

UNCLASSIFIED

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

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

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

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

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

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

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

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

_____ Other [Provide brief explanation]:

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

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

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

_____ NO _____ YES

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

UNCLASSIFIED

UNCLASSIFIED//FOUO



(OGC/PCLU (Rev. 08/19/2013))

b3
b7E

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

b3
b7E

BIKR FBI Unique Asset ID: NET-0000073

Derived From: SSP, 30 Dec 2014 Classified By: E52M26K53 Reason: Declassify On: 20391231 <i>DOCUMENT IS NOT CLASSIFIED</i>	SYSTEM/PROJECT POC Name: Technical Architect Program Office: Data Center Hardware & OS Section Division: ITID Phone: Room Number: CHY-102	FBI OGC/PCLU POC Name: AGC Phone: Room Number: 7350 JEH
--	---	---

b3
b6
b7C
b7E

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: Information Technology Applications and Data Division (ITAD)	Signature: Date signed: 6/11/14 Name: David J. Bukovich Title: Section Chief, Intelligence and Investigative Applications Section	Signature: Date signed: 6/11/2014 Name: ITS Title: ITID/VCSU Privacy Officer
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

UNCLASSIFIED//FOUO



b3
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.

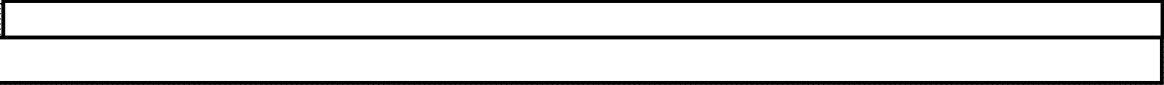
System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).

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).

Other:



b3
b7E

Applicable SORN(s): Department of Justice Computer Systems Activity and Access Records, DOJ-002, published at 64 Fed. Reg. 73585 (Dec. 30, 1999).

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

SORN/SORN revision(s) required? No Yes

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

Form FD-889, *FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form*, provides a Privacy Act Statement of users of FBI IT systems. All FBI personnel with access to FBI IT systems must electronically sign form FD-889 as part of their annual INFOSEC training.

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:



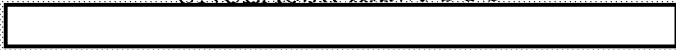
Unit Chief, Privacy and Civil Liberties Unit
FBI Privacy and Civil Liberties Officer

Signature
Date Sig



6/25/14

b6
b7C



I. INFORMATION ABOUT THE SYSTEM / PROJECT

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





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.]

b3
b7E

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

(Check all that apply.)

The information directly identifies specific individuals.

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

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

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

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

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

NO

YES

b3
b7E

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.]

b3
b7E

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 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 was last accredited on March 15, 2012 and has authority to operate (ATO) through March 22, 2015 at the following risk levels:

Confidentiality: Low Moderate High

Integrity: Low Moderate High

Availability: Low Moderate High

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. [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? 2004
2. Has the system/project undergone any significant changes since April 17, 2003?

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



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

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

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

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

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

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

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

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

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

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

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

X Other [Provide brief explanation]:



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

X NO YES

If yes:

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

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

NO YES

[The PIA 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:

b7E

BIKR FBI Unique Asset ID: SYS-0000090

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: <input type="text"/>	Name: <input type="text"/>
Reason:	Program Office: Investigative	Phone: <input type="text"/>
Declassify On:	Applications Support Unit (INVASU)	Room Number: 7350 JEH
	Division: ITSD	
	Phone: <input type="text"/>	
	Room Number: 1333B JEH	

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: Critical Incident Response Group (CIRG)	Signature: <input type="text"/> Date signed: 4/26/11 Name: <input type="text"/> Title: Deputy Commander, Hostage Rescue Team (HRT)	Signature: <input type="text"/> Date signed: 4/26/2011 Name: <input type="text"/> (CIRG) Title: Chief Division Counsel
FBIHQ Division: IT Services Division (ITSD)	Signature: <input type="text"/> Date signed: 4/13/2011 Name: <input type="text"/> Title: Acting Section Chief, System Support Section (SSS)	Signature: <input type="text"/> Date signed: 4-13-11 Name: <input type="text"/> Title: Information Technology Specialist

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: [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):

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

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

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):

Privacy Act (e)(3) statements will be prepared to accompany medic cards and deployment sheets provided to personnel from whom information is collected and will be stored within TRMS.

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

Other:

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

Signature: 

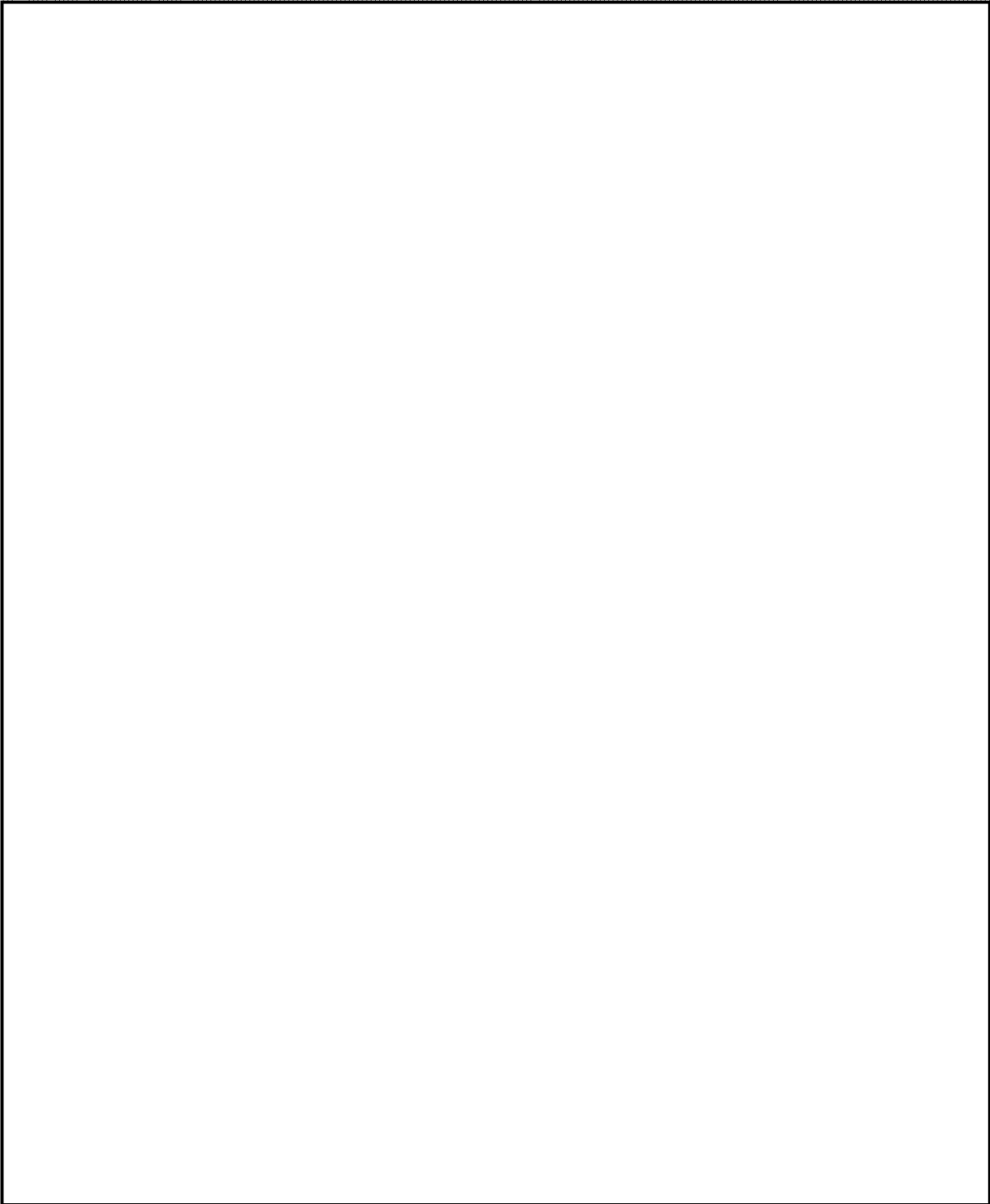
Date Signed: 7/11/11

[UNCLASSIFIED]

[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.



b7E

[UNCLASSIFIED]



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.]

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.]

[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.]

b7E

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

b7E

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

NO

YES [If yes, proceed to question 7.]

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

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

b7E

[UNCLASSIFIED]



_____ 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:

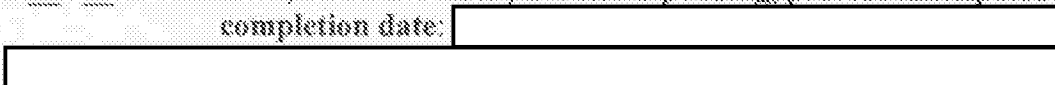
8. Is the system operated by a contractor?

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 PII and additional requirements may be imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

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

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





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

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

Confidentiality: ___Low___Moderate ___High ___Undefined

Integrity: ___Low___Moderate ___High ___Undefined

Availability: ___Low___Moderate ___High ___Undefined

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

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

___X___ NO

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

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

___X___ NO

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

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

___X___ NO _____ YES

13. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? FY2005-2006

[UNCLASSIFIED]

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):
The system was DEVELOPED and IMPLEMENTED post-April 17, 2003.

_____ 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.

Explanation: Content will be accessible through a new application that provides for additional features. This will take the form of a new repository for information on individuals 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.

[UNCLASSIFIED]

[UNCLASSIFIED]

_____ 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 PIA 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)

NAME OF SYSTEM / PROJECT:

b3
b7E

BIKR FBI Unique Asset ID: Proj2013-014-01

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: 	Name: AGC
Reason:	Program Office: Strategic Technology Unit	Phone:
Declassify On:	Division: Directorate of Intelligence	Room Number: 7350
	Phone: 	
	Room Number: 11079-M	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: <i>Amy L. Sareeram</i>	Signature:
Directorate of Intelligence	Date signed: <i>2/7/14</i>	Date signed: <i>2/6/2014</i>
	Name: Amy L. Sareeram	Name:
	Title: Section Chief, Strategic Services Section	Title: Privacy Officer

b6
b7C

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

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.

A PIA was conducted for the Secret version of FIDS- dated 9/19/2011. TS FIDS is consistent with the Secret FIDS PIA.

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

Other (describe):

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

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


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:

Unit Chief
Privacy and Civil Liberties Unit
Privacy and Civil Liberties Officer

Signature: 
Date Signed: 2/7/14

b6
b7c

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

Name of the system/project, including associated acronyms:

b3
b7E

Purpose of the system/project:

Structure of the system/project, including interconnections with other projects or systems:

b3
b7E

Nature of the information in the system and how it will be used:

b3
b7E

Who will have access to the information in the system?

Manner of transmission to all users:

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

NO [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. 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

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:**

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.

_____ 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**

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:

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 changes that apply, and provide brief explanation for each marked change**):

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

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

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

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

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

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

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

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

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

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

_____ Other [**Provide brief explanation**]:

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

_____ NO _____ YES

If yes:

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

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

___ NO ___ YES

[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 // FOR OFFICIAL USE ONLY
FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Terrorist Screening Center Network (TSCNET)

BIKR FBI Unique Asset ID: Sys-0000183

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [Redacted] Program Office: TSC II Division: TSDC Phone: [Redacted] Room Number: 3176	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number: 3346
--	---	---

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: TSC II	Signature: [Redacted] Date signed: 4/14/12 Name: [Redacted] Title: Program Manager	Signature: [Redacted] Date signed: [Redacted] Name: [Redacted] Title: [Redacted]
FBIHQ Division: TSC II	Signature: [Redacted] Date signed: 4/14/12 Name: [Redacted] Title: IT Branch Chief	Signature: [Redacted] Date signed: 4/14/12 Name: [Redacted] Title: TSC Privacy Officer

b6
b7C

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

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

PIA is required by the E-Government Act.

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

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? Yes. No (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): TSCNet is a Windows network environment designed to host and provide connectivity to other systems; significant applications will be described in subsequent privacy documentation on an as-needed basis.

Applicable SORN(s): N/A

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

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

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

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

Other:

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

Signature:

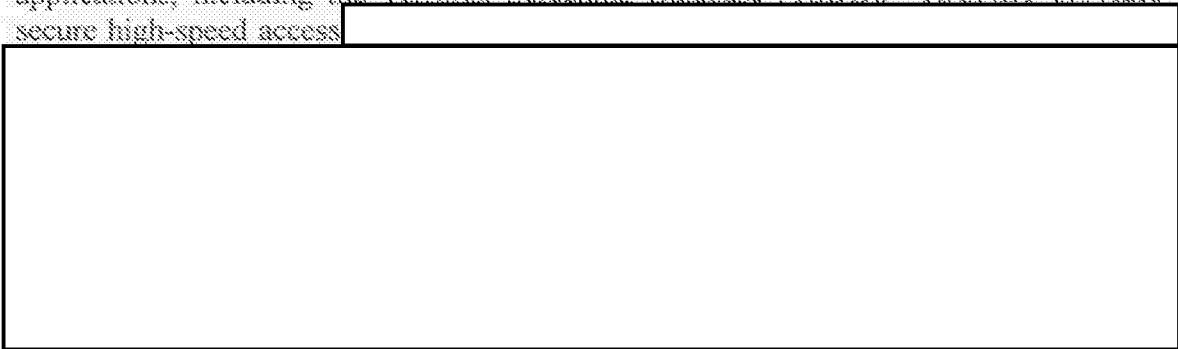
Date Signed: 4/19/12

UNCLASSIFIED // FOR OFFICIAL USE ONLY

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Terrorist Screening Center Network (TSCNET) is an unclassified windows network environment designed to host and provide connectivity to other systems. TSCNET provides the Terrorist Screening Center (TSC) with access to unclassified networks so that personnel can use Federal Bureau of Investigation (FBI) mission essential applications, including the Terrorist Screening Database (TSDB). TSCNET provides secure high-speed access

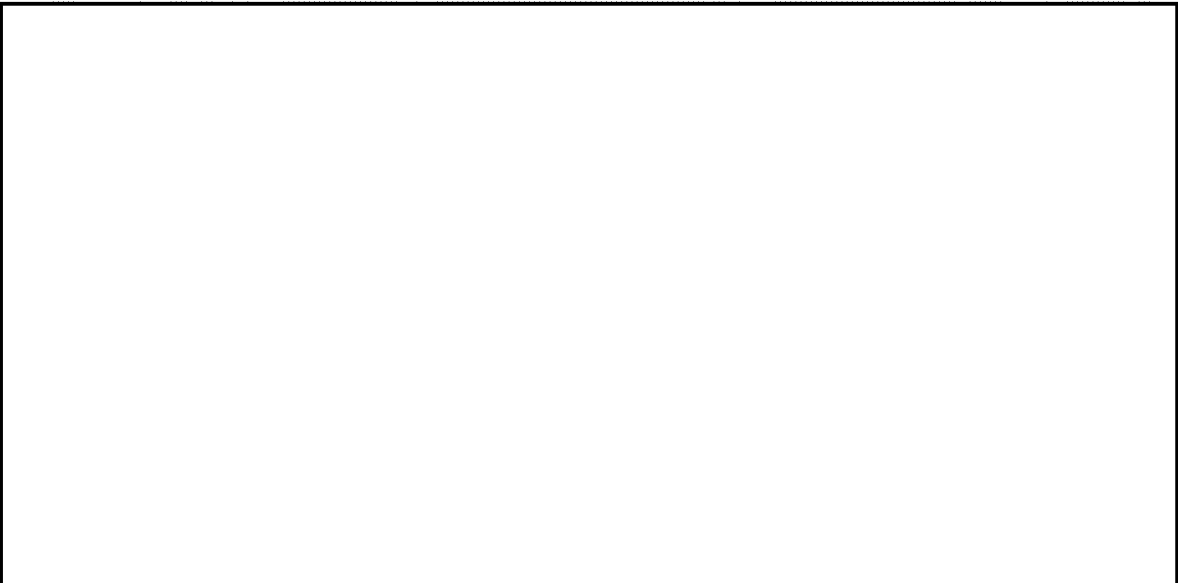


b7E

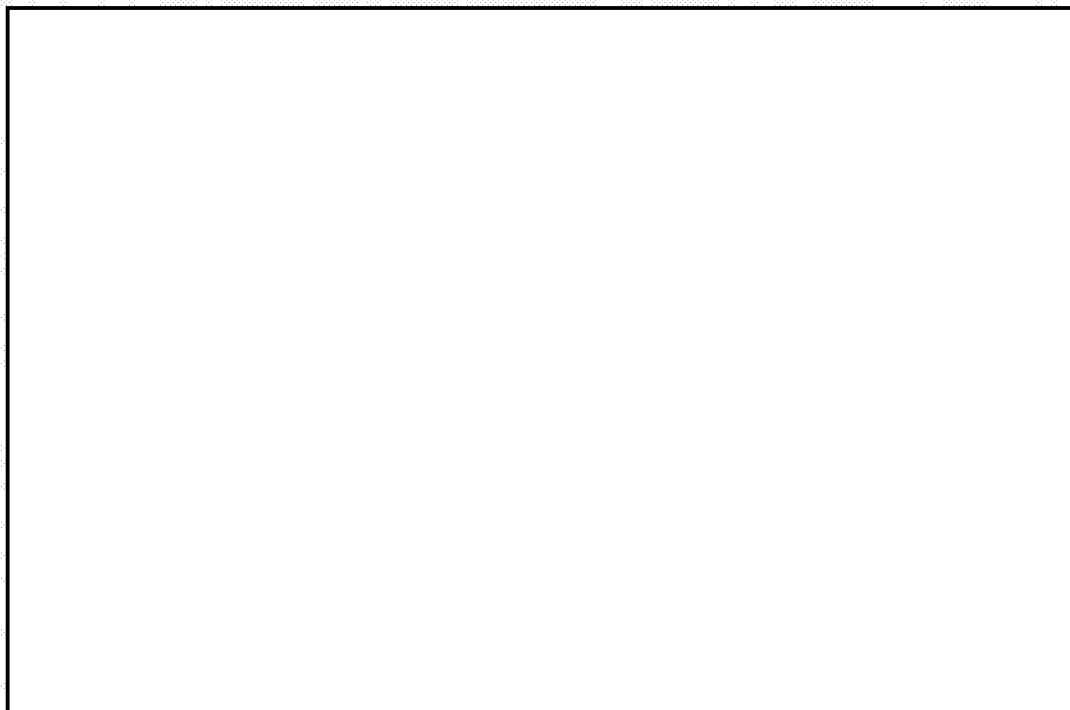
TSCNet access is restricted to cleared FBI/TSC personnel. TSCNET does not allow



b7E



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.]

*TSCNet collects audit log and general logon information. Other types of PII collected, maintained, or disseminated by TSCNet will be described in the privacy documentation associated with the specific application that performs such function.

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).

UNCLASSIFIED // FOR OFFICIAL USE ONLY

*TSCNet collects audit log and general logon information. Other types of PII collected, maintained, or disseminated by TSCNet will be described in the privacy documentation associated with the specific application that performs such function.

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.] Don't we get the log-on info from the user?

..... 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).]

UNCLASSIFIED // FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

_____ 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 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.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

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: March 02, 2010

Confidentiality: ___ Low ___ Moderate ___ High ___ Undefined

Integrity: ___ Low ___ Moderate ___ High ___ Undefined

Availability: ___ Low ___ Moderate ___ High ___ Undefined

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

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

_____ NO

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

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

_____ NO

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

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

_____ NO

_____ YES

13. Status of System/ Project:

_____ This is a new system/ project in development. [If you checked this block, STOP. The PTA is now complete and after division approval(s) should be

UNCLASSIFIED // FOR OFFICIAL USE ONLY

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? April 2005
2. Has the system/project undergone any significant changes since April 17, 2003?

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

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

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

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

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

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

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

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

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

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

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

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

_____ Other [Provide brief explanation]:

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

NO YES

If yes:

a. Provide date/title of the PIA:

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

NO YES

[The PIA 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.]

(OGC/PCLU (Rev. 05/15/09))

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

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: Technical Management Services Unit (TMSU) Division: Operational Technology Division (OTD) Phone: <input type="text"/> Room Number: ERF, B-221	FBI OGC/PCLU POC Name: <input type="text"/> Phone: <input type="text"/> Room Number: 7350 JEH
--	---	---

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: Operational Technology Division (OTD)	Signature: Date signed: Name: <input type="text"/> Title: Unit Chief, Technical Management Services Unit (TMSU)	Signature: Date signed: Name: Patrick N. DeVall Title: Section Chief, Technical Program Section
FBIHQ Division: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

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

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

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

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

b6
b7C

SENSITIVE BUT 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 (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): N/A

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

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:

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

Signature:
Date Signed: /s/ 7/19/2010

SENSITIVE BUT UNCLASSIFIED

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1 [redacted] is composed of the FBI, and security agencies [redacted]

b7E

[redacted] The Operational Technology Division (OTD) is the FBI host and sponsor of this network. [redacted]

[redacted]

[redacted]

b7E

- A. Type of FBI employee/contractor information stored includes:
 - a. The full name of the FBI participants, both employee and contractors
 - b. Internet Protocol (IP) address of the workstation they are logging into;

- B. Purpose for collecting the information and how it will be used:
 - a. For security auditing purposes only

~~(S)~~ (U)

[redacted]

b1
b3
b7E

[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 are the definition of personally identifiable information (PII))?

NO [If no, STOP. The PIA 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?

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:**

____ 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]

___X___ YES, but only log-on and password information

a. Does the system/project support criminal, CT, or FCI investigations or assessments? It provides a means of sharing technical information that might lead to possible improvements in current collection system designs.

___X___ 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:**

YES **If yes, provide date of last C&A certification/re-certification:**
04/09/2008

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? 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 boxes that apply)**:

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

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

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

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

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

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

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

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

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

_____ 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]:

b7E

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

NO PTA 5/16/2007

b7E

YES Previous

If yes:

a. Provide date/title of the PIA:

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

NO YES No change that would impact privacy.

[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

(OGC/PCLU (Rev. 04/01/2011))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Uniform Crime Reporting Redevelopment Project (UCRRP)

BIKR FBI Unique Asset ID: 2009-056-01-P-115-046-3367

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [Redacted]	Name: [Redacted]
Reason:	Program Office: UCRRP	Phone: [Redacted]
Declassify On:	Division: CJIS Division, Information Technology Management Section (ITMS)	Room Number:
	Phone: [Redacted]	
	Room Number: Module B-2	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature:	Signature:
	Date signed:	Date signed:
	Name:	Name:
	Title: [Redacted]	Title: [Redacted]
FBIHQ Division: CJIS Division	Signature: [Redacted]	Signature: [Redacted]
	Date signed: September 3, 2015	Date signed: 9/3/2015
	Name: [Redacted]	Name: [Redacted]
	Title: UCR Program Manager/Chief, Crime Statistics Management Unit (CSMU)	Title: CJIS Division Privacy Officer - Supervisory IT Specialist

b6
b7C

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 :

UNCLASSIFIED

Applicable SORN(s): <u>Central Records System</u>	
Notify FBI RMD/RIDS per MIOG 190.2.3? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd	
SORN/SORN revision(s) required? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes	
Prepare/revise/add Privacy Act (e)(3) statements for related forms? <input checked="" type="checkbox"/> No <input type="checkbox"/> 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:	
<div style="border: 1px solid black; width: 100px; height: 20px; display: inline-block;"></div> Unit Chief Privacy and Civil Liberties Unit FBI Privacy and Civil Liberties Officer	Signature:  Date Signed: 12/4/13

b6
b7C

UNCLASSIFIED

L. 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 Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division Uniform Crime Reporting (UCR) Program is a collective effort on the part of federal, state, local, and tribal law enforcement agencies to present a nationwide view of crime. Law Enforcement Agencies (LEAs) throughout the country participating in the FBI UCR Program provide crime statistics related to offenses known to law enforcement and reports on persons arrested. These offenses are defined according to criteria established by the FBI's UCR Program. Congressional mandates and through coordination with the law enforcement community via the CJIS Advisory Policy Board (APB). The data is currently compiled/published on a semi-annual and annual basis. Agencies also provide Hate Crime statistical data and aggregate Law Enforcement Officers Killed and Assaulted (LEOKA) information, and the number of full-time law enforcement employees. All statistical data submitted to the UCR Program is provided without Personally Identifiable Information (PII).



In addition to the aggregate LEOKA data mentioned above, there is separate, detailed LEOKA data that is collected by the UCR Program via paper-based forms that contain PII. The New UCR system will store both the aggregate statistical LEOKA data and the additional detailed LEOKA data. The additional detailed LEOKA data contains information about the victim officer that was assaulted or killed during the incident being reported. This data includes the officer's name, rank, total law enforcement experience, date of birth, gender, race, height, weight, and circumstances surrounding the incident. [REDACTED]

b7E

[REDACTED]



[REDACTED]

The intent of the FBI UCR Redevelopment Project (UCRRP) effort is to meet user need by:

- Creating a centralized, searchable data repository for internal FBI stakeholders. *Note: Only designated LEOKA staff will be given access to the LEOKA PII data. The PII data is collected and stored for research purposes only and is not included in the resulting research product publications or training. The NARA has agreed to allow the LEOKA system PII data to be stored indefinitely for research purposes.*
- Establishing UCR interoperability between the FBI and law enforcement data contributors via the Law Enforcement Enterprise Portal (LEEP). The user access information that is exchanged between LEEP and UCR to ensure system access privileges within UCR includes the following data elements: user name, user id, user group(s), e-mail address, phone number, password.
- 
- 
- Provide a web-based interface for State Programs and direct contributing LEAs to submit data via the LEEP
- Provide a web-based interface for State Programs to manage their data via the LEEP
- Creating an external web-based portal for statistical data for public use. *Note: there will be no access to the LEOKA PII data via this portal.*

b7E

For the purposes of this document, the resulting system from the UCRRP will be referred to as the New UCR System.


 Data will be submitted to the New UCR System through a variety of means: web services, email, and manual data entry.

b7E



b7E

The New UCR system will also maintain an externally viewable database with crime statistics data cleared for public release. This publicly accessible, external database called the UCR Crime Data Explorer (UCR CDE), will not contain LEOKA Program PII data.

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

UNCLASSIFIED

_____ NO

YES [If yes, please continue.]

The New UCR system will store the following LEOKA PII data, but this data will not be able to be pushed to UCR CDE and will only be accessible by internal FBI LEOKA staff:

- Victim Officer's Name
- Victim Officer's Date of Birth

-
-
-
-

- Narrative of Incident (May contain PII if entered by the submitting LEA in the Narrative)

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

The information directly identifies specific individuals.

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

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

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

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

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

NO _____ YES

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

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

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

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

UNCLASSIFIED

UNCLASSIFIED

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?

UNCLASSIFIED

UNCLASSIFIED

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: The system is still under development. C&A will be performed as a part of the UCRRP and is expected to be completed by January 5, 2014.

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.