10. Status of System/Project:
   X  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.
UNCATEGORIZED

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:

ea. 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))

<table>
<thead>
<tr>
<th>NAME OF SYSTEM / PROJECT:</th>
<th>HR</th>
<th>SYSTEM/PROJECT POC</th>
<th>FBI OGC/PCLU POC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derived From:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classified By:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reason:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Declassify On:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Program Division: CIRG</th>
<th>FBIHQ Division: CIRG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(or other appropriate executive as Division determines)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature: /s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date signed:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title:</td>
<td>Supervisory Special Agent</td>
<td>Section Chief, Tactical Section</td>
</tr>
</tbody>
</table>

| Division Privacy Officer |                        |                      |
| Signature:              |                        |                      |
| Date signed:            |                        |                      |
| Name:                   | Kenneth R. Gross, Jr.  | James F. Yacone      |
| Title:                  | CIRG SSA\CDC            | Title:                |

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

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

<table>
<thead>
<tr>
<th>PIA required:</th>
<th>___X___No</th>
<th>___Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Applicable SORN(s):</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Notify FBI RMD/RIDS per MIOG 190.2.3:</th>
<th>___No</th>
<th>___Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Consult with RMD to identify/resolve any Federal records/electronic records issues:</th>
<th>___No</th>
<th>___Yes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Prepare/revise/add Privacy Act (e)(3) statements for related forms?</th>
<th>___No</th>
<th>___Yes-forms affected:</th>
</tr>
</thead>
</table>

Other:

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

Signature: /s David C. Larson 3/3/10
FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

Hostage Rescue Team (HRT)
FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

Hostage Rescue Team (HRT)

1. 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)

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

   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?

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.
FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

Hostage Rescue Team (HRT)

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)

- 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)?

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) □

☑ 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)

☐ 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]:

☐ 7

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

<table>
<thead>
<tr>
<th>SYSTEM/PROJECT POC</th>
<th>FBI OGC/PCLU POC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>Name:</td>
</tr>
<tr>
<td>Program Office: FBI Police - Admin</td>
<td>Phone:</td>
</tr>
<tr>
<td>Division: Security Division</td>
<td>Room Number: JEH, 7350</td>
</tr>
<tr>
<td>Phone:</td>
<td></td>
</tr>
<tr>
<td>Room Number: M-281, JEH</td>
<td></td>
</tr>
</tbody>
</table>

**FBI DIVISION INTERMEDIATE APPROVALS**

<table>
<thead>
<tr>
<th>Program Division: FBI Police</th>
<th>Division Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager (for other appropriate executive)</td>
<td>Signature:</td>
</tr>
<tr>
<td>Date signed: 7/1/2011</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Title: Unit Chief</td>
<td></td>
</tr>
<tr>
<td>Signature: Colleen Corgyham</td>
<td></td>
</tr>
<tr>
<td>Date signed: 10/2/11</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Title: Section Chief</td>
<td></td>
</tr>
</tbody>
</table>

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:

- **X** 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 reductions)? **X** 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 MI0G 190.2.3? ___ No **X** 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

SORN/SORN revision(s) required? **X** No ___ Yes:

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

<table>
<thead>
<tr>
<th>Unit Chief</th>
<th>Signature</th>
<th>Date Signed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Civil Liberties Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>James J. Landon, Deputy General Counsel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FBI Privacy and Civil Liberties Officer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

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.)

   _____ 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.]

X YES

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

X 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).]

X 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?

____ X__ NO

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


____ X__ NO

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

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

____ X__ NO __________ YES

13. Status of System/Project:

____ X__ 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

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:

Derived From:
Classified By:
Reason:
Declassify On:

SYSTEM/PROJECT POC
Name:
Program Office: ITB
Division: ITSD
Phone:
Room Number: 8979

FBI OGC/PCLU POC
Name:
Phone:
Room Number: Rm 7350

FBI DIVISION INTERMEDIATE APPROVALS

Program Manager (or other appropriate executive as Division determines)

Program Division: CD
Signature: 8/29/12
Date signed: 8/29/12
Name:
Title: MAPA

FBIHQ Division: ITSD
Signature:
Date signed: 11/12
Name:
Title: IT Specialist

Division Privacy Officer

Signature: 8/29/12
Date signed: 8/29/12
Name:
Title: SSA

Signature: 7/1/12
Date signed: 7/1/12
Name:
Title: Chief, Process Policy & Metrics Unit
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):

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_mioig190-2-3_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:

James J. Landon, Deputy General Counsel and FBI Privacy and Civil Liberties Officer
Signature:
Date Signed: 5/30/12
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.
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
UNCLASSIFIED //FOUO

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.
X 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:**

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

---

8. Is the system operated by a contractor?

X 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: 04/26/2010

Confidentiality: Low Moderate High Undefined

Integrity: Low Moderate High Undefined

Availability: Low Moderate High Undefined

   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.

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_

<table>
<thead>
<tr>
<th>SYSTEM/PROJECT POC</th>
<th>FBI OGC/PCLU POC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>Name:</td>
</tr>
<tr>
<td>Program Office:</td>
<td>Phone:</td>
</tr>
<tr>
<td>National Industry</td>
<td>Room Number:</td>
</tr>
<tr>
<td>Partnership Unit (NIPU)</td>
<td>JEH, Rm 7350</td>
</tr>
<tr>
<td>Division: Cyber</td>
<td></td>
</tr>
<tr>
<td>Phone:</td>
<td></td>
</tr>
<tr>
<td>Room Number:</td>
<td></td>
</tr>
</tbody>
</table>

FBI DIVISION INTERMEDIATE APPROVALS

<table>
<thead>
<tr>
<th>FBIHQ Division: Cyber</th>
<th>Signature:</th>
<th>Date signed:</th>
<th>Date signed:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>7/31/2012</td>
<td>3/28/2013</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

___ X ___ PIA is required by the E-Government Act.

___ X ___ 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)?  ___ X Yes.  ___ No:

___ X ___ 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:


 Notify FBI RMD/RIDS per MIOG 190.2.3?  ___ No  ___ X Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_mioig190-2-3_ec.wpd

SORN/SORN revision(s) required?  ___ X No  ___ Yes

Prepare/revise/add Privacy Act (e)(3) statements for related forms?  ___ X 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:

<table>
<thead>
<tr>
<th>Acting Unit Chief</th>
<th>Signature</th>
<th>Date Signed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Civil Liberties Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brian F. Binney, Acting Deputy General Counsel</td>
<td>Signature:</td>
<td>Date Signed:</td>
</tr>
<tr>
<td>FBI Privacy and Civil Liberties Officer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

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.¹

¹ 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. 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.

      ___ 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.

___ NO  ___ YES  If yes, check all that apply:

___ 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.

___ X___ 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.

___ X 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  ___ YES  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: 27 March 2013

Confidentiality:  __Low   _X_Moderate   _High   _Undefined

Integrity:     __Low   _X_Moderate   _High   _Undefined

Availability:  __Low   _X_Moderate   _High   _Undefined

_____ Not applicable — this system is only paper-based.


__X__ NO

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

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

__X__ 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).]

__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.

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

   9
# FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

**BIKR FBI Unique Asset ID:** APP-0000275

<table>
<thead>
<tr>
<th>SYSTEM/PROJECT POC</th>
<th>FBI OGC/PCLU POC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: SSA</td>
<td>Name: AGC</td>
</tr>
<tr>
<td>Program Office: Crimes Against Children Unit</td>
<td>Phone:</td>
</tr>
<tr>
<td>Division: CID</td>
<td>Room Number: JEH, 7350</td>
</tr>
<tr>
<td>Phone:</td>
<td>Room Number: G-300</td>
</tr>
</tbody>
</table>

## FBI DIVISION INTERMEDIATE APPROVALS

<table>
<thead>
<tr>
<th>Program Division: Crimes Against Children</th>
<th>Division Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager (or other appropriate executive as Division determines)</td>
<td></td>
</tr>
<tr>
<td>Signature:</td>
<td>Signature:</td>
</tr>
<tr>
<td>Date signed: 2015.04.07</td>
<td>Date signed: 2015.04.20</td>
</tr>
<tr>
<td>Name:</td>
<td>Name:</td>
</tr>
<tr>
<td>Title: Unit Chief</td>
<td>Title: Special Assistant to the Assistant Director</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FBIHQ Division: Criminal Investigative Division</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager (or other appropriate executive as Division determines)</td>
<td></td>
</tr>
<tr>
<td>Signature: 2015.04.20</td>
<td>Signature: 2015.04.20</td>
</tr>
<tr>
<td>Date signed: 2015.04.20</td>
<td>Date signed: 2015.04.20</td>
</tr>
<tr>
<td>Name:</td>
<td>Name:</td>
</tr>
<tr>
<td>Title: Unit Chief</td>
<td>Title: Special Assistant to the Assistant Director</td>
</tr>
</tbody>
</table>

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.

_____ X 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.

_____ X 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 MOG 190:2.3?  _____ X No  _____ Yes—See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_mog190-2-3_ec.wpd

SORN/SORN revision(s) required?  _____ X No  _____ Yes

Prepare/revise/add Privacy Act (p)(3) statements for related forms?  _____ X 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:

<table>
<thead>
<tr>
<th>Privacy and Civil Liberties Unit</th>
<th>Unit Chief</th>
<th>Signature:</th>
</tr>
</thead>
<tbody>
<tr>
<td>James J. Landon, Deputy General Counsel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FBI Privacy and Civil Liberties Officer | Signature: |
|---------------------------------------|------------|

Date Signed: 7/14/19
1. 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.

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.
locate information needed for ongoing 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

   ___ 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 linkable 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?

   ___ X____ 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?

   X 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:


    X__ NO

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

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

    X__ 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?

    X__ 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:


   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 Updates

BIKR FBI Unique Asset ID: APP-00000275

<table>
<thead>
<tr>
<th>SYSTEM/PROJECT POC</th>
<th>FBI OGC/PCLU POC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: SSA</td>
<td>Name: AGC</td>
</tr>
<tr>
<td>Program Office: CACU</td>
<td>Phone:</td>
</tr>
<tr>
<td>Division: CID</td>
<td>Room Number: JEH, 7350</td>
</tr>
<tr>
<td>Phone:</td>
<td></td>
</tr>
<tr>
<td>Room Number: JEH, G-300</td>
<td></td>
</tr>
</tbody>
</table>

FBI DIVISION INTERMEDIATE APPROVALS

<table>
<thead>
<tr>
<th>Program Division: Crimes Against Children Unit</th>
<th>Division Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Date signed: 03/19/12</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Title: Unit Chief</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program Division: Criminal Investigative Division (CID)</th>
<th>Division Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Date signed: 03/19/12</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Title: Assistant Section Chief</td>
<td></td>
</tr>
</tbody>
</table>

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:

_X_ 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 MI0G 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

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:

<table>
<thead>
<tr>
<th>Unit Chief</th>
<th>Signature:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Civil Liberties Unit</td>
<td></td>
</tr>
<tr>
<td>Brian Binney, Acting Deputy General Counsel</td>
<td></td>
</tr>
<tr>
<td>FBI Privacy and Civil Liberties Officer</td>
<td></td>
</tr>
</tbody>
</table>

UNCLASSIFIED//FOR OFFICIAL USE ONLY
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.

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.

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. 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):

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
   ___ YES  [If yes, please continue.]

5. 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.
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.]

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.

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)?
UNCLASSIFIED//FOR OFFICIAL USE ONLY

NO

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?

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.


_____ 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.)]
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.

____ 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.

X  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?
NO  X YES (see above)