

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED] National Intellectual Property Rights Coordination Center
(IPR Center) [REDACTED]

b7E

BIKR FBI Unique Asset ID: N/A [REDACTED]

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: MPA [REDACTED] Office: Intellectual Property Rights Unit Division: Criminal Investigative Phone: [REDACTED] Room Number: IPRC, Crystal City	FBI OGC/PCLU POC Name: AGC [REDACTED] Phone: [REDACTED] Room Number: 7350 JEH
--	--	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Criminal Investigative Division	Signature: [REDACTED] Date signed: 6/25/13 Name: SSA [REDACTED] Title: Unit Chief, Intellectual Prop. Rights Unit	Signature: [REDACTED] Date signed: 6/25/13 Name: SMPA [REDACTED] Title: Unit Chief, CID Executive Staff

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:

<p><input type="checkbox"/> PIA is required by the E-Government Act.</p> <p><input 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 type="checkbox"/> Yes. <input type="checkbox"/> No (indicate reason):</p> <p><input checked="" type="checkbox"/> PIA is not required for the following reason(s):</p> <ul style="list-style-type: none"><input type="checkbox"/> System does not collect, maintain, or disseminate PII.<input type="checkbox"/> System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).<input type="checkbox"/> Information in the system relates to internal government operations.<input type="checkbox"/> System has been previously assessed under an evaluation similar to a PIA.<input type="checkbox"/> No significant privacy issues (or privacy issues are unchanged).<input checked="" type="checkbox"/> Other: The IPR Center SharePoint site is not an FBI information technology (IT) asset. See comments section below.	
<p>Applicable SORN(s): <u>U.S. Immigration and Customs Enforcement, External Investigations System of Records, DHS/ICE -- 009, 75 Fed. Reg. 23274 (Jan. 5, 2010)</u></p> <p>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</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 Recordkeeping Certification and any necessary updates.</p> <p>Other:</p> <p>The DHS/ICE manages the IPR Center: </p> <div style="border: 1px solid black; width: 800px; height: 30px; margin-top: 5px;"></div>	
<div style="border: 1px solid black; width: 100px; height: 20px; display: inline-block;"></div> Unit Chief Privacy and Civil Liberties Unit	Signature: <div style="border: 1px solid black; width: 150px; height: 20px; display: inline-block;"></div> Date Signed: <u>6/27/13</u>
Christine M. Costello, Acting Deputy General Counsel and FBI Privacy and Civil Liberties Officer	Signature: <u>[Signature]</u> Date Signed: <u>6/27/13</u>

b7E


b6
b7C

~~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.

Established in 1999, the mission of the National Intellectual Property Rights Coordination Center (the IPR Center) is to ensure national security by protecting the public's health and safety, the U.S. economy, and to stop predatory and unfair trade practices that threaten the global economy. Restructured in July, 2008, the IPR Center now brings together more than twenty investigative agencies involved in the federal enforcement of intellectual property (IP) laws in a task force setting. Partner agencies include the FBI, U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection, the U.S. Postal Inspection Service, the U.S. Patent and Trademark Office, the Nuclear Regulatory Commission, along with other investigative and regulatory agencies.

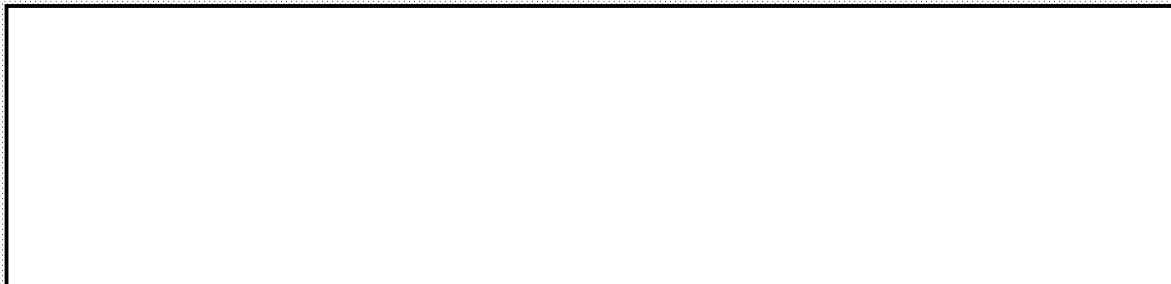


b7E

Individuals and entities wishing to report a possible IP crime may do so by filing an online complaint at www.iprcenter.gov, by calling the IPR Center Tip Line, by emailing iprcenter@dhs.gov, or by contacting one of the Center's partner agencies.



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 FTA 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:**

_____ 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. 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 SecDY)?

_____ NO

_____ YES

12. Status of System/ Project:

_____ This is a new system/ project in development. [If you checked this block, STOP. 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.]

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 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.]

~~SECRET~~

CLASSIFIED BY NSICG/C32W33B91
REASON: 1.4 (C)
DECLASSIFY ON: 11-04-2039
DATE: 11-04-2014

(OGC/PCLU (Rev. 08/16/2010))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

b3

b7E

BIKR FBI Unique Asset ID: 2009-034-01-P-113-215-9999

Derived From: FBI NSISCG-06152009	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: <input type="text"/>	Name: <input type="text"/>
Reason:	Program Officer: CNSS	Phone: <input type="text"/>
Declassify On: 20351013	Division: Cyber (16)	Room Number: JEH, Rm 7350
	Phone: <input type="text"/>	
	Room Number: Westfields 4F33	

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: Cyber Division	Signature: <i>Peter Trahon</i> Date signed: 11/04/10 Name: Peter Trahon Title: Section Chief	Signature: Date signed: Name: Title:
FBIHQ Division: Cyber Division	Signature: <i>Peter Trahon</i> Date signed: 11/04/10 Name: Peter Trahon Title: Section Chief	Signature: Date signed: Name: Title:

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.)

~~SECRET~~

~~SECRET SORN~~

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):

☐ is a National Security system and as such, it will not be published.

b3
b7E

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

_____ System does not collect, maintain, or disseminate PI.

_____ 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): CRS, FBI-092

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_mio190-2-3_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:

Elizabeth Withnell, Acting Deputy General Counsel
FBI Privacy and Civil Liberties Officer

Signature:
Date Signed:

Elizabeth Withnell 12/19/10

~~SECRET SORN~~

~~SECRET//NOFORN~~

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.



b1
b3
b7E



b1 (S)
b3 (S)
b7E



b1
b3
b7E



(S)
b1
b3
b7E

¹ Derived from National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive (HSPD), *Cyber Security*, 23 dated 8 January 2008

~~SECRET//NOFORN~~

~~SECRET NOFORN~~

(S)

b1
b3
b7E

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

☐ NO [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?

~~SECRET NOFORN~~

~~SECRET NOFORN~~

☒ 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:

~~SECRET NOFORN~~

~~SECRET//NOFORN~~

_____ 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.

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

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

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

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

Provide date of last C&A certification/re-certification: 7/1/2010

Confidentiality: ___Low___Moderate X High ___Undefined

Integrity: ___Low___ X Moderate ___High___Undefined

Availability: ___Low___ X Moderate ___High___Undefined

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

~~SECRET//NOFORN~~

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

☒ NO (However, it is the subject of an Exhibit 53 budget submission.)

☐ 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 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.

~~SECRET//NOFORN~~

(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.]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

CLASSIFIED BY NSICG/C32W33B91
REASON: 1.4 (C)
DECLASSIFY ON: 01-30-2040
DATE: 01-30-2015

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

(equivalent to the DOJ Initial Privacy Assessment (IPA))

NAME OF SYSTEM / PROJECT: [REDACTED] b3 b7E		
Derived From: Multiple Sources Classified By: Program Manager Reason: Sources/Methods Declassify On: TBD	SYSTEM/PROJECT POC Name: [REDACTED] Program Office: [REDACTED] Division: WMDD Phone: [REDACTED] Room Number: 6387	FBI OGC/PCLU POC Name: [REDACTED] Phone: [REDACTED] Room Number: [REDACTED]

b6
b7C
b7E

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: WMDD	Signature: [REDACTED] Date signed: 9/14/10 Name: [REDACTED] Title: SSA	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]
FBIHQ Division: WMDD	Signature: [REDACTED] Date signed: 8/14/10 Name: [REDACTED] Title: Unit Chief	Signature: [REDACTED] Date signed: [REDACTED] 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)
(if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530) | 1 - OGC/PCLU intranet |
| 2 - FBI OCIO / OIPP (JEH 9376, attn: [REDACTED]) | 1 - PCLU UC |
| 1 - FBI SecD/AU (elec. copy: via e-mail to UC [REDACTED]) | 1 - PCLU Library |
| 1 - RMD/RMAU (attn: [REDACTED]) | 1 - PCLU Tickler |
| 2 - Program Division POC /Privacy Officer | |
| 2 - FBIHQ Division POC /Privacy Officer | |

b6
b7C

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FBI PTA:

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 (describe):

National Security System

Applicable SORN(s): U65 - FBI - D02

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:

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

Signature:
Date Signed:

Christopher R. ... 9/30/10

b3
b7E

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FBI PTA:

b3
b7E

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.

(S) b1
b3
b7E

b1
b3
b7E

b1
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?

_____x_____ NO. _____ YES.

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

_____ NO. _____x_____ YES.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FBI PTA: ☐

b3
b7E

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:

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

☐ Don't Know.

b3
b7E

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FBI PTA:

b3
b7E

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.]

~~SECRET//NOFORN~~

~~SECRET~~

(OGC/PCLU (Rev. 07/06/2010))

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

NAME OF SYSTEM / PROJECT: [REDACTED]

(S)

b1
b3
b7E

BIKR FBI Unique Asset ID: N/A

Derived From: Classified By: FBI NSISCG - 20080301 Reason: Declassify On: 20350714	SYSTEM/PROJECT POC Name: Special Agent [REDACTED] Program Office: Squad CD-5 Division: Los Angeles Phone: [REDACTED] Room Number: 5318 JEH	FBI OGC/PCLU POC Name: AGC [REDACTED] Phone: [REDACTED] Room Number: 7350 JEH
---	--	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Los Angeles Field Office	Signature: Date signed: Name: [REDACTED] Title: Supervisory Special Agent, CI-7	Signature: Date signed: Name: [REDACTED] Title: Chief Division Counsel
FBIHQ Division: Counterintelligence	Signature: Date signed: Name: [REDACTED] Title: Unit Chief, [REDACTED]	Signature: Date signed: Name: [REDACTED] Title: Supervisory Special Agent

b6
b7C
b7E

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.)

~~SECRET~~

~~SECRET//NF~~

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS

____ PIA is required by the E-Government Act.

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

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

The contents of the [] PIA will be classified; it is therefore not feasible to publish the PIA.

b3
b7E

____ 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): Central Records System (CRS), Justice/FBI-002

Notify FBI RMD/RIDS per MIOG 190.2.3? ____ No X Yes--See sample EC on PCLU intranet website here:
http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

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

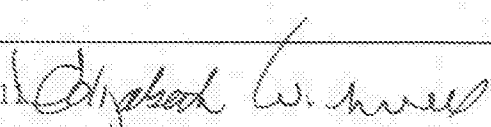
Prepare/revise/add Privacy Act (e)(3) statements for related forms? ____ No ____ Yes (indicate forms affected):
N/A

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:

Elizabeth Ross Withnell
Acting Deputy General Counsel and
FBI Privacy and Civil Liberties Officer

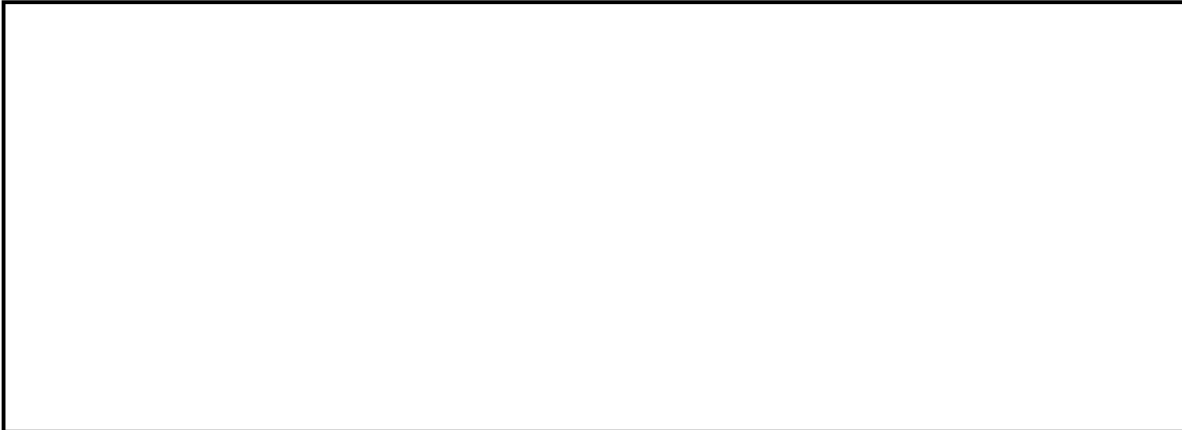
Signature: /s/
Date Signed: 1/11/2011



~~SECRET//NF~~

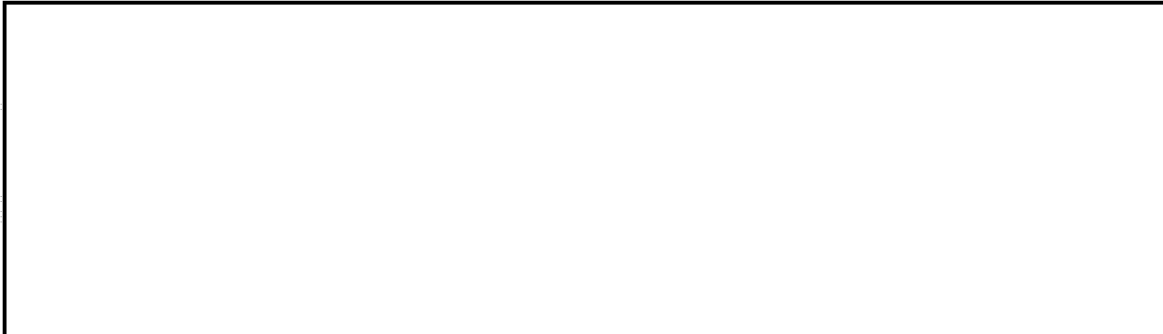
I. INFORMATION ABOUT THE SYSTEM / PROJECT

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.

A large rectangular black box used for redaction, covering the first major section of the document.

(S)

b1
b3
b7E

A large rectangular black box used for redaction, covering the second major section of the document.

b1
b3
b7E

A large rectangular black box used for redaction, covering the third major section of the document.

b1
b3
b7E

A rectangular black box used for redaction, covering the fourth major section of the document. A small 'X' mark is visible in the top-left corner of the box.

b1
b3
b7E

[Redacted]

(S)

b1
b3
b7E

[Redacted]

b1
b3
b7E

[Redacted]

(S)

b1
b3
b7E

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

_____ NO

 X YES

[Redacted]

(S)

b1
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).

☐ 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 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 project by name or other personal identifier?

☐ NO.

☒ YES.

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

☒ NO

☐ YES

The FBI does not collect information [redacted] as part of

[redacted]

(S)

b1
b3
b7E

a. Does the 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 project? Full SSNs should only be used as identifiers in limited instances.

_____ NO X YES

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

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

 X SSNs are important for other reasons.

(S)

b1
b3
b7E

 X The 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:

(S) b1
b3
b7E

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

8. Is the project operated by a contractor?

 X No.

_____ Yes. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates PII and additional requirements may be

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

9. Has the project 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:

(S)

b1
b3
b7E

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 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 project 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:

(S)

b1
b3
b7E

(S)

b1
b3
b7E

b7E

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

NO

☒ YES

13. Status of Project:

☒

This is a new project in development.

b7E

III/ EXISTING SYSTEMS / PROJECTS

When was the system/project developed?

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

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

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.

~~SECRET/NF~~

_____ 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.]

~~SECRET/NF~~

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Form Rev. 9/9/08

CHECKLIST FOR PRIVACY COMPLIANCE FOR
FBI ROUTINE DATABASES
(including comparable applications)

NAME OF SYSTEM / PROJECT: [REDACTED]

b7E

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: IT Specialist [REDACTED]	Name: AGC [REDACTED]
Reason:	Program Office: ATSU	Phone: [REDACTED]
Declassify On:	Division: ITSD	Room Number: 7350 JEH
	Phone: [REDACTED]	
	Room Number: 1376 JEH	

b6
b7C

This checklist is based on the FBI Privacy Impact Assessment (PIA) for FBI Routine Databases of 4/7/08 as approved 8/29/08 (190-HQ-C1321794 Serial 432, 9/8/08). In accordance with the PIA, this checklist may be used in lieu of any additional PIA (or PTA), so long as every one of the twelve blocks below can be checked. This checklist should be completed by the database manager (or other appropriate official/ as determined by the division) and approved by the Division Privacy Officer.

A. Provide date checklist prepared: March 29, 2011

B. 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.

[REDACTED]
[REDACTED] is installed on
individual central processing units (CPUs) and operates on the Secret Enclave. [REDACTED]

b7E

[REDACTED]

[REDACTED]

b7E

UNCLASSIFIED//FOR OFFICIAL USE ONLY

[redacted] it does not contain the actual names of individual users or specific personal identifiers. It does, however, contain limited personally identifiable information (PII) consisting of user names, IP addresses and inventory property numbers of CPUs [redacted]

b7E

[redacted] resides on the Secret Enclave and is presently undergoing certification and accreditation.

C. Complete checklist (all must be checked as being accurate for this database/application):

- X 1. Information in the system identifies individuals, either directly or indirectly. An individual can be identified indirectly through a combination of descriptors such as gender, race, birth data, geographic indicator, license number, or license plate number.¹
- X 2. The system derives information from FBI records covered by existing Privacy Act system of records notices (http://foia.fbi.gov/rec_sys.htm) regardless of format in which those records are maintained and/or from information that is publicly available at no cost. (If information comes from FBI records that are not covered by existing systems of records notices, contact the PCLU.)
- X 3. Neither commercial data nor paid subscription service data is included in the database unless that information is derived from existing FBI records.
- X 4. The system can be accessed only by members of a particular office, unit, squad or other similar FBI entity and sharing of information is based strictly on an operational need to know.
- X 5. The system is not used for purposes of pattern-based data mining.
- X 6. Initial and continued access to the system is subject to permission controls enforced by FBI supervisory personnel, including the use of access passwords.
- X 7. Access to the system can be audited.
- X 8. The system is part of an established platform on which a Security Certification and Accreditation has been performed.
- X 9. The system was developed after April 17, 2003.²
- X 10. If the system maintains information about U.S. citizens or legal permanent residents, it is covered by a published Privacy Act System of Records Notice.

¹ Systems that do not contain any personally identifiable information need not complete this checklist.

² Systems developed before April 17, 2003, and not modified since then are not required to conduct a PIA until a modification occurs that would change the privacy risks to information in the system.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

X 11. Records retention issues have been discussed with the Records Management Division.

X 12. Any personally identifiable information placed on a mobile device or on media that is transported outside FBI facilities must comply with the FBI policy on encryption and must be password protected.

D. If a database contains information that may be considered sensitive/controversial or is maintained as part of a larger FBI program, the database administrator or program manager (or division privacy officer) must consult with the FBI's Office of the General Counsel, Privacy and Civil Liberties Unit about the potential need to assess the privacy risks in a separate PIA.

E. File Notes (summarize any additional information that may be warranted for record purposes, e.g., coordination with OGC, etc.):

APPROVING OFFICIALS

Program Manager (or other appropriate official as division determines)	Division Privacy Officer
Signature: [Redacted]	Signature: [Redacted]
Date signed: 3/1/11	Date signed: 4-1-11
Name: [Redacted]	Name: [Redacted]
Title: Unit Chief, Analytical Tools Support Unit	Title: IT Specialist, Information Technology Branch

b6
b7C

DISTRIBUTION:

- File signed original (or copies) in one or more official division/program files for documentation, inspection, records, and other oversight purposes.
- Forward copy to the FBI Privacy and Civil Liberties Unit (PCLU) (JEH 7350).

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1272295-0

Total Deleted Page(s) = 1
Page 5 ~ b7E;

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)         X
X   No Duplication Fee      X
X   For this Page           X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

FBI Privacy Threshold Analysis (PTA) Cover Sheet (OGC/PCLU (Rev. 1/17/07))

NAME OF SYSTEM: [REDACTED]

b7E

FBI SYSTEM CONTACT PERSON

Name: [REDACTED]

Program Office: OCIO

Division: IT Operations

Phone: [REDACTED]

Room Number: 1334

Date PTA submitted for approval: 9/5/2008

PCLU POC: [REDACTED]
JEH 7338

b6
b7C

FBI DIVISION APPROVALS

	Program Division:	FBIHQ Division: IT Operations
Program Manager (or other appropriate executive as Division determines)	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]	Signature: [REDACTED] Date signed: 9/5/2008 Name: [REDACTED] Title: IT Specialist
Division Privacy Officer	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]	Signature: [REDACTED] Date signed: 9/23/08 Name: [REDACTED] Title: Asst. Section 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: [REDACTED] Date Signed: 10/26/08 Name: Patrick W. Kelley Title: Deputy General Counsel
---	--

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

1 - Original signed copy to 190-HQ-C1321794

Copies:

1 - DOJ Privacy and Civil Liberties Office-Main Justice, Room 4259

1 - FBI OCIO

1 - FBI SecD (electronic copy via e-mail)

2* - Program Division POC /Privacy Officer

2* - FBIHQ Division POC /Privacy Officer

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

1 - OGC/PCLU intranet website

1 - PCLU Library

1 - PCLU Tickler

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-22-2014 BY NSICG/C32W33B91

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: [REDACTED]

b7E

A. General System Description:

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 [REDACTED] is a General Support System that consists of the [REDACTED] needed to operate some of the FBI's [REDACTED]. The [REDACTED] itself does not capture any data but rather provides [REDACTED] necessary to [REDACTED] to the FBI user community. Each [REDACTED] will provide its own PTA/PIA. The attached document, [REDACTED] contains the list of [REDACTED]

b7E

The [REDACTED] is the replacement for the [REDACTED]

b7E

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

[REDACTED] will capture logs of events for each [REDACTED]. These logs are available to the [REDACTED] support teams to assist in identifying bugs in [REDACTED]. No [REDACTED] data is kept as part of the logs.

b7E

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

The [REDACTED] will consist of [REDACTED] that are scheduled for implementation are [REDACTED]

b7E

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

Most [REDACTED] will have a link off the FBI Homepage (listed under [REDACTED] but it is not a requirement. All [REDACTED] utilize the Internet Explorer browser to present the [REDACTED] to the users. All [REDACTED] are now required to utilize the [REDACTED] to hide and secure the login passwords. [REDACTED] is utilized and all [REDACTED] will use the [REDACTED]

b7E

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:

This is based on the [REDACTED] used for data access.

b7E

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: [REDACTED]

b7E

There is a very finite set of System Administrators who have access to the [REDACTED]
[REDACTED] An even smaller set of [REDACTED] Administrators would have access to the [REDACTED]
[REDACTED] All user activity is logged [REDACTED]

b7E

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:

Absolutely no one outside the FBI will have direct access to the information in the [REDACTED]
[REDACTED] Should the need arise and proper justification is submitted, reports from the [REDACTED]
[REDACTED] may be produced and turned over.

b7E

7. Has this system been certified and accredited by the FBI Security Divisions? ☐ Yes ☒ No
The [REDACTED] received an ATO on 07/17/2007.
The [REDACTED] are targeted for ATO testing in September 2008.

b7E

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

1. 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)?:

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: [REDACTED]

b7E

☐ 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):

To provide the [REDACTED] necessary to support [REDACTED]

[REDACTED] To provide the [REDACTED] necessary to support the [REDACTED]

[REDACTED]

b7E

(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?

☐ 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.)

III. Full or Short-Form PIA

1. Is the system 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," please continue to question 2.)

FOR OFFICIAL USE ONLY

(OGC/PCLU (Rev. 12/05/08))

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

NAME OF SYSTEM / PROJECT: Automated Fingerprint Identification System (AFIS) [REDACTED] b7E		
Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [REDACTED]	Name: [REDACTED]
Reason:	Program Office: AFIS Blade Rahost Manager	Phone: [REDACTED]
Declassify On:	Division: CJIS	Room Number: JEH 7338
	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: Criminal Justice Information Services (CJIS)	Signature: [REDACTED] Date signed: 12/18/08 Name: William G. McKinsey Title: CHIEF, ITMS	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]
FBIHQ Division: Criminal Justice Information Services (CJIS)	Signature: [REDACTED] Date signed: 12/29/08 Name: [REDACTED] Title: CJIS Division Privacy Officer	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]

b6
b7C

Additional division(s) approvals may be added as warranted:

--	--	--

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

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

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

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

1 - DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov)
(if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)

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

FOR OFFICIAL USE ONLY

14-06-04-FBI-FOIA-20150417-5th-Production

EPIC-1430

epic.org

2007-12-18 14:48:48

184

13:50 8002-61-083

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-22-2014 BY NSICG/C32W33B91

FOR OFFICIAL USE ONLY

FBI PTA: Automated Fingerprint Identification System (AFIS)

b7E

PIA required: ☒ No ☐ Yes:

SORN/SORN revision required: ☒ No ☐ Yes:

Applicable SORN(s): The underlying system is covered by JUSTICE/FBI-009 (FIRS). However, this is just a technical upgrade to the system.

Notify FBI RMD/RIDS per MIOG 190.2.3: ☒ No ☐ Yes

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ☒ N/A ☐ Yes-forms affected:

The program should consult with RMD to identify/resolve any Federal records/electronic records issues.

Other:

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

Signature:

Date Signed:

[Handwritten Signature]
[Handwritten Date: 1/14/2009]

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

FBI PTA: Automated Fingerprint Identification System (AFIS) [REDACTED]

b7E

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

This project involves a proposed technical upgrade to the Automated Fingerprint Identification System (AFIS) [REDACTED] which is used to process fingerprint submissions that have been provided to the Criminal Justice Information Services (CJIS) Division for authorized national security, criminal, and civil purposes. This upgrade will increase the AFIS' processing capacity and processing speed to provide the CJIS Division with the interim technical capacity to timely process the ever increasing number of fingerprint submissions, which is a critical part of CJIS Division's mission. Increased capacity issues will be more thoroughly addressed during the acquisition of Next Generation Identification (NGI) technology; in the meantime, this interim solution will permit the FBI to meet its current mission needs.

b7E

As background, the FBI maintains an automated database that integrates criminal history records including arrest information and corresponding disposition information, submitted by Federal, State, local, tribal, and certain foreign criminal justice agencies. Currently, the FBI maintains criminal history records on more than 56 million different individuals, with many of the individuals having multiple entries of separate encounters with the criminal justice system. These records are searchable for various established purposes, and the preliminary electronic search is performed by the FBI's Integrated Automated Fingerprint Identification System (IAFIS).¹

The AFIS Segment of IAFIS began to experience performance and daily throughput capacity issues in January 2008 due to a significant increase in electronic submissions.² It has become clear that to address these performance issues, the IAFIS needs to be technically upgraded or enhanced to ensure current criminal and civil fingerprint processing will not be negatively impacted. The current system architecture is based on [REDACTED] however, upgrade capabilities are limited with this configuration. [REDACTED] configuration currently deployed is no longer

b7E

¹ The FBI has established the Fingerprint Identification Record System (FIRS) (Justice/FBI-609) as a Privacy Act system of records to support identification and criminal history record information functions for local, state, tribal, and federal criminal justice agencies, and for noncriminal justice agencies and other entities where authorized by federal statute, statute pursuant to Public Law 92-544, Presidential executive order, or regulation or order of the Attorney General of the United States. (See 28 CFR 20.31; (64 FR 52343, 52347).) IAFIS is a component of the FIRS, providing an automated fingerprint search capability, latent fingerprint search capability, electronic image storage, and electronic exchange of fingerprints and responses 24/7. AFIS is in turn the component of IAFIS which actually processes the automated fingerprint comparisons conducted by IAFIS.

² The CJIS Division processed approximately 35.5 million fingerprint submissions during Fiscal Year 2008, and FY 2009 is expected to be millions higher.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

FBI PTA: Automated Fingerprint Identification System (AFIS) [REDACTED]

b7E

available for purchase and a new upgrade solution is required. It is imperative that the CJIS Division maintain the capability to process fingerprint submissions efficiently, and merely adding new [REDACTED] and using existing technology does not provide a reasonable solution.

b7E

CJIS Division has determined that there is an interim solution available that will meet the requirement for additional processing capacity. This solution involves the reutilization of several [REDACTED]

[REDACTED] and the purchase of several AFIS [REDACTED]. This interim solution will be superseded upon receipt for deliverables from the Next Generation Identification (NGI) project; however, this long-term solution will not be available for approximately 30 months.

b7E

The proposed solution is based on [REDACTED] technology and is expected to be easily expandable for expected workloads through Calendar Year 2012. [REDACTED] technology is an [REDACTED]. In effect, this technology is faster and cheaper than what is currently being utilized. This new technology is needed because the current Operational Environment (OE) is exceeding its design capacity and the [REDACTED] has been successfully proven. [REDACTED] technology has completed a proof-of-concept (POC) comparison, and an AFIS rapid prototype with full functionality and with required performance capability is scheduled to be built as the first stage of the [REDACTED] project. This [REDACTED] will migrate the current AFIS application from its current [REDACTED] to the proposed new [REDACTED].

b7E

This initiative does not contemplate changes to the AFIS interfaces or functionality. Likewise, the upgrade will not influence the submission or retention of criminal and civil fingerprints, other than increasing processing capacity.

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.]

The underlying IAFIS system does contain fingerprints and PII. IAFIS has been in existence since well before April 17, 2003, and although there have been privacy-significant changes to IAFIS since then, such changes have been addressed in separate PTAs and PIAs. See, e.g., PIA dated June 8, 2008, for the Next Generation Identification-Interstate Photo System; and PIA dated May 4, 2008, for the Outsourcing of Noncriminal Justice Purposes. This initiative is merely a project to provide additional processing capacity by upgrading system hardware and does not itself pertain to maintenance, collection, or dissemination of the PII in the underlying system. This initiative: does not affect the number of authorized recipients; does not affect the categories of individuals for whom personally identifiable information is processed or retained; and does not affect the types of information that is being disseminated.

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1272295-0

Total Deleted Page(s) = 2
Page 1 ~ Duplicate;
Page 2 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)         X
X   No Duplication Fee      X
X   For this Page           X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1272295-0

Total Deleted Page(s) = 8

Page 1 ~ Duplicate;
Page 2 ~ Duplicate;
Page 3 ~ Duplicate;
Page 4 ~ Duplicate;
Page 5 ~ Duplicate;
Page 6 ~ Duplicate;
Page 7 ~ Duplicate;
Page 8 ~ Duplicate;

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)         X
X   No Duplication Fee      X
X   For this Page           X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Form Rev. 6/19/2006

Privacy Threshold Analysis for the

b7E

Federal Bureau of
Investigation

Contact Point

Operational Technology Division
Radio Systems Development Unit

b6
b7C

Reviewing Official:

Patrick W. Kelley,
Senior Privacy Official
Office of the General Counsel
Federal Bureau of Investigation
Department of Justice

Privacy Threshold Analysis

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

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

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

☒ YES

☐ NO

(If the answer is "yes" proceed to Question 1.)


(If the answer is "no", proceed to Section II.)

1. Has the system undergone any significant changes¹ since April 17, 2003?

☐ YES

☒ NO

¹ "Significant Changes" are defined as changes which create new privacy risks, such as, converting paper-based records to electronic systems; changing anonymous information into information in identifiable form; new uses of an IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system; merging, centralizing, or matching databases that contain information in identifiable form with other databases, or otherwise significantly manipulating such databases; newly applying any user-authenticating technology to an electronic information system that is accessed by members of the public; systematically incorporating into existing information systems databases of information in identifiable form that are purchased or obtained from commercial or public sources; working with another agency or agencies on shared functions that involving significant new interagency uses or exchanges of information in identifiable form; altering a business process that results in significant new uses or disclosures of information or the incorporation into the system or addition items of information in identifiable form; or adding new information in identifiable form, the character of which raises the risks to personal privacy (for example, adding health or financial information).

 18 JUL 2006

b7E

Approval Signature Page:

/s/ Dave C. Larson for PWK 8/6/07

Patrick W. Kelley

Senior Privacy Official, Office of the General Counsel, Federal Bureau of Investigation

Department of Justice

FBI Privacy Threshold Analysis (PTA) Cover Sheet

(OGC/PCLU (Rev. 07/06/07))

NAME OF SYSTEM: Law Enforcement Officers Killed and Assaulted (LEOKA)

FBI SYSTEM CONTACT PERSON Name: [Redacted] Unit Chief Program Office: Uniform Crime Reporting, LEOKA program Division: CJIS Division, LATSS, CSMU Phone: [Redacted] Room Number: Module E-3 Date PTA submitted for approval:	FBI OGC/PCLU POC Name: [Redacted] [Redacted] Phone: [Redacted] Room Number: 7338
---	---

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: CJIS	FBIHQ Division: CJIS
Program Manager (or other appropriate executive as Division determines)	Signature: /s/ Date signed: 4/30/2008 Name: [Redacted] Title: Unit Chief	Signature: Date signed: Name: Title:
Division Privacy Officer	Signature: /s/ Date signed: 5/19/2008 Name: [Redacted] Title: Division Privacy Officer	Signature: Date signed: Name: Title:

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: /s/ Date Signed: 5/20/2008 Name: David C. Larson Title: Acting Deputy General Counsel
---	---

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

1 - Signed original to 190-HQ-C1321794

Copies:

1 - DOJ Privacy and Civil Liberties Office-Main Justice, Room 4259

2 - FBI OCIO / OIPP

1 - FBI SecD (electronic copy via e-mail)

2* - Program Division POC /Privacy Officer

2*- FBIHQ Division POC /Privacy Officer

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

1 - OGC/PCLU intranet website

1 - PCLU Library

1 - PCLU Tickler

NAME OF SYSTEM: Law Enforcement Officers Killed and Assaulted

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:

In the instance of a line-of-duty officer death, the case agent from the jurisdictional FBI field office sends a notification EC to the FBI's LEOKA program. Within this EC, details include the description of the circumstances surrounding the death; victim officer's name, rank, date of birth, and law enforcement experience; offender's name, age, and current status, such as deceased, at large, or arrested and charged; and survivor information, such as names, ages, addresses, and relationships to the victim officer. In addition, the LEOKA program is notified of officer assaults involving injury with firearms or knives/other cutting instruments by the monthly UCR collection. This monthly collection is aggregate totals only and does not include any personal information.

In response to both notifications, the LEOKA program's staff requests that the victim officer's employing agency complete Form 1-701, "Analysis of Law Enforcement Officers Killed and Assaulted," to obtain additional details concerning the circumstances surrounding the incident. For line-of-duty deaths, Form 1-701 is provided to the victim officer's employing agency via the case agent from the jurisdictional FBI field office, and for officer assault incidents, Form 1-701 is provided to the victim officer's employing agency via the State Program or directly by the LEOKA program's staff. Form 1-701 is used to collect the victim officer's name, rank, total law enforcement experience, date of birth, gender, race, height, weight, and circumstances surrounding the death or assault of the officer. Offender data collected includes name, date of birth, gender, race, height, weight, place of birth, current or known residence, FBI number, and criminal history. Upon receipt of the completed Form 1-701, the information is stored within an electronic database utilizing Access software.

NAME OF SYSTEM: Law Enforcement Officers Killed and Assaulted

If an officer has been feloniously killed, the International Justice and Public Safety Information Sharing Network (Nlets) is utilized to transmit an All-Points Bulletin message providing preliminary information concerning the circumstances surrounding the felonious death of an officer. These Nlets messages are also stored in the electronic LEOKA database.

The above-mentioned survivor information is maintained by the LEOKA program's staff in paper-based format; however, it is not currently stored in the electronic LEOKA database. The victim officer's agency information; victim's name, age, and law enforcement experience; survivors' names, ages of children, and addresses; and a brief description of the incident are provided to the White House for condolence purposes.

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:

Not applicable.

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

Officer killed information is collected to report the number of incidents and to help law enforcement/data users better understand the situations which lead to officer deaths. Also, contributing law enforcement agencies report their officer assaults, identifying the instances that resulted in injuries. In addition, contributing law enforcement agencies provide expanded data on those officers who sustained personal injury from a firearm or a knife/other cutting instrument. Officers killed and assaulted data are collected and annually published in an effort to assist law enforcement training programs and ultimately improve officer safety. However, these publications do not contain personally identifiable information.

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

The system is an MS Access [REDACTED] The data is maintained at the CJIS Division [REDACTED]

b7E

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

The LEOKA database system is accessed through FBINET utilizing a username and password. Information supplied on Form 1-701 is entered into the system by the LEOKA program's staff.