X The information can be used to distinguish or trace an individual’s identity (i.e., it is linked or linkable to specific individuals). However, this information is only in the audit logs which are not accessible to the general user.

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  X 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.]

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 (c)(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:

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 PHI 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:
    July 1, 2008
Confidentiality: _Low _Moderate X High _Undefined
Integrity: _Low _Moderate _X High _Undefined
Availability: _Low _Moderate _X High _Undefined

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

10. Does the system conduct data mining as defined in Section 804 of the

  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

  _____ 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? Fall 2001

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.) However, this
change will be reflected in separate privacy documentation (Next Gen SCION).

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

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

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

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

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

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

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

______ Other [Provide brief explanation]:

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

   __ NO       ____ YES

   If yes:

   a. Provide date/title of the PIA:

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

      __ NO       ____ YES
**FBI PRIVACY THRESHOLD ANALYSIS (PTA)**
(equivalent to the DOJ Initial Privacy Assessment (IPA))

<table>
<thead>
<tr>
<th>NAME OF SYSTEM / PROJECT:</th>
<th>Scattered Castles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derived From:</td>
<td></td>
</tr>
<tr>
<td>Classified By:</td>
<td></td>
</tr>
<tr>
<td>Reassess:</td>
<td></td>
</tr>
<tr>
<td>Declassify On:</td>
<td></td>
</tr>
</tbody>
</table>

**SYSTEM/PROJECT POC**
- **Name**: [Redacted]
- Program Office: Information Assurance Technology Infusion
- Division: Security Division
- Phone: [Redacted]
- Room Number: SpyB-601

**FBI OGC/PCLU POC**
- **Name**: [Redacted]
- Phone: [Redacted]
- Room Number: 7338

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

<table>
<thead>
<tr>
<th>Program Division: Security Division</th>
<th>Signature: /s</th>
<th>Date signed:</th>
<th>Name: [Redacted]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Title: Information Assurance Technology Unit Chief</td>
</tr>
<tr>
<td>Program Division: Security Division</td>
<td>Signature: /s</td>
<td>Date signed:</td>
<td>Name: [Redacted]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Title: Information Assurance Technology Unit Chief</td>
</tr>
</tbody>
</table>

| FIBHQ Division: Security Division   | Signature: /s | Date signed: | Name: Michael F.A. Morehart |
|                                     |               |             | Title: Deputy Assistant Director Security Division |
| FIBHQ Division: Security Division   | Signature: /s | Date signed: | Name: Michael F.A. Morehart |
|                                     |               |             | Title: Deputy Assistant Director Security Division |

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

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

1. Signed original to file 190-HQ-C1321794 (fwd to JEH 18204 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) (if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)  
   1. FBI OCG/PCLU intranet  
   1. PCLU UC  
   1. PCLU Library  
   1. PCLU Tickler
2. FBI OCG/PCLU OIPP (JEH 9376, attr [Redacted])
3. FBI SecD/AU (e-mail copy: via e-mail to UC [Redacted])  
   1. RMD/RMAU (attr [Redacted])  
   1. Program Division POC/Privacy Officer  
   1. FBIHQ Division POC/Privacy Officer
**UNCLASSIFIED // FOR OFFICIAL USE ONLY**

**FBI PTA:** Scattered Castles

---

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

- ___ PIA is required by the E-Government Act.
- ___ PIA is to be completed as a matter of FBI/DOJ discretion.

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

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

**Applicable SORN(s):**

- Notify FBI RMD/RIDS per MIOG 190.2.3? ___ No. ___ Yes (see sample EC on PCLU intranet website).

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

1. Provide a general description of the system or project that includes: name of the system/project, including associated acronyms; structure of the system/project, purpose; nature of the information in the system and how it will be used; who will have access to the information in the system and the manner of transmission to all users. (This kind of information may be available in the System Security Plan, if available, or from a Concept of Operations document, and can be cut and pasted here):

The Scattered Castles

[Redacted]

Scattered Castles (SC) is an Intelligence Community (IC) security clearance application hosted on the TS/SCI Joint Worldwide Intelligence Communications System (JWICS). To track clearance and access information for Bureau personnel, the FBI

With the SC

[Redacted]

The SC

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

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

   But as a stand-alone system, SC does not collect, maintain or disseminate PII as contemplated by the Privacy Act.

   _____ YES. [If yes, please continue.] SYSTEM IS INFRASTRUCTURE ONLY. THE FOLLOWING QUESTION ARE NOT APPLICABLE

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

   _____ NO.   _____ YES.
4. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system/project by name or other personal identifier?

_____ NO.  _____ YES.

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

_____ 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 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:

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?

_____ YES.  [If yes, proceed to question 7.]

_____ NO.

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

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

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

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

_____ NO.  If no, indicate reason; if C&A is pending, provide anticipated completion date:
8. Is this system/project the subject of an OMB-300 budget submission?

____ NO. ______ Don't know. ______ YES. If yes, please provide the date and name or title of the OMB submission.

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

____ NO. ______ YES. ______ Don't know.

10. Status of System/Project:

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

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.)

____ 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.
UNCLASSIFIED // FOR OFFICIAL USE ONLY

FBI PTA: Scattered Castle

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

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

7. 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.

8. 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.

[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: Security Access Control System (SACS)  

BIKR FBI Unique Asset ID: SYS-0000078

SYSTEM/PROJECT POC
Name:  
Program Office: Access Control  
Division: Security  
Phone:  
Room Number: 1358, JEH

FBI OGC/PCLU POC
Name:  
Phone:  
Room Number: 7350, JEH

FBI DIVISION INTERMEDIATE APPROVALS

<table>
<thead>
<tr>
<th>Program Division:</th>
<th>Program Manager (or other appropriate executive or Division determines)</th>
<th>Division Privacy Officer</th>
</tr>
</thead>
</table>
| Access Control          | Signature:  
Date signed: 3/18/11  
Name:  
Title: Acting Unit Chief  | Signature:  
Date signed:  
Name:  
Title: Assistant General Counsel |
| FBIHQ Division:         | Signature: Colleen Connolly  
Date signed: 3/18/11  
Name: Colleen Connolly  
Title: Section Chief  | Signature:  
Date signed: 4/12/11  
Name:  
Title: Assistant General Counsel |

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.

epic.org
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 redactions)?  _____ Yes  _____ No:

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

_____ System does not collect, maintain, or disseminate PIL.
_____ 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/ITB/PCLU/PrivacyCivil%20Liberties%20library/form_for_mlog190-2-3_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: Privacy and Civil Liberties Unit</th>
<th>Signature:</th>
</tr>
</thead>
<tbody>
<tr>
<td>James J. Landen, Deputy General Counsel</td>
<td>Date Signed: 9/1/11</td>
</tr>
<tr>
<td>FBI Privacy and Civil Liberties Officer</td>
<td>Signature:</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; and (f) the manner of transmission to all users.

The Security Access Control System (SACS) provides controlled access into the FBI HQ, J. Edgar Hoover building, a subcomponent of the overall SACS system. Since the 2008 privacy documentation, SACS is the only part of SACS that has changed.

The SACS main structure will not change. The main structure will still consist of

Access to SACS will be controlled by unique user accounts and system roles. Only users assigned to the FBI's Access Control Unit (ACU), SACS Administrator and ISSO roles will have access to user account data. Information within SACS is not transmitted to any other agency outside of the FBI. Only FBI personnel will use or access to the system or to the information in the system. SACS
SACS uses access control measures for providing authorized users access to SACS. Essentially, SACS

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.

___ 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 information from the information subject:

Privacy Act (e)(3) statements are [__________] where the information is collected directly from the individual.

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 X YES If yes, check all that apply:

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

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

_____ SSNs are important for other reasons. Describe:

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: SSN's are hidden from view on the main viewing screen.

_______ It is not feasible for the system/project to provide special protection to SSNs. Explain:
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:
August 5, 2011

Confidentiality: ___Low ___Moderate _X_High ___Undefined

Integrity: ___Low _X Moder ate ___High ___Undefined

Availability: ___Low _X Moder ate ___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:

   This is a new system/project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? March 26, 2008

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

   NO [If no, proceed to next question (IL3).]

   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.

   X A change that results in a new use or disclosure of information in identifiable form.
Previously, this information was maintained only in electronic form viewable by select personnel.

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.

X Other [Provide brief explanation]:

ACU will continue to SACS

ACU will also have the ability to

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?

X NO YES
**FBI PRIVACY THRESHOLD ANALYSIS (PTA)**

*(Equivalent to the DOJ Initial Privacy Assessment (IPA))*

**NAME OF SYSTEM / PROJECT:**

<table>
<thead>
<tr>
<th>Derived From:</th>
<th>SYSTEM/PROJECT POC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classified By:</td>
<td>Name: Security Information Database</td>
</tr>
<tr>
<td>Reason:</td>
<td>Program Office: Polygraph Unit</td>
</tr>
<tr>
<td></td>
<td>Division: Security Division</td>
</tr>
<tr>
<td></td>
<td>Phone:</td>
</tr>
<tr>
<td></td>
<td>Room Number: 7350</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FBI OGC/PCLU POC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Phone:</td>
</tr>
<tr>
<td>Room Number: GRB 210</td>
</tr>
</tbody>
</table>

**FBI DIVISION INTERMEDIATE APPROVALS**

<table>
<thead>
<tr>
<th>Program Division: Polygraph Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
</tr>
<tr>
<td>Date signed:</td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Title:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Division Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
</tr>
<tr>
<td>Date signed:</td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Title:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FBIHQ Division: Security Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
</tr>
<tr>
<td>Date signed:</td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Title:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Division Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
</tr>
<tr>
<td>Date signed:</td>
</tr>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Title:</td>
</tr>
</tbody>
</table>

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

(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

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

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

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

1. DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov) (if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)
2. FBI OCIO / OIPP (JEH 9376, attn:
1. FBI SecD/AU (elec. copy; via e-mail to CC
1. RMD/RMAU (attn:
2. Program Division POC /Privacy Officer
2. FBIHQ Division POC /Privacy Officer
UNCLASSIFIED/NOT SENSITIVE

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>PIA is required by the E-Government Act.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PIA is to be completed as a matter of FBI/DOJ discretion.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? X Yes. No (indicate reason): This is a national security system so it will not be published.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PIA is not required for the following reason(s):</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System does not collect, maintain, or disseminate PII.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information in the system relates to internal government operations.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System has been previously assessed under an evaluation similar to a PIA.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No significant privacy issues (or privacy issues are unchanged).</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other (describe):</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Applicable SORN(s): None

Notify FBI RMD/RIDS per MIOG 190.2.3? No X Yes—See sample EC on PCLU intranet website here: http://home/DO/OGC/TLB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miofg190-2-3_ec.wpd

SORN/SORN revision(s) required? No X Yes (indicate revisions needed): New SORN required since data from other agencies will also be stored in this system.

Prepare/revise/add Privacy Act (e)(3) statements for related forms? No X Yes (indicate forms affected): FD-328 – this will need to be revised to indicate that the information may be used for intelligence purposes and also may be shared with government agencies beyond just those responsible for investigating or prosecuting a violation.

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

Other:

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

Signature: 
Date Signed: 7/26/2016
1. INFORMATION ABOUT THE SYSTEM / PROJECT

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

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

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

   ______ YES [If yes, please continue.]
3. Does the system/project pertain only to government employees, contractors, or consultants?

   X NO   YES

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

   NO   YES

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

   NO   YES If yes, check all that apply:

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

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

   SSNs are important for other reasons. Describe:

   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 SSN will be masked so that only the last four digits are visible.

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

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
UNCLASSIFIED/NOT SENSITIVE

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

___ YES [If yes, proceed to question 7.]

___ NO (The primary purpose of this system is to facilitate information sharing; however, the information could be used in the future to support criminal, CT, or FCI investigations or assessments.)

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

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

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

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

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

The system is currently under review by the Information Systems Security Unit with an anticipated completion date of December 2010.

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

_________ Don’t Know.

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

   _____ 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.
UNCLASSIFIED/NOT SENSITIVE

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

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

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

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

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

Other [Provide brief explanation]:

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

   _____ NO   _____ YES

   If yes:

   a. Provide date/title of the PIA:

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

      _____ NO   _____ YES
**FBI PRIVACY THRESHOLD ANALYSIS (PTA)**

**NAME OF SYSTEM / PROJECT:** SIOC

**BIKR FBI Unique Asset ID:** APP-00000098

<table>
<thead>
<tr>
<th>Derived From</th>
<th>SYSTEM/PROJECT POC</th>
<th>FBI OGC/PCLU POC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classified By</td>
<td>Name:</td>
<td>Name:</td>
</tr>
<tr>
<td>Reason:</td>
<td>Program Office: SIOC</td>
<td>Phone:</td>
</tr>
<tr>
<td></td>
<td>Division: CIRG</td>
<td>Room Number: 5370</td>
</tr>
</tbody>
</table>

**FBI DIVISION INTERMEDIATE APPROVALS**

<table>
<thead>
<tr>
<th>Program Division: [insert division name]</th>
<th>Program Manager (or other appropriate executive as Division determines)</th>
<th>Division Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Date signed: 2/14/12</td>
<td>Date signed: 2/17/2012</td>
<td></td>
</tr>
<tr>
<td>Name: Asst. Section Chief</td>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Title:</td>
<td>Title: Analysis Office, SIOC</td>
<td></td>
</tr>
</tbody>
</table>

**FBIHQ Division: [insert division name]**

<table>
<thead>
<tr>
<th>Signature:</th>
<th>Signature:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date signed: 2/14/12</td>
<td>Date signed: 2/17/2012</td>
</tr>
<tr>
<td>Name: Christopher H. Combs</td>
<td>Name:</td>
</tr>
<tr>
<td>Title: Section Chief</td>
<td>Title:</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 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): DOJ/FBI-002, Central Records System (CRS)

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_mlog190-2-3_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 Record keeping Certification and any necessary updates.

Other:

Elizabeth Withnell, Unit Chief
Privacy and Civil Liberties Unit

Signature: ___________________________
Date Signed: _______________________

Brian Briney, (Acting) Deputy General Counsel
(Acting) FBI Privacy and Civil Liberties Officer

Signature: ___________________________
Date Signed: _______________________

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]
I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Strategic Information and Operations Center (SIOC) operates a command center on a 24/7/365 basis to maintain enterprise-wide situational awareness and provide FBI executives with timely notification and dissemination of strategic information. In support of its mission, SIOC employs the [redacted] with access to that limited to members only of that unit and SIOC administrative personnel.

[redacted] contains information relating to the following, all of which is classified at no higher than the SECRET level:
Access to the system is limited to authorized SIOC personnel only, who are granted read/write access, and occasionally to other FBI personnel on an as-needed basis when authorized by SIOC's senior leadership. No outside agency personnel have access to

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

3. 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. [If you checked this item, STOP here after providing the requested description.]

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?

_ X_ NO  [If no, proceed to question 7.]

_____ YES

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

_____ NO
b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (c)(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   X_ YES If yes, check all that apply:

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

SSNs will only be entered into the [ ] when necessary to

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

_____ SSNs are important for other reasons. Describe:

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).

SSN data will only be made available to SIOC staff authorized to access

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

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)?

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

_________________________ is to be reviewed by SecD for potential operation as part of the SecD review and approval will be documented through EC as receiving an Approval for Use (AFU).

___ 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.


_X_ NO

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

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

_X_ YES

12. Status of System/ Project:

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]
II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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?

_X_ NO  _____ YES

A PTA was prepared for this application on July 11, 2008.

If yes:

a. Provide date/title of the PIA:

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

__ NO  ___YES

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

FBI Privacy Threshold Analysis (PTA) Cover Sheet

NAME OF SYSTEM: 

Derived From: 
Classified By:  
Reason:
Declassify On: 

SYSTEM POC  
Name: 
Program Office: Public Access 
Center Unit 
Division: Counterterrorism 
Phone: 
Room Number: 4981  

FBI OGC/PCLU POC  
Name: 
Phone: 
Room Number: 7338

FBI DIVISION APPROVALS. A PIA (and/or PTA) should be prepared/approved by the cognizant program management in collaboration with IT, security, and end-user management and OGC/PCLU. (PIAs/PTAs relating to electronic forms/questionnaires implicating the Paperwork Reduction Act should also be coordinated with the RMD Forms Desk.) If the subject of a PTA/PIA is under the program cognizance of an FBIHQ Division, prior to forwarding to OGC the PTA/PIA must also be referred to the FBIHQ Division for program review and approval, if required by the FBIHQ Division.

Program Division: Counterterrorism  
Program Manager (or other appropriate executive as Division determines) 
Signature: 
Date signed: 
Name: 
Title: 

Division Privacy Officer  
Signature: 
Date signed: 
Name: 
Title: 

Upon Division approval, forward signed hard copy plus electronic copy to OGC/PCLU (JEH Room 7338).

FINAL FBI APPROVAL:

FBI Privacy and Civil Liberties Officer  
Signature: 
Date Signed: 
Name: David C. Larson 
Title: Deputy General Counsel

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

1 - Signed original to 190-HQ-C1321794 
Copies:

1 - DOJ Privacy and Civil Liberties Office-Main Justice, Room 4259  
2 - FBI OCIO / OIPP 
1 - FBI SecD (electronic copy via e-mail) 
2* - Program Division POC /Privacy Officer 
2* - FBIHQ Division POC /Privacy Officer  
(*please reproduce as needed for Program/Division file(s))
FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: 

For efficiency, a system owner or program manager can be aided in making the determination of whether a Privacy Impact Assessment (PIA) is required by conducting and following Privacy Threshold Analysis (PTA).

Whether or not a PIA is required, the system owner/program manager should consult with the FBI Records Management Division (RMD) to identify and resolve any records issues relating to information in the system.

A PTA contains basic questions about the nature of the system in addition to a basic system description. The questions are as follows:

A. General System Description: Please briefly describe:

1. Type of information in the system:
   a. If the system is solely related to internal government operations please provide a brief explanation of the quantity and type of employee/contractor information:

   The information retained by this system is information that is publicly submitted to the "Report a Crime" link found on the FBI public website, www.fbi.gov. In addition to collecting the information provided by the individual submitting a tip:

2. Purpose for collecting the information and how it will be used:

   The information collected is researched and analyzed to determine whether it is relevant to the FBI or other law enforcement agencies. The tips are stored in a database.

3. The system's structure (including components/subsystems):

   The data is maintained on:

4. Means of accessing the system and transmitting information to and from the system:

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

   Only employees assigned to the FBI Public Access Center Unit (PACU) have access to the information stored in the system. The Unit Chief approves all new accounts. is only installed only on PACU computers, therefore access to the system cannot be achieved from outside.
6. Who outside the FBI will have access to the information in the system and controls for ensuring that only authorized persons can access the information:

No one outside the FBI will have access to the system or the information stored on it.

7. Has this system been certified and accredited by the FBI Security Divisions?  X Yes  ___ No

8. Is this system encompassed within an OMB-300?  ___ Yes  ___ No  X Don't Know
   (If yes, please attach copy of latest one.)

I. Was the system developed prior to April 17, 2003?

   X YES  (If "yes," proceed to Question 1.)
   ___ NO  (If "no," proceed to Section II.)

1. Has the system undergone any significant changes since April 17, 2003?
   ___ YES  If "yes," please explain the nature of those changes:

   (Continue to Question 2.)

   X NO  (If "no," the PTA is complete and should be sent to FBI OGC's Privacy and Civil Liberties Unit (PCLU) for review, approval, and forwarding to DOJ's Privacy and Civil Liberties Office. Unless you are otherwise advised, no PIA is required.)

2. Do the changes involve the collection, maintenance, or dissemination of information in identifiable form about individuals?
   ___ YES  (If "yes," please proceed to Question 3.)
   ___ NO  (If "no," the PTA is complete and should be sent to FBI OGC's Privacy and Civil Liberties Unit (PCLU) for review, approval, and forwarding to DOJ's Privacy and Civil Liberties Office. Unless you are otherwise advised, no PIA is required.)

3. Is the system solely related to internal government operations?
   ___ YES  If "yes," is this a Major Information System (as listed on OGC's FBINET website)?:
   ___ Yes  (If "yes," a full PIA is required. PTA is complete.)
FBI DIVISION APPROVALS. A PIA (and/or PTA) should be prepared/approved by the cognizant program management in collaboration with IT, security, and end-user management and OGC/PCLU. (PIAs/PTAs relating to electronic forms/questionnaires implicating the Paperwork Reduction Act should also be coordinated with the RMD Forms Desk.) If the subject of a PTA/PIA is under the program cognizance of an FBIHQ Division, prior to forwarding to OGC, the PTA/PIA must also be referred to the FBIHQ Division for program review and approval, if required by the FBIHQ Division.

Upon Division approval, forward signed hard copy plus electronic copy to OGC/PCLU (JEH Room 7338).

**FINAL FBI APPROVAL:**

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

1. Signed original to 190-HQ-C1321794

Copies:

1. DOJ Privacy and Civil Liberties Office-Main Justice, Room 4259
2. FBI OCIO / OIPP
1. - FBI SecD (electronic copy via e-mail)
2*. - Program Division POC / Privacy Officer
2*. - FBIHQ Division POC / Privacy Officer

(*please reproduce as needed for Program/Division file(s))
A. General System Description: Please briefly describe:

1. Type of information in the system:

   The SIOC Daily Log contains various miscellaneous information to include, but not limited to:
   - Receipt and dissemination of Urgent Reports, National Center of Missing and Exploited Children Reports, and Law Enforcement Death Notifications. Log entries may contain some names and other identifiers.
   - Shift personnel on duty
   - Contact numbers for traveling FBI Executives and Agents
   - Any domestic or international event/crisis where the FBI has jurisdiction, an interest, or assistance has been requested by local authorities or OGAs.
   - Taskings for each SIOC shift/personnel (i.e. secured/unsecured conferencing bridges, Director's Briefing Materials, SVTS, etc.)
   - Tasks completed by SIOC staff (i.e. Teletypes reviewed, NCIC checks, TEC checks, and ACS or IDW checks conducted for Legal Offices). The log entry may capture names and other personal identifiers.

   a. If the system is solely related to internal government operations please provide a brief explanation of the quantity and type of employee/contractor information:

2. Purpose for collecting the information and how it will be used:

   The SIOC Daily Log is an informal internal FBI document utilized by the SIOC staff to record domestic and international occurrences/events/crises that the FBI has a vested interest in.

3. The system's structure (including components/subsystems):
4. Means of accessing the system and transmitting information to and from the system:

SIIOC staff members can only access the SIIOC Daily Log through the secure FBI Intranet site. Information is entered into the log via the SIIOC web-page wherein access to the log is restricted to SIIOC personnel only.

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

Only SIIOC staff members have been granted access and the ability to enter information in the SIIOC Daily Log. SIIOC controls who has access to the log.

6. Who outside the FBI will have access to the information in the system and controls for ensuring that only authorized persons can access the information:

Currently no agency or personnel outside the FBI have access to the SIIOC Daily Log.

7. Has this system been certified and accredited by the FBI Security Divisions? X Yes ___ No

8. Is this system encompassed within an OMB-300? ___ Yes ___ No X Don't Know

(If yes, please attach copy of latest one.)

I. Was the system developed prior to April 17, 2003?

X YES (If “yes,” proceed to Question 1.)

___ NO (If “no,” proceed to Section II.)

1. Has the system undergone any significant changes since April 17, 2003?

___ YES If “yes,” please explain the nature of those changes:

(Continue to Question 2.)
X NO (If “no,” the PTA is complete and should be sent to FBI OGC’s Privacy and Civil Liberties Unit (PCLU) for review, approval, and forwarding to DOJ’s Privacy and Civil Liberties Office. Unless you are otherwise advised, no PIA is required.)

2. Do the changes involve the collection, maintenance, or dissemination of information in identifiable form about individuals?

_____ YES (If “yes,” please proceed to Question 3.)

_____ NO (If “no,” the PTA is complete and should be sent to FBI OGC’s Privacy and Civil Liberties Unit (PCLU) for review, approval, and forwarding to DOJ’s Privacy and Civil Liberties Office. Unless you are otherwise advised, no PIA is required.)

3. Is the system solely related to internal government operations?

_____ YES If “yes,” is this a Major Information System (as listed on OGC’s FBINET website)?:

_____ Yes. (If “yes,” a full PIA is required. PTA is complete.)

_____ No. (If “no,” the PTA is complete and should be sent to FBI OGC’s Privacy and Civil Liberties Unit (PCLU) for review, approval, and forwarding to DOJ’s Privacy and Civil Liberties Office. Unless you are otherwise advised, no PIA is required. (FBI and DOJ reviewing officials reserve the right to require a PIA.))

_____ NO (If “no,” go to section III to determine if a full or short-form PIA is required.)

II. For systems developed after April 17, 2003.

1. What is the purpose of the system? (Answer in detail unless details already provided in A. 2 above):

(Continue to Question 2.)

2. Does the system collect, maintain or disseminate information in identifiable form about individuals?

_____ YES (If “yes,” please proceed to Question 3.)

_____ NO (If “no,” the PTA is complete and should be sent to FBI OGC’s Privacy and Civil Liberties Unit (PCLU) for review, approval, and forwarding to DOJ’s Privacy and Civil Liberties Office. Unless you are otherwise advised, no PIA is required.)

3. Is the system solely related to internal government operations?
FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: ________________

BIKR FBI Unique Asset ID: ________________

<table>
<thead>
<tr>
<th>Derived From:</th>
<th>SYSTEM / PROJECT POC</th>
<th>FBI OGC / PCLU POC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classified By:</td>
<td>Name: Program Office: Language Services Sec</td>
<td>Name:</td>
</tr>
<tr>
<td>Reason:</td>
<td>Division: Directorate of Intelligence</td>
<td></td>
</tr>
<tr>
<td>Declassify On:</td>
<td>Phone:</td>
<td>Room Number:</td>
</tr>
<tr>
<td>Room Number:</td>
<td>WB-603</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Program Division:</th>
<th>Program Manager (or other appropriate executive as Division determines)</th>
<th>Division Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>[insert division name]</td>
<td>Date signed: [Signature]</td>
<td>Date signed: [Signature]</td>
</tr>
<tr>
<td></td>
<td>Name:</td>
<td>Name:</td>
</tr>
<tr>
<td></td>
<td>Title:</td>
<td>Title:</td>
</tr>
</tbody>
</table>

FBI HQ Division: Directorate of Intelligence

<table>
<thead>
<tr>
<th>Signature:</th>
<th>Date signed: 11/18/15</th>
<th>Name: Amy L. Pepper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title:</td>
<td>Section Chief - Language Services</td>
<td>Title: Superv Mgmt/Program Analyst</td>
</tr>
</tbody>
</table>

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC / PCLU (J6H 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: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PTA drafter should skip to the next page and continue.]

___ PIA is required by the E-Government Act.

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

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

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).

___ System is related 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):

[Signature]

Applicable SORN(s):

.Notify FBI RMD/RIDS per MIG 190.2.3? ___ No ___ Yes ___ See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_mig190-2-3_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):

[Signature]

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:

[Signature]

Date Signed: 6/29/12

Deputy General Counsel
FBI Privacy and Civil Liberties Officer
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. (This kind of information may be available in the System Security Plan, if available, or from a Concept of Operations document, and can be cut and pasted here.):

   The [redacted] resides on a restricted access SharePoint teamsite. The Language Services Section (LSS), Directorate of Intelligence (DI), has a requirement to open the site to all authenticated FBINet users. The project will proceed in two phases.

Phase 1

Phase 1 will [redacted] The data will reside in a SharePoint [redacted]. In this phase, [redacted] will only be made available to [redacted] (employees and contractors), managers and supervisors across the field and at headquarters. Access to the data will allow LSS to

The first step in the Phase 1 rollout will be to instruct all [redacted] to update [redacted] within a 45-day time period. At that time, [redacted] will be presented with the standard Privacy Act notice, as required by 5 U.S.C. § 552a(e)(2), along with a note explaining that this data may be made accessible to all FBI users at a later date. The Privacy Act notice below appears on the

After the 45-day update period, any records that have not been updated will be deleted from the system under the assumption that the users do not agree to have their personal data included in the system.
UNCLASSIFIED

It is noted that during the first 45 days of the Phase I rollout, legacy data collected
without the Privacy Act notice) will be viewable by all
Although SharePoint allows any user to suggest edits of
these edits must be approved by owners, and
or their designees) before being accepted in the system and becoming
visible to other users. To ensure data integrity, the owners will only
approve changes to an that have been submitted by the

Phase II

After the completion of Phase I, the SharePoint site will be made accessible to all
authenticated users on FBINet. Providing access to this data will

The homepage contains the standard Privacy Act notice and will include a statement that all personal information provided by
the user will be accessible to all authenticated FBINet 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 [If no, STOP. The PTA is now complete and after division approval(s)
should be submitted to FBI OGC/PCLU for final FBI approval. Unless you are
otherwise advised, no PIA is required.]

☒ 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.

☐ 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. [If you checked this item,
STOP here after providing the requested description.]

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

   NO   X   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 (c)(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).] Future users will be presented with the Privacy Act statement, but legacy data was obtained without this notification. See 1.1 above for details.

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

      The homepage contains the standard Privacy Act notice.

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.
UNCLASSIFIED

X 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:

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 PHI 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)?

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

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

NOTE: The __________ isn’t a system but rather a teamsite that resides individual Intranet sites do not go through C&A.

Provide date of last C&A certification/re-certification: Contact WSSU, ITSID

UNCLASSIFIED
UNCLASSIFIED

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 SecDef)?

   _X_ NO  _____ YES

13. Status of System/Project:

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

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.