

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

Unclassified ~~FOUO~~

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

NAME OF SYSTEM / PROJECT: HRT [redacted]

<b>Derived From:</b> <b>Classified By:</b> <b>Reason:</b> <b>Declassify On:</b>	<b>SYSTEM/PROJECT POC</b> Name: [redacted] Program Office: HRT/GREY Unit Division: CIRG Phone: [redacted] Room Number: FBI Academy, QT	<b>FBI OGC/PCLU POC</b> Name: [redacted] Phone: [redacted] Room Number: 7458, JEH
--	---	--

b7E

b6  
b7C

**FBI DIVISION INTERMEDIATE APPROVALS**

	Program Division: CIRG	FBIHQ Division: CIRG
Program Manager (or other appropriate executive as Division determines)	Signature: /s Date signed: Name: [redacted] Title: Supervisory Special Agent	Signature: /s Date signed: Name: James F. Yacone Title: Section Chief, Tactical Section
Division Privacy Officer	Signature: Date signed: Name: Kenneth R. Gross, Jr. Title: CIRG SSA\CDC	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: Date Signed: /s/ David C. Larson 3/3/10

Unclassified ~~FOUO~~

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

Hostage Rescue Team (HRT), [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

1 - PCLU UC

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

1 - PCLU Library

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

1 - PCLU Tickler

1 - RMD/RMAU (attn: [redacted])

2 - Program Division POC /Privacy Officer

2 - FBIHQ Division POC /Privacy Officer

b6

b7C



FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

Hostage Rescue Team (HRT), [redacted]

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:

Hostage Rescue Team (HRT), [redacted]

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

[redacted]

Working with ITOD and SecD to determine whether a full scale C&A effort is needed or whether it may fit within another system's C&A.

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

[redacted]

b7E

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

[redacted]

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.

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

Hostage Rescue Team (HRT)

b7E

6. Access

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

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. This system supports law enforcement and/or intelligence activities. Every deployment is unique and may collect different types of information to support the current mission requirements.

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?

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

Hostage Rescue Team (HRT)

b7E

- 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. This system may be used for any number of reasons due to the fact that each deployment supports a unique situation/FBI program. The equipment is deployed to support training, special events, investigations, etc.

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

Hostage Rescue Team (HRT)

b7E

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):

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.)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

Hostage Rescue Team (HRT),

b7E

- 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]:

b7E

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 .**

### FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: iDetect Security System

BIKR FBI Unique Asset ID: N/A

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: [Redacted] Program Office: FBI Police - Admin Division: Security Division Phone: [Redacted] Room Number: M-281, JEH	Name: [Redacted] Phone: [Redacted] Room Number: JEH, 7350

b6  
b7C

#### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive)	Division Privacy Officer
Program Division: FBI Police	Signature: [Redacted] Date signed: 10/16/11 Name: [Redacted] Title: Unit Chief	Signature: [Redacted] Date signed: [Redacted] Name: [Redacted] Title: Assistant General Counsel
FBIHQ Division: Security Division	Signature: <i>Colleen H. Conyngham</i> Date signed: 10/3/11 Name: Colleen Conyngham Title: Section Chief	Signature: [Redacted] Date signed: [Redacted] Name: [Redacted] Title: Assistant General Counsel

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

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 :

Applicable SORN(s): Justice/FBI-013, Security Access Control System (SACS)

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"/> Unit Chief Privacy and Civil Liberties Unit	Signature: <input type="checkbox"/> Date Signed: 10/12/11
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 10/12/11

b6  
b7c

UNCLASSIFIED

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.

FBI Police Management purchased the IDetect Security System in order to assist with security measures in the FBI Headquarters' Visitor Center.

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.



UNCLASSIFIED

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

UNCLASSIFIED

information from the information subject: Privacy Act (e)(3) statements are posted in the location where an officer asks for information.

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:

It is not feasible for the system/project to provide special protection to SSNs. Explain: However, only a small, select group of FBI Police personnel, with a need to know for their official duties, will have access to the system (and SSNs) at all.

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: C&A is pending.

UNCLASSIFIED

\_\_\_\_\_ 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. 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.

## 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):

UNCLASSIFIED

UNCLASSIFIED

\_\_\_\_\_ 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

UNCLASSIFIED

### FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

BIKR FBI Unique Asset ID:

b3

Derived From: Classified By: Reason: Declassify On:	<b>SYSTEM/PROJECT POC</b> Name: <input type="text"/> Program Office: ITB Division: ITSD Phone: <input type="text"/> Room Number: 8979	<b>FBI OGC/PCLU POC</b> Name: <input type="text"/> Phone: <input type="text"/> Room Number: Rm 7350
--	--	--

b6  
b7C

#### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: CD	Signature: <i>[Signature]</i> Date signed: <i>8/29/12</i> Name: <input type="text"/> Title: MAPA	Signature: <i>[Signature]</i> Date signed: <i>8/29/12</i> Name: <input type="text"/> Title: SSA
FBIHQ Division: ITSD	Signature: <i>[Signature]</i> Date signed: <i>11/6/12</i> Name: <input type="text"/> Title: IT Specialist	Signature: <i>[Signature]</i> Date signed: <i>11/6/12</i> Name: <input type="text"/> Title: Chief, Process Policy & Metrics Unit

b6  
b7C

~~UNCLASSIFIED // FOUO~~

**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 (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):

b3  
b7E

Applicable SORN(s): JUSTICE/FBI-002 (Central Records System); JUSTICE/FBI-021 (DIVS  
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 (indicate revisions needed):

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

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:

b3  
b7D

James J. Landon, Deputy General Counsel and  
FBI Privacy and Civil Liberties Officer

Signature: *William H. Wells, Acting*  
Date Signed: *8/30/12*

~~UNCLASSIFIED // FOUO~~

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

**I. 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



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 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:

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



b3  
b7E

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:  
04/26/2010

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)?

X  NO

\_\_\_\_\_ YES If yes, please describe the data mining function:

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

\_\_\_\_\_ NO  X  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? 10/1991

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

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

X  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.

X  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.)

X  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.

X  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?

X  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: InfraGard Network (IGN)

BIKR FBI Unique Asset ID: SYS-2011-025-01

	<b>SYSTEM/PROJECT POC</b> Name: [REDACTED] Program Office: National Industry Partnership Unit (NIPU) Division: Cyber Phone: [REDACTED] Room Number:	<b>FBI OGC/PCLU POC</b> Name: [REDACTED] Phone: [REDACTED] Room Number: JEH, Rm 7350
--	---	---

b6  
b7C

#### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
FBIHQ Division: Cyber	Signature: [REDACTED] Date signed: 3/21/13 Name: [REDACTED] Title: Supervisory Special Agent, IGN Program Manager	Signature: [REDACTED] Date signed: 3/28/13 Name: [REDACTED] Title: CyD Privacy Officer

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

**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 :

Applicable SORN(s): DOJ/FBI-002, Central Records System, published at 63 Fed. Reg. 8671 (Feb. 20, 1998) as amended at 66 Fed. Reg. 17200 (March 29, 2001) and 66 Fed. Reg. 29994 (June 4, 2001)

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 records 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"/> Acting Unit Chief Privacy and Civil Liberties Unit	Signature: <input type="checkbox"/> Date Signed: 3/29/2013
Brian F. Binney, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 3/29/2013

b6  
b7c

UNCLASSIFIED

## 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.

InfraGard is a joint FBI-Industry partnership that is used to facilitate information sharing between Industry partners and the FBI. Members come from all segments of industry. The information shared is associated with the full spectrum of potential threats directed against the United States. InfraGard as an organization has existed in a variety of forms since the late 1990's.

InfraGard is organized into regionally based chapters. Every member must be a member of a chapter. Each chapter has an FBI coordinator. The FBI coordinator is an agent from the local FBI field office.

The InfraGard Network (IGN) is used to facilitate the information sharing. The old IGN consists of a web site that is hosted at the Criminal Justice Information Services Division (CJIS). Due to technical limitations, the old site must be shut down and migrated to a new site by 1 April 2013. The new IGN consists of a Public web site and a Private web site. The Public web site is hosted at CJIS in a specially protected local area network where FBI applications accessible from the Internet are hosted, and is accessible by anyone from the Internet.

[REDACTED]

b7E

Users apply for InfraGard membership by filling out an application located on the Public site. The application includes personally identifiable information (PII) that is used to identify the applicant for an FBI conducted records check. The application includes a section that advises the applicant of their Privacy Act rights and the purposes for which the submitted data will be used as well as an acknowledgement that he/she has read and understands the purposes and his/her rights. Once the applicant has filled out the application online and selects submit, the personal information is moved using an encrypted link from the Public server to the Private server where it is stored in encrypted form. The personal information is deleted from the application and is not maintained on the Public site.

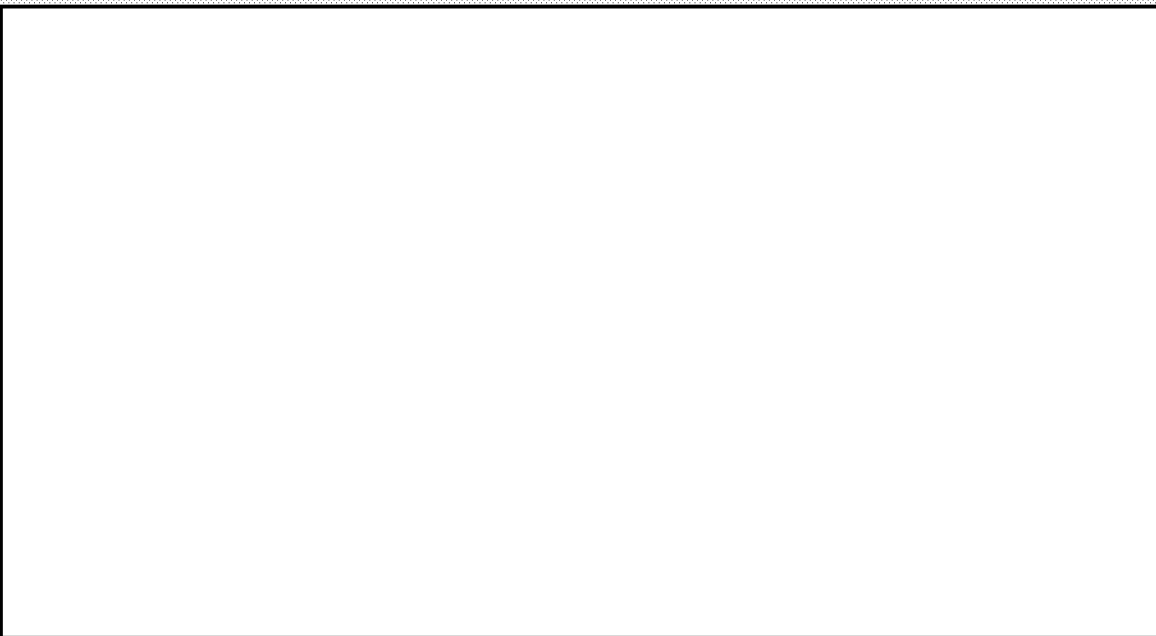
Once the IGN membership application has been submitted, the application goes through a workflow on the IGN system. Part of the workflow requires the FBI chapter coordinator or other FBI coordinator at FBI Headquarters to perform a records check and either

approve or disapprove the application. The records check requires the use of the applicant's Social Security Number (SSN) for identity.

The applicant's personal information is retained and stored encrypted on the Private server, until needed for periodic revalidation. The revalidation occurs every five years and follows a similar workflow as the initial application.

Additionally, once his/her membership is approved, each user creates his/her own profile. The profile includes selected PII (but not SSNs). The user can elect to share or not share his/her own PII in the profile. The PII in the user profile is not viewable by other users unless the owner elects to share it. This selected PII may include user information such as phone, address, email, and company name. The user profile data is encrypted in motion and at rest.

InfraGard published information is shared by posting it to either the Public or Private web sites. However, any information considered for sharing is first submitted to the IGN help desk and then reviewed by chapter coordinators or IGN unit staff at Headquarters for approval to share prior to being posted on either the Public or Private site. Information for sharing that is received from FBI chapter coordinators or IGN unit staff at Headquarters is presumed to be approved for sharing and is posted to the appropriate web site without review. Information received from another Government agency (such as DHS or TSA) is presumed to be approved for sharing and is posted to the appropriate web site without further FBI review. Once approved for sharing, the information is posted on the site by the IGN help desk. In all cases, prior to being posted on the web site, the information to be shared is reviewed for IGN appropriate content.<sup>1</sup>



b7E

<sup>1</sup> For example, articles disparaging other IGN members or containing someone's PII are not considered appropriate for sharing.



In addition to information sharing, the IGN Private site provides collaborative tools (bulletin boards, blogs) that allow members to interact within IGN. The IGN system sends emails to users alerting them to changes in content of interest on the IGN site. The mail system is also used for administrative purposes such as letting users know to change their passwords. Emails generated by a user will include the first line of the message, or something similar. [REDACTED]

b7E

[REDACTED] For example, if a user puts sensitive information in the first line, the IGN application will not determine that the information is sensitive and will send the email. If discovered, the user could be removed from IGN membership. Sensitive information is described in the InfraGard Rules of Behavior.

The new IGN system is currently undergoing certification and accreditation by FBI SecD. The new IGN system was designed to meet all FISMA, DOJ and FBI security requirements.

The only PII that is retained by the system is that associated with membership applications. The PII is stored encrypted. The PII is encrypted when in motion between systems. The PII is normally accessible only by FBI chapter coordinators or unit personnel conducting membership related records checks. Some PII that indirectly identifies a user is included in the user Profile. Each user individually decides what information to share or not share from within his/her profile. As with all computer systems, privileged users, such as system administrators, can gain access to the information. However, access is monitored for misuse using security audit tools reviewed by IGN Information Systems Security Officers. The membership PII is stored on backup media in an encrypted form.

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.

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

  X   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 – The only information maintained is membership information.



b7E

\_\_\_\_\_ 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: Potential members are provided an (e)(3) statement on the application to become a member.

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: **SSNs are used by FBI personnel to identify InfraGard membership applicants as part of the conduct of a records check used in the determination of suitability for InfraGard membership. Once a person is approved for membership, SSNs are used again for a records check for periodic re-validation of membership suitability that is performed every 5 years.**

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: **The SSNs are encrypted when in transit or at rest in storage. Access to the PII is managed by roles within the IGN application. The only users allowed to access the SSNs are the FBI chapter coordinators or FBI National Industry Partnership Unit (NIPU) personnel at FBI Headquarters.**

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:  
27 March 2013

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: Operational system that is undergoing transition migration to a new environment.

This is a new system/ project in development.

**II. EXISTING SYSTEMS / PROJECTS**

1. When was the system/project developed? The system has been operating in various capacities since 1996.

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: **InfraGard, June 23, 2009**

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

\_\_\_\_\_ NO  YES

### FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM/PROJECT: Innocence Lost Database (ILDB)

BIKR FBI Unique Asset ID: APP-0000275

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: SSA [REDACTED] Program Office: Crimes Against Children Unit Division: CID Phone: [REDACTED] Room Number: G-300	Name: AGC [REDACTED] Phone: [REDACTED] Room Number: JEH, 7350

b6  
b7C

#### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Crimes Against Children	Signature: [REDACTED] Date signed: 10/27/2011 Name: [REDACTED] Title: Unit Chief	Signature: [REDACTED] Date signed: 11/28/2011 Name: [REDACTED] Title: Special Assistant to the Assistant Director
FBIHQ Division: Criminal Investigative Division	Signature: [REDACTED] Date signed: 11/28/2011 Name: [REDACTED] Title: Unit Chief	Signature: [REDACTED] Date signed: 11/28/2011 Name: [REDACTED] 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.)

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

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): The Central Records System, Justice/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"/> Unit Chief Privacy and Civil Liberties Unit	Signature: <input type="checkbox"/> Date Signed: <input type="checkbox"/>
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: <i>[Handwritten Signature]</i> Date Signed: <i>7/5/14</i>

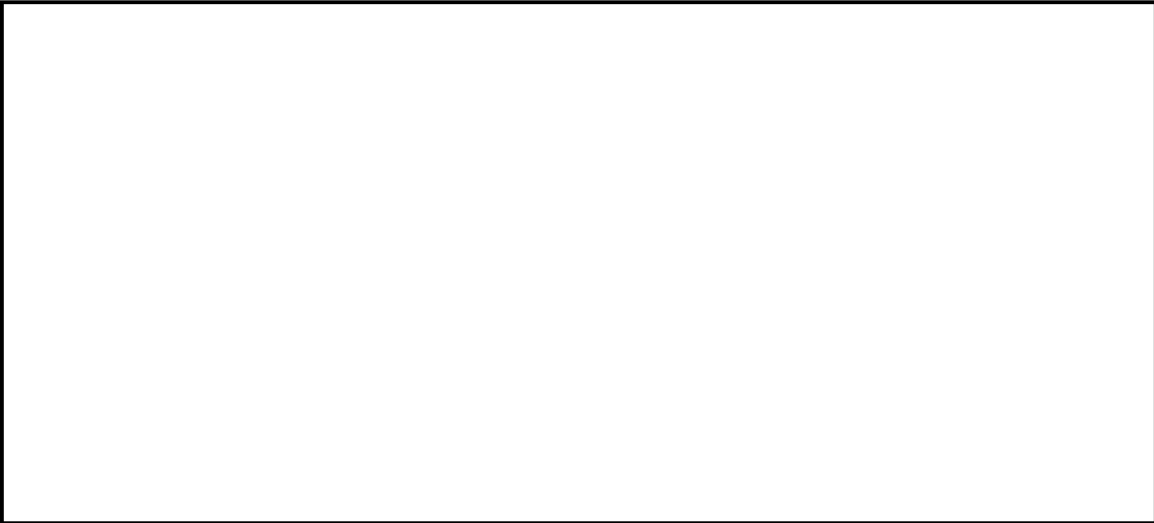
b6  
b7c



## 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.

To facilitate the interagency sharing of intelligence information necessary to combat the commercial sexual exploitation of children through prostitution, the Innocence Lost Database (ILDB), a national child prostitution database, was developed to record biographical information regarding suspected pimps and victims of prostitution. The ILDB permits the sharing of intelligence by local law enforcement agencies that previously and independently collected and gathered intelligence on prostitution activities within their Areas of Responsibility (AOR), that may not have realized that the individuals and organizations whom they were investigating were also involved in criminal activity in other cities, states and regions. Because of the enterprise nature of child prostitution, centralizing the intelligence gathered from local law enforcement has facilitated the effective investigation and prosecution of crimes against children that cross legal and geographic jurisdictional boundaries.



b7E

The Innocence Lost database is maintained on Law Enforcement Online (LEO), which is a secure controlled-access communications and information sharing repository accessible to authorized law enforcement users through a password-protected system. LEO operates as an SBU network and is certified and accredited under the Federal Information Security Management Act. [REDACTED]

b7E

[REDACTED] These devices prevent unauthorized access to or reading of data as it passes over the links. End users will have varying levels of read/write access based on their involvement in Innocence Lost Child Prostitution Task Forces. [REDACTED]



[redacted] locate information needed for on-going investigations, based on their particular role. The FBI is the sole agency to authorize the end users of the Innocence Lost database. In addition, an FBI data steward from the CACU is ultimately responsible for the database and, through oversight, ensures adherence to database rules.

Development of the ILDB has ultimately led to the initiation of more effective investigations, location of more missing children, and prosecution of more offenders.

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.

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

  X   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?

  X   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.]

  X   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 It is possible that some of the information in the ILDB will come directly from law enforcement interviews of pimps or victims as well as from online advertisements posted by the pimp.

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:

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

Before individuals are granted access to the ILDB and the SSNs it contains, they must demonstrate involvement in the investigation and/or prosecution of child prostitution. The ILDB administrators carefully review and vet access requests. As a result, individuals with access to the ILDB have demonstrated a particular need for this detailed and sensitive information before they are granted access.

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:

Innocence Lost is included in LEO's C & A, which expires March, 2012.

Provide date of last C&A certification/re-certification:  
March 18, 2010

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.

## II. EXISTING SYSTEMS / PROJECTS

- 1. When was the system/project developed? June 2008

- 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      X   YES

If yes:

a. Provide date/title of the PIA: Innocence Lost Database, November 15, 2007.

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

  X   NO    \_\_\_\_\_ YES

### FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Innocence Lost Database Updates

BIKR FBI Unique Asset ID: APP-0000275

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: SSA [redacted]	Name: AGC [redacted]
Program Office: CACU	Phone: [redacted]
Division: CID	Room Number: JEH, 7350
Phone: [redacted]	
Room Number: JEH, G-300	

b6  
b7C

#### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Crimes Against Children Unit	Signature: [redacted] Date signed: 7/21/2012 Name: [redacted] Title: Unit Chief	Signature: [redacted] Date signed: 7/21/2012 Name: [redacted] Title: Special Assistant to the Assistant Director
FBIHQ Division: Criminal Investigative Division (CID)	Signature: [redacted] Date signed: 7/11/2012 Name: [redacted] Title: Assistant Section Chief	Signature: [redacted] Date signed: 7/13/2012 Name: [redacted] 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.)

**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: Due to the sensitive nature of this database, the PIA update will not be published.

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): Central Records System, Justice/FBI-002, until such time as a new SORN is published to cover the new upgrades.

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:

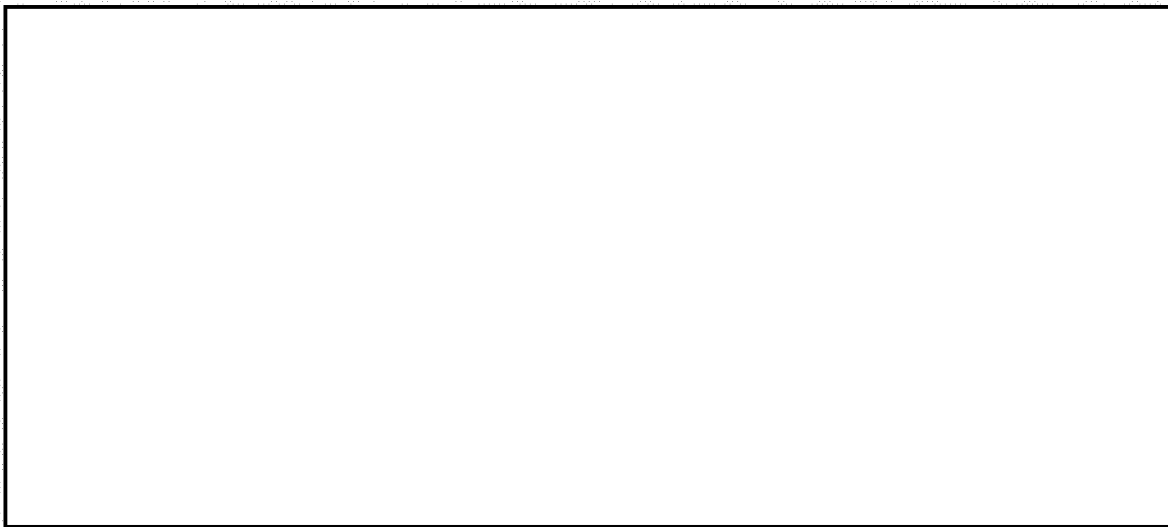
<input type="checkbox"/> Unit Chief Privacy and Civil Liberties Unit	Signature: <input type="checkbox"/> Date Signed: 8/7/12
Brian Binney, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 8/14/12

b6  
b7c

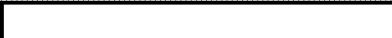
## I. INFORMATION ABOUT THE SYSTEM / PROJECT

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



To facilitate the interagency sharing of intelligence information necessary to combat the commercial sexual exploitation of children through prostitution, the Innocence Lost Database (ILDB), a national child prostitution database, was developed to record biographical information regarding suspected pimps and victims of prostitution. The ILDB permits the sharing of intelligence by local law enforcement agencies that previously collected and gathered intelligence on prostitution activities within their areas of responsibility and may not have realized that the individuals and organizations whom they were investigating were also involved in criminal activity in other cities, states and regions. Because of the enterprise nature of child prostitution, centralizing the intelligence gathered from local law enforcement has facilitated the effective investigation and prosecution of crimes against children that cross legal and geographic jurisdictional boundaries.



b7E

The Innocence Lost database is maintained on Law Enforcement Online (LEO), which is a secure controlled-access communications and information sharing repository accessible to authorized law enforcement users through a password-protected system. LEO operates as a Sensitive But Unclassified network and is certified and accredited under the Federal Information Security Management Act. 

b7E

  
 These devices prevent unauthorized access to or reading of data as it passes over the links. End users will have varying levels of read/write access based on their involvement in Innocence Lost Child Prostitution Task Forces.

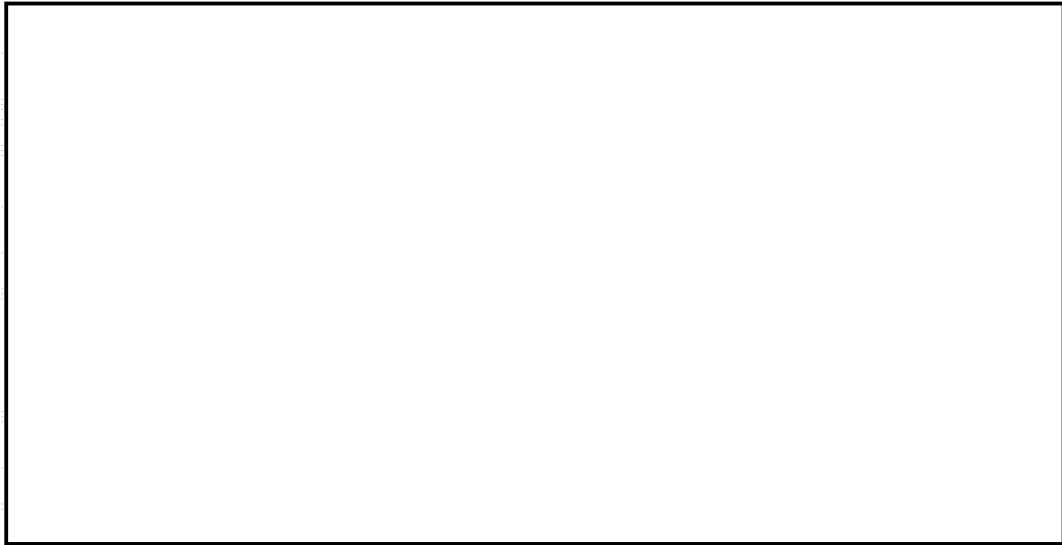


An FBI data steward from the CACU is ultimately responsible for the database and, through oversight, ensures adherence to database rules. These rules provide that end users' access is based on their role in the Innocence Lost Child Prostitution Task Forces and only FBI personnel can authorize end user participation in the database.

b7E

locate information needed for on-going investigations, based on their particular role.

The following upgrades and additions are proposed for the ILDB (and will be discussed in additional detail in a PIA update):



b7E

Development of the ILDB has ultimately led to the initiation of more effective investigations, location of more missing children, and prosecution of more offenders. The upgrades mentioned above are designed to continue this progress.

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 Information  is likely to have been posted by the suspected pimp and may contain his/her phone number or contact information. In addition, it is possible that some of the information in the ILDB will come directly from law enforcement interviews of pimps or victims.

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:

It is not feasible for the system/project to provide special protection to SSNs. Explain: Before individuals are granted access to the ILDB and the SSNs contained within it, they must demonstrate involvement in the investigation and/or prosecution of child prostitution. The ILDB administrators carefully review and vet access requests. As a result, individuals with access to the ILDB have demonstrated a particular need for this detailed and sensitive information before they are granted access.

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: Innocence Lost is included in LEO's C&A, which is currently undergoing reaccreditation. The below information is from LEO's most recent C&A.

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? June 2008

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: Innocence Lost Database, November 15, 2007

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

NO  YES (see above)