_\_\_\_ YES    [If yes, proceed to question 7.]

\_\_\_\_\_ NO

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

\_\_\_\_\_ NO [The program will need to work with PCLU to develop/implement the necessary form(s).]

\_\_\_\_\_ YES Identify any forms, paper or electronic, used to request such information from the information subject:

7. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

\_\_\_\_\_ NO If no, indicate reason; if C&A is pending, provide anticipated completion date:

X  YES If yes, provide date of last C&A certification/re-certification:

09/03/2009

\_\_\_\_\_ Don't Know.

8. Is this system/project the subject of an OMB-300 budget submission?

X  NO \_\_\_\_\_ Don't know

\_\_\_\_\_ YES If yes, please provide the date and name or title of the OMB submission:

9. Is this a national security system (as determined by the SecD)?

X  NO

\_\_\_\_\_ YES

\_\_\_\_\_ Don't know

10. Status of System/ Project:

\_\_\_\_\_ This is a new system/ project in development. [If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

The NCIC is not a new system/project in development, nor does the WPF meet this definition. Instead, this is an initiative that adds an additional data field to the WPF.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? NCIC was developed in 1967
2. Has the system/project undergone any significant changes since April 17, 2003?

\_\_\_\_\_ NO [If no, proceed to next question (II.3).]

YES If yes, indicate which of the following changes were involved (mark all boxes that apply):

\_\_\_\_\_ A conversion from paper-based records to an electronic system.

\_\_\_\_\_ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.

\_\_\_\_\_ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

\_\_\_\_\_ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

\_\_\_\_\_ A new method of authenticating the use of and access to information in identifiable form by members of the public.

\_\_\_\_\_ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

A change that results in a new use or disclosure of information in identifiable form.

A change that results in new items of information in identifiable form being added into the system/project.

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

\_\_\_\_\_ Changes do not involve a change in the type of records maintained,  
the individuals on whom records are maintained, or the use or  
dissemination of information from the system/project.

\_\_\_\_\_ Other [Provide brief explanation]:

the NCIC has undergone numerous changes over the years. The NCIC has  
been in existence for decades and, in fact, predates the Privacy Act and the E-  
Government Act. At this time, a new System of Records Notice is being drafted and all  
initiatives are being reviewed for the appropriate PTA or PIA documentation.

b7E

3. Does a PIA for this system/project already exist?

NO  YES

If yes:

a. Provide date/title of the PIA:

b. Has the system/project undergone any significant changes since the PIA?

NO  YES

[The PTA is now complete and after division approval(s) should be submitted to  
FBI OGC/PCLU for final FBI approval and determination if PIA and/or other  
actions are required.]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

~~SECRET~~

**FBI PRIVACY THRESHOLD ANALYSIS (PTA)**  
(equivalent to the DOJ Initial Privacy Assessment (IPA))

b7E

NAME OF SYSTEM / PROJECT:

Derived From: Classified By: Reason: Declassify On:	<b>SYSTEM/PROJECT POC</b> Name: <input type="text"/> Program Office: National Assets Response Unit Division: CIRG Phone: <input type="text"/> Room Number: Gateway Bldg 3rd Flr	<b>FBI OGC/PCLU POC</b> Name: <input type="text"/> Phone: <input type="text"/> Room Number: 7458, JEH
--	--	--

b6  
b7C

**FBI DIVISION INTERMEDIATE APPROVALS**

	Program Division: Critical Incident Response Group (CIRG)	FBIHQ Division: CIRG
Program Manager (or other appropriate executive as Division determines)	Signature: /s Date signed: Name: <input type="text"/> Title: Render Safe Program Manager	Signature: /s Date signed: Name: Clifford C. Holly Title: Section Chief, Hazardous Devices Operations Section (HDOS)
Division Privacy Officer	Signature: /s Date signed: Name: <input type="text"/> Title: SSA/CDC/Privacy Officer, CIRG	Signature: Date signed: Name: Title:

b6  
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7338).

**FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:**

PIA required: <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes: _____ SORN/SORN revision required: <input type="checkbox"/> No <input type="checkbox"/> Yes: _____	
Applicable SORN(s): _____	
Notify FBI RMD/RIDS per MIOG 190.2.3: <input type="checkbox"/> No <input type="checkbox"/> Yes	
Consult with RMD to identify/resolve any Federal records/electronic records issues: <input type="checkbox"/> No <input type="checkbox"/> Yes:	
Prepare/revise/add Privacy Act (e)(3) statements for related forms? <input type="checkbox"/> No <input type="checkbox"/> Yes-forms affected:	
Other: _____	
David C. Larson, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: /s Date Signed: 9/29/2009

~~SECRET~~

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED]

b7E

Upon final FBI approval, FBI OGC/PCLU will distribute as follows:

1 - Signed original to file 190-HQ-C1321794 (fwd to JEH 1B204 via PA-520)

Copies (recipients please print/reproduce as needed for Program/Division file(s)):

1 - DOJ Office of Privacy and Civil Liberties (via e-mail to [privacy@usdoj.gov](mailto:privacy@usdoj.gov))  
(if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)

1 - OGC\PCLU intranet

2 - FBI OCIO / OIPP (JEH 9376, attn [REDACTED])

1 - PCLU UC

1 - FBI SecD/AU (electronic copy: via e-mail to UC [REDACTED])

1 - PCLU Library

1 - RMD/RMAU (attn [REDACTED])

1 - PCLU Tickler

2 - Program Division POC /Privacy Officer

2 - FBIHQ Division POC /Privacy Officer

b6  
b7C

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

b7E

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Name of the system/project. Provide current name, any previous or anticipated name changes, and any associated acronyms:

b7E

2. Briefly describe the system's/project's structure (including identification of any components/subsystems or parent system, if applicable).

b1  
b7E

3. What is the purpose for the system/project?

b1  
b7E

4. Please provide a general summary of the nature of information in the system/project and how it will be used:

5. Does the system/project collect, maintain, or disseminate any information about individuals in identifiable form, i.e., is information linked to or linkable to specific individuals (which is the definition of personally identifiable information (PII))?

NO.

**Stop. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are otherwise advised, no PIA is required.**

YES.

If yes, please continue.

6. Access

a. Describe the means of accessing the system/project and transmitting information to and from the system/project:



FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

b7E

b. Describe who within the FBI will have access to the information in the system and the controls for ensuring that only authorized persons can access the information:

c. Describe who outside the FBI will have access to the information in the system/project and the controls for ensuring that only authorized persons can access the information:

7. Does the system/project pertain only to government employees, contractors, or consultants?

NO

YES. If yes, provide a brief explanation of the quantity and type of information:

8. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

NO  YES

9. Are Social Security Numbers collected, maintained or disseminated from the system/project?

NO

YES. If yes, for systems/projects **other than** those supporting law enforcement or intelligence activities:

- What is the purpose for the collection, maintenance or dissemination of SSNs?
- Is it feasible to eliminate SSNs from the system/project (please indicate why or why not)?
- In light of Federal policy to reduce the use of SSNs, is it feasible to minimize system/project-user access to SSNs in the system/project (why or why not)?

10. Does the system/project collect any information directly from the person who is the subject of the information?

NO

YES. If yes, for systems/projects **other than** those relating to criminal investigations, CT, or CI:

- Indicate how such information is collected:
- Identify by name and form number any forms used to request such information from the information subject (this includes paper or electronic forms):
- Are information subjects from whom information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?  Yes  No

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

b7E

11. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?

NO. If no, please indicate reason; if C&A is pending, provide anticipated completion date:

YES. If yes, please:  
- Provide date of last C&A certification/re-certification:

Don't Know

12. Is this system/project the subject of an OMB-300 budget submission?

NO  Don't know

YES. If yes, if the name of the OMB 300 is not the same as the name of the system/project, please provide OMB name:

13. Is this a national security system (as determined by the SecD)?

NO  YES  Don't know

14. Status of System/ Project:

This is a new system/ project in development. **[Stop. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required.]**

This is an existing system/project. [Continue to Section II.]

**II. EXISTING SYSTEMS / PROJECTS**

1. When was the system/project developed?

2. Has the system/project undergone any significant changes since April 17, 2003?

NO. If no, proceed to next question (II.3).

YES. If yes, indicate which of the following changes were involved **(mark all boxes that apply):**

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

b7E

- A conversion from paper-based records to an electronic system.
- A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.
- A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)
- A change that results in information in identifiable form being merged, centralized, or matched with other databases.
- A new method of authenticating the use of and access to information in identifiable form by members of the public.
- A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.
- A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.
- A change that results in a new use or disclosure of information in identifiable form.
- A change that results in new items of information in identifiable form being added into the system/project.
- Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.
- Other. [Please provide brief explanation]:

3. Does a PIA for this system/project already exist?

NO

YES. If yes, please provide date/title of the PIA:

**The PTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if PIA and/or other actions are required .**