

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  YES

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

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

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

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

NO [If no, proceed to question 7.]

YES

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

NO

YES [If yes, proceed to question 7.]

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

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

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

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

NO  YES If yes, check all that apply:

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

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

SSNs are important for other reasons. Describe:

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

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

Integrity:  Low  Moderate  High  Undefined

Availability:  Low  Moderate  High  Undefined

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

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

NO

YES If yes, please describe the data mining function:

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

NO

YES

12. Status of System/ Project:

This is a new system/ project in development.

## II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? Fall 2001

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.) 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))

NAME OF SYSTEM / PROJECT: Scattered Castles [redacted] b7E

Derived From: Classified By: Reason: Declassify On:	<b>SYSTEM/PROJECT POC</b>	<b>FBI OGC/PCLU POC</b>
	Name: [redacted]	Name: [redacted]
	Program Office: Information Assurance Technology Infusion	Phone: [redacted]
	Division: Security Division Phone: [redacted] Room Number: SpyB-601	Room Number: 7338

b6  
b7C

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

	Program Manager: Security Division	Division Privacy Officer: Security Division
Program Division: Security Division	Signature: /s Date signed: Name: [redacted] Title: Information Assurance Technology Unit Chief	Signature: /s Date signed: Name: [redacted] Title: Information Assurance Technology Unit Chief
FBIHQ Division: Security Division	Signature: /s Date signed: Name: Michael F.A. Morehart Title: Deputy Assistant Director Security Division	Signature: /s Date signed: Name: Michael F.A. Morehart Title: Deputy Assistant Director Security Division

b6  
b7C

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

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

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

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

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

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

- 1 - OGC/PCLU intranet
- 1 - PCLU UC
- 1 - PCLU Library
- 1 - PCLU Tickler

b6  
b7C

FBI PTA: Scattered Castles

b7E

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

PIA is required by the E-Government Act.

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

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

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

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

FBI PTA: Scattered Castles [redacted]

b7E

David C. Larson, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: /s/ David C. Larson 3/3/2010
--	---

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 al 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]

[redacted]

[redacted] SC [redacted] enables the FBI to [redacted] personnel security clearance data, [redacted]

[redacted]

b7E

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 [redacted]

[redacted]

b7E

With the SC [redacted]

[redacted]

b7E

The SC [redacted]

[redacted]

b7E

[redacted]

b7E

FBI PTA: Scattered Castles [redacted]

b7E

[redacted]

b7E

The SC [redacted] that provides access to each SC [redacted]  
SC [redacted]

b7E

[redacted] within the SC [redacted]  
[redacted] The SC [redacted]  
[redacted] the SC [redacted]  
and SC [redacted] The SC [redacted] the SC [redacted]  
[redacted] This SC [redacted]  
[redacted] the SC [redacted]  
[redacted] Thus no PII remains on the SC [redacted] following  
[redacted]

b7E

No general users will have access to SC [redacted] Only privileged users with TS/SCI clearances will have log-on access to SC [redacted]

b7E

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

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

b7E

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

...X... 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.



FBI PTA: Scattered Castles

b7E

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 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:**

FBI PTA: Scattered Castles

b7E

..... 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?

..... 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.

FBI PTA: Scattered Castles

b7E

- ..... 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.

[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) [REDACTED]

b7E

BIKR FBI Unique Asset ID: SYS-0000078

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: [REDACTED]	Name: [REDACTED]
Program Office: Access Control	Phone: [REDACTED]
Division: Security	Room Number: 7350, JEH
Phone: [REDACTED]	
Room Number: 1358, JEH	

b6  
b7C

#### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Access Control	Signature: [REDACTED] Date signed: 8/18/11 Name: [REDACTED] Title: Acting Unit Chief	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: Assistant General Counsel [REDACTED]
FBIHQ Division: Security Division	Signature: <i>Colleen Conyngham</i> Date signed: 8/18/11 Name: Colleen Conyngham Title: Section Chief	Signature: [REDACTED] Date signed: 8/18/11 Name: [REDACTED] Title: Assistant General Counsel

b6  
b7C

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



UNCLASSIFIED

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

PIA is required by the E-Government Act.

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

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

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

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

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



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

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

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

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

Other:

<input type="checkbox"/> Unit Chief Privacy and Civil Liberties Unit	Signature:  Date Signed:
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature:  Date Signed: 9/11/11

b6  
b7C

UNCLASSIFIED

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

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

b7E

[redacted]

The SACS [redacted]

[redacted]

b7E

The main structure of SACS will not change [redacted]  
[redacted] The main structure will still consist of [redacted]

[redacted]

b7E

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. [redacted]

[redacted] 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 [redacted]

b7E

[redacted] SACS uses access control measures for providing authorized users access to SACS. Essentially, SACS [redacted]

b7E

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

\_\_\_\_\_ NO

X  YES [If yes, please continue.]

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

X  The information directly identifies specific individuals.

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

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

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

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

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

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

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

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

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

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

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

YES

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:

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

b7E

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: 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?

No.

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

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

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

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

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

August 5, 2011

Confidentiality:  Low  Moderate  High  Undefined

Integrity:  Low  Moderate  High  Undefined

Availability:  Low  Moderate  High  Undefined

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

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

NO

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

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

NO

YES If yes, please describe the data mining function:

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

NO  YES

13. Status of System/ Project:

This is a new system/ project in development.

## II. EXISTING SYSTEMS / PROJECTS

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

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

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

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

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

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

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

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

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

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

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

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

[Redacted]

b7E

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.

Other [Provide brief explanation]:

ACU will continue to [Redacted] SACS [Redacted]

[Redacted]

[Redacted] ACU will also have the ability to [Redacted]

b7E

[Redacted]

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))

<b>NAME OF SYSTEM / PROJECT:</b> [REDACTED]		
<b>Derived From:</b>	<b>SYSTEM/PROJECT POC</b>	<b>FBI OGC/PCLU POC</b>
<b>Classified By:</b>	Name: Security Information Database	Name: [REDACTED]
<b>Reason:</b>	Program Office: Polygraph Unit	Phone: [REDACTED]
<b>Declassify On:</b>	Division: Security Division	Room Number: 7350
	Phone: [REDACTED]	
	Room Number: GRB 210	

b3  
b7E  
b6  
b7C

#### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager	Division Privacy Officer
<b>Program Division:</b> Polygraph Unit	Signature: [REDACTED] Date signed: 10/26/2010 Name: [REDACTED] Title: Unit Chief	Signature: [REDACTED] Date signed: 11/02/10 Name: [REDACTED] Title: Division Privacy Officer
<b>FBIHQ Division:</b> Security Division	Signature: [REDACTED] Date signed: 10/26/2010 Name: [REDACTED] Title: Unit Chief	Signature: [REDACTED] Date signed: 10/27/10 Name: [REDACTED] Title: Division Privacy Officer

b6  
b7C

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

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

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

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

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

b6  
b7C



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.)

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):  
This is a national security system so it 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 (describe):

Applicable SORN(s): None

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


SORN/SORN revision(s) required?  No  Yes (indicate revisions needed): 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  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: 1/13/2010

UNCLASSIFIED/NOT SENSITIVE

**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

b3  
b7E

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

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

  X   YES [If yes, please continue.]

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

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 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

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:

b3  
b7E

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?

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 FTA is now complete and after division approval(s) should be submitted to FBI OGC/PCLU for final FBI approval and determination if FIA 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.

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

UNCLASSIFIED/NOT SENSITIVE

### FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: SIOC [redacted]

b3  
b7E

BIKR FBI Unique Asset ID: APP-0000092

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [redacted]	Name:
Reason:	Program Office: SIOC	Phone:
Declassify On:	Division: CIRG	Room Number:
	Phone: [redacted]	
	Room Number: 5370	

b6  
b7C

#### FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: [insert division name]	Signature: [redacted] Date signed: 2/15/12 Name: [redacted] Title: Asst. Section Chief	Signature: [redacted] Date signed: 2/17/2012 Name: [redacted] Title: DIVISION PRIVACY OFF, CIRG
FBIHQ Division: [insert division name]	Signature: [Signature] Date signed: 2/15/12 Name: Christopher H. Combs Title: Section Chief	Signature: Date signed: Name: Title:

b6  
b7C

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



[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

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

<p><input type="checkbox"/> PIA is required by the E-Government Act.</p> <p><input checked="" type="checkbox"/> PIA is to be completed as a matter of FBI/DOJ discretion.</p> <p>Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? <input checked="" type="checkbox"/> Yes. <input type="checkbox"/> No (indicate reason):</p> <p><input type="checkbox"/> PIA is not required for the following reason(s):</p> <ul style="list-style-type: none"><li><input type="checkbox"/> System does not collect, maintain, or disseminate PII.</li><li><input type="checkbox"/> System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).</li><li><input type="checkbox"/> Information in the system relates to internal government operations.</li><li><input type="checkbox"/> System has been previously assessed under an evaluation similar to a PIA.</li><li><input type="checkbox"/> No significant privacy issues (or privacy issues are unchanged).</li><li><input type="checkbox"/> Other (describe):</li></ul>	
<p>Applicable SORN(s): <u>DOJ/FBI-002, Central Records System (CRS)</u></p> <p>Notify FBI RMD/RIDS per MIOG 190.2.3? <input type="checkbox"/> No <input checked="" type="checkbox"/> Yes--See sample EC on PCLU intranet website here: <a href="http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd">http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd</a></p> <p>SORN/SORN revision(s) required? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes (indicate revisions needed):</p>	
<p>Prepare/revise/add Privacy Act (e)(3) statements for related forms? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes (indicate forms affected):</p>	
<p>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.</p>	
<p>Other:</p>	
<p>Elizabeth Withnell, Unit Chief Privacy and Civil Liberties Unit</p>	<p>Signature: Date Signed:</p>
<p>Brian Binney, (Acting) Deputy General Counsel (Acting) FBI Privacy and Civil Liberties Officer</p>	<p>Signature: <i>Elizabeth Withnell</i> Date Signed: <i>9/13/12</i></p>

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]



[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

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

1. Provide a general description of the system or project that includes: (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]

b3  
b7E

[REDACTED]

[REDACTED]

b3  
b7E

[REDACTED] with access to that [REDACTED] limited to members only of that unit and SIOC administrative personnel.

[REDACTED]

b3  
b7E

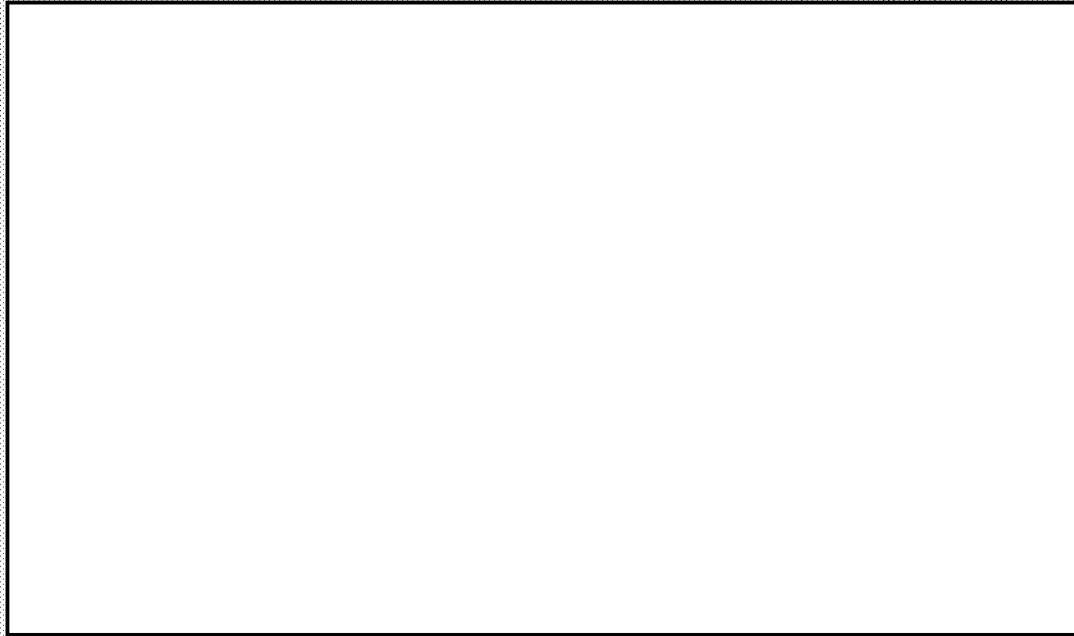
[REDACTED] contains information relating to the following, all of which is classified at no higher than the SECRET level:

b3  
b7E

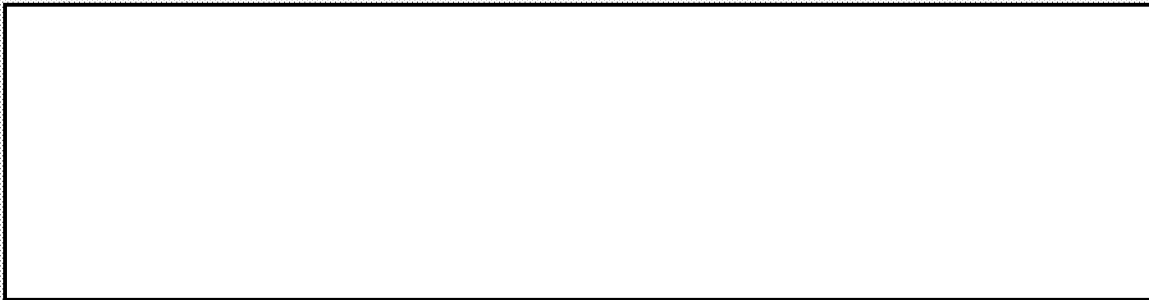
[REDACTED]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]



b3  
b7E




b3  
b7E



b3  
b7E



b3  
b7E

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.]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

YES [If yes, please continue.]

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

(Check all that apply.)

The information directly identifies specific individuals.

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

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

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

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

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

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

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 will only be entered into the  when necessary to

b3  
b7E

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).

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

b3  
b7E

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

8. Is the system operated by a contractor?

No.

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

\_\_\_\_ 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:

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).

b3  
b7E

\_\_\_\_ YES If yes, please indicate the following, if known:

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

Confidentiality:  Low  Moderate  High  Undefined

Integrity:  Low  Moderate  High  Undefined

Availability:  Low  Moderate  High  Undefined

\_\_\_\_ Not applicable -- this system is only paper-based.

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

NO

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

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

NO

YES

12. Status of System/ Project:

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]



[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

\_\_\_\_\_ 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?

b3  
b7E

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.

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

\_\_\_\_\_ 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

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.]

[INSERT CLASSIFICATION/CONTROL MARKINGS,  
IF APPROPRIATE]

[UNCLASSIFIED]

FBI Privacy Threshold Analysis (PTA) Cover Sheet

(OGC/PCLU (Rev. 05/02/07))

NAME OF SYSTEM: [REDACTED]

Derived From:	<b>SYSTEM POC</b>	<b>FBI OGC/PCLU POC</b>
Classified By:	Name: [REDACTED]	Name: [REDACTED]
Reason:	Program Office: Public Access	Phone: [REDACTED]
Declassify On:	Center Unit	Room Number: 7338
	Division: Counterterrorism	
	Phone: [REDACTED]	
	Room Number: 4981	

b7E

b6  
b7C

**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	FBIHQ Division: Counterterrorism
Program Manager (or other appropriate executive as Division determines)	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]	Signature: [REDACTED] Date signed: 6/2/2008 Name: [REDACTED] Title: Unit Chief
Division Privacy Officer	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]	Signature: [REDACTED] Date signed: 6/2/2008 Name: [REDACTED] Title: Unit Chief

b6  
b7C

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: [Handwritten Signature] Date Signed: 7/1/08 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
- 1 - OGC/PCLU intranet website
- 1 - PCLU UC
- 1 - PCLU Library
- 1 - PCLU Tickler

(\*please reproduce as needed for Program/Division file(s))

[UNCLASSIFIED]



[UNCLASSIFIED]

**FBI PRIVACY THRESHOLD ANALYSIS (PTA)**

NAME OF SYSTEM: [REDACTED]

b7E

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 publically submitted to the "Report a Crime" link found on the FBI public website, [www.fbi.gov](http://www.fbi.gov). In addition to collecting the information provided by the individual submitting a tip [REDACTED]

b7E

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 a [REDACTED]

b7E

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

[REDACTED]

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. [REDACTED] is only installed only on PACU computers, therefore access to the system cannot be achieved from outside

[UNCLASSIFIED]

[UNCLASSIFIED]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: [REDACTED]

b7E

the unit.

[REDACTED]

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?  Yes  No

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

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

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.)

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.)

[UNCLASSIFIED]

[INSERT CLASSIFICATION/CONTROL MARKINGS]

FBI Privacy Threshold Analysis (PTA) Cover Sheet (OGC/PCLU (Rev. 05/02/07))

NAME OF SYSTEM: [insert both here and in header next page] *SIOC Watch Log*

Derived From:	<b>SYSTEM POC</b>	<b>FBI OGC/PCLU POC</b>
Classified By:	Name: [redacted]	Name: [redacted]
Reason:	Program Office: <i>SIOC</i>	Phone: [redacted]
Declassify On:	Division: <i>C186</i>	Room Number: <i>7338</i>
	Phone: [redacted]	
	Room Number:	

b6  
b7C

**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: [insert division name]	FBIHQ Division: [insert division name]
Program Manager (or other appropriate executive as Division determines)	Signature: [redacted] Date signed: <i>6-26-2008</i> Name: [redacted] Title: <i>Asst</i>	Signature: <i>Ethel L. McGuire</i> Date signed: <i>6/26/08</i> Name: <i>Ethel L. McGuire</i> Title: <i>Section Chief</i>
Division Privacy Officer	Signature: [redacted] Date signed: [redacted] Name: [redacted] Title: [redacted]	Signature: [redacted] Date signed: <i>7/1/08</i> Name: [redacted] Title: <i>PRIVACY OFFICER / LDC</i>

b6  
b7C

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: <i>David C. Larson</i> Date Signed: <i>7/1/08</i> Name: <i>David C. Larson</i> Title: <i>Deputy General Counsel</i>
---	---

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
- 1 - OGC/PCLU intranet website
- 2 - FBI OCIO / OIPP
- 1 - PCLU UC
- 1 - FBI SecD (electronic copy via e-mail)
- 1 - PCLU Library
- 2\* - Program Division POC /Privacy Officer
- 1 - PCLU Tickler
- 2\* - FBIHQ Division POC /Privacy Officer

(\*please reproduce as needed for Program/Division file(s))

[INSERT CLASSIFICATION/CONTROL MARKINGS]

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.

[Redacted]

- 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.)

[Redacted]

[Redacted]

- Tasks completed by SIOC staff (i.e. Teletypes reviewed, NCIC checks, TEC checks, and ACS or IDW checks conducted for Legat Offices). The log entry may capture names and other personal identifiers.

[Redacted]

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.

[Redacted]

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

[Redacted]

b7E

b7E

b7E



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

SIOC staff members can only access the SIOC Daily Log through the secure FBI intranet site. Information is entered into the log via the SIOC web-page wherein access to the log is restricted to SIOC 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 SIOC staff members have been granted access and the ability to enter information in the SIOC Daily Log. SIOC 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 SIOC Daily Log.

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

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

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

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

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.)

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)


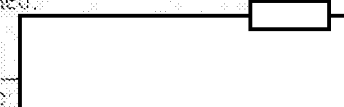
NAME OF SYSTEM/ PROJECT:  b7E

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

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: <input type="text"/> Program Office: Language Services Sec Division: Directorate of Intelligence Phone: <input type="text"/> Room Number: WB-603	FBI OGC/PCLU POC Name: Phone: Room Number:
--	--	---

b6  
b7C

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

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Directorate of Intelligence	Signature:  Date signed: 11/19/2013 Name: Amy L. Pepper Title: Section Chief - Language Services	Signature:  Date signed: 11/28/2013 Name: <input type="text"/> Title: Supv Mgmt/Program Analyst

b6  
b7C

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

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

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

PIA is required by the E-Government Act.

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

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

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

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

Other (describe):

*Please put this document on the [redacted] website to send to the PCLU's site.*

Applicable SORN(s): 025-FBI-002

Notify FBI RMD/RIDS per MIOG 190.2.3?  No  Yes--See sample EC on PCLU intranet website here: [http://home/DO/OGC/LTB/PCLU/Privacy/Civil%20Liberties%20Library/form\\_for\\_mlog190-2-3\\_ec.wpd](http://home/DO/OGC/LTB/PCLU/Privacy/Civil%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)G3 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. AUSTIN*  
Deputy General Counsel  
FBI Privacy and Civil Liberties Officer

Signature:

Date Signed:

*[Handwritten Signature]*  
*6/29/12*

[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. (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.):

[Redacted]

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 FBI Net users. [Redacted] project will proceed in two phases.

b7E

Phase I

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

b7E

The first step in the Phase I rollout will be to instruct all [Redacted] to update [Redacted] within a 45-day time period. [Redacted] At that time, [Redacted] will be presented with the standard Privacy Act notice, as required by 5 U.S.C. § 552a(e)(3), 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 [Redacted]

b7E

[Redacted]

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 [redacted] [redacted] (without the Privacy Act notice) will be viewable by all [redacted] [redacted]. Although SharePoint allows any user to suggest edits of [redacted] these edits must be approved by [redacted] owners [redacted] and [redacted] (or their designees) before being accepted in the system and becoming visible to other users. To ensure data integrity, the [redacted] owners will only approve changes to an [redacted] that have been submitted by the [redacted]

b7E

Phase II

After the completion of Phase I, the SharePoint site will be made accessible to all authenticated users on FBI Net. Providing access to this data will [redacted] [redacted] [redacted]. The [redacted] 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 FBI Net users.

b7E

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

       NO [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 PTA 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.

       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

UNCLASSIFIED

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

NO  YES

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

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

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

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

NO [If no, proceed to question 7.]

YES

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

NO

YES [If yes, proceed to question 7.]

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

NO [The program will need to work with PCLU to develop/implement the necessary form(s).] Future users will be presented with the Privacy Act statement, but legacy data was obtained without this notification. See I.1 above for details.

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

The  homepage contains the standard Privacy Act notice.

b7E

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

UNCLASSIFIED

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 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:

NOTE: The [redacted] isn't a system but rather a teamsite that resides [redacted]  
Individual intranet sites do not go through C&A.

b7E

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

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.

UNCLASSIFIED

UNCLASSIFIED

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

NO

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

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

NO

YES If yes, please describe the data mining function:

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

NO  YES

13. Status of System/ Project:

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

UNCLASSIFIED