

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Law Enforcement Officers Killed and Assaulted

Safeguards are in place to protect personally identifiable information (e.g., victims' and offenders' names and FBI numbers), to include limiting the number of authorized users and requiring unique passwords. Moreover, personally identifiable information that is maintained in the electronic LEOKA data system is never disseminated outside the CJIS Division.

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:

FBI CJIS Division, Crime Statistics Management Unit, Communications Group

Supervisor

FBI CJIS Division, Crime Statistics Management Unit, Operations Group

Technical Information Specialist

b6
b7C

FBI CJIS Division, Crime Statistics Management Unit, Operations Group

Technical Information Specialist

FBI CJIS Division, Technology Integration & Support Unit,
Enterprise Software Development Group

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

No outside access is allowed to the database.

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

The database has not been accredited. The software that it is written in has been accredited by the Information Technology Operations Division

b7E

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

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

YES (If "yes," proceed to Question 1.)

NO (If "no," proceed to Section II.)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Law Enforcement Officers Killed and Assaulted

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

YES If "yes," please explain the nature of those changes:

(Continue to Question 2.)

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

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

YES (If "yes," please proceed to Question 3.)

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

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

YES If "yes," is this a Major Information System (as listed on OGC's FBINET website)?:

Yes. (If "yes," a full PIA is required.. PTA is complete.)

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

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

II. For systems developed after April 17, 2003.

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

(Continue to Question 2.)

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

YES (If "yes," please proceed to Question 3.)

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

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

YES If "yes," is this a Major Information System (as listed on OGC's FBINET website)?:

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Law Enforcement Officers Killed and Assaulted

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.)

2. Does the system involve routine information AND have limited use/access?

YES A short-form PIA is required. (I.e., you need only answer Questions 1.1, 1.2, 2.1, 3.1, 4.1, 5.1 (if appropriate), 6.2, 6.3, and 8.9 of the PIA template.) Please note that FBI and DOJ reviewing officials reserve the right to require completion of a full PIA. (PTA is complete--forward with PIA.)

NO (If "no," a full PIA is required. PTA is complete.)

Privacy Threshold Analysis for the

National Name Check Program (NNCP)

Federal Bureau of Investigation
Contact Point

[REDACTED]

**Information Technology Operations Division
(ITOD)**

[REDACTED]

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).

National Name Check Program (NNCP)

(If "yes," please continue to Question 2.)
(If "no," the PTA is complete and should be sent to your component's Senior Privacy Officer if the system is a non-MIS or the PCLO if it is a MIS.)

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

YES

NO

(If the answer to Question 2 is "yes" please proceed to Question 3.)
(If the answer is "no" the Threshold Analysis is complete. Please send to your component's Senior Privacy Officer if the system is a non-MIS or the PCLO if it is a MIS.)

3. Is the system solely related to internal government operations?²
See page 6 of the PIA Manual.

YES

NO

(If the answer to Question 3 is "yes" the Threshold Analysis is complete.)

² When a PIA is NOT Required: No PIA is required where information relates to internal government operations; has been previously assessed under an evaluation similar to a PIA; or where privacy issues are unchanged. Examples of when a PIA would not be required: For government-run websites, IT systems, or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public or where the information pertains to government personnel, contractors, or consultants; for government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback or obtaining additional information; when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act of 1974; when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and the resulting data is protected under Title V of the E-Government Act of 2002; when developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generate information in identifiable form; and for minor changes to a system or collection that do not create new privacy risks.

National Name Check Program (NNCP)

Please send to your components Senior Privacy Officer if the system is a non-MIS or the PCLO if it is a MIS.)
(If the answer to Question 3 is "no" go to subsection 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 and proceed to Question 2.)

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

YES

NO

(If the answer to Question 2 is "yes" please proceed to Question 3.)
(If the answer is "no" the Threshold Analysis is complete. Please send to your components Senior Privacy Officer if the system is a non-MIS or the PCLO if it is a MIS.)

3. Is the system solely related to internal government operations?
See page 6 of the PIA Manual.

YES

NO

(If the answer to Question 3 is "yes" the Threshold Analysis is complete. Please send to your components Senior Privacy Officer if the system is a non-MIS or the PCLO if it is a MIS.)
(If the answer to Question 3 is "no" go to subsection III to determine if a full or short-form PIA is required.)

National Name Check Program (NNCP)

III. Full or Short-Form PIA

1. Is the system a major information system?

YES

NO

(If "yes", a full PIA is required.)

(If "no", please continue to question 2.)

2. Does the system involve routine information AND have limited use/access?
Please explain what type of information is collected and the access provided.
Please note that the reviewing official has the right to require the component
complete a full PIA.

YES (Please explain what type of information is collected and the
access provided.

<<ADD ANSWER HERE>>

If "yes", a short-form PIA is required. You need only answer
Questions 1.1, 1.2, 2.1, 3.1, 4.1, 5.1 (if appropriate), 6.2, 6.3,
and 8.9.

NO (If "no", a full PIA is required. In the interim, you must
complete a short form PIA. A full PIA will be required at a later date)

National Name Check Program (NNCP)

Responsible Official:

b6
b7C

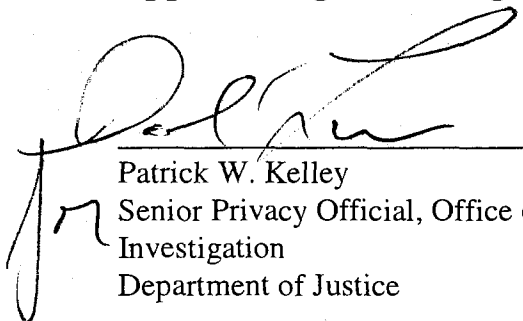
6/14/86
-<<Sign Date>>

Federal Bureau of Investigation
Department of Justice

National Name Check Program (NNCP)

Please note: If any significant changes are made to the program a new PTA should be completed.

Approval Signature Page:

 4/27/07 <<Sign Date>>

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: [Redacted]

b7E

Nothing about this on Internet/site is someone's survivalist site now

FBI SYSTEM CONTACT PERSON Name: [Redacted] Program Office: Interagency Integration Unit Division: Directorate of Intelligence Phone: [Redacted] Room Number: 11079E Date PTA submitted for approval: 10/15//2007	FBI OGC/PCLU POC Name: Phone: Room Number:
---	--

b6
b7C

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

	Program Div:	FBIHQ Div: Directorate of Intelligence
Program Manager (or other appropriate executive as Division determines)	Signature: /s/ Date signed: 10/15/2007 Name: [Redacted] Title: Management and Program Analyst	Signature: /s/ Date signed: 10/15//2007 Name: [Redacted] Title: Unit Chief
Division Privacy Officer	Signature: Date signed: Name: Title:	Signature: /s/ Date signed: 10/18/2007 Name: [Redacted] Title: Unit Chief

b6
b7C

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

FINAL FBI APPROVAL:

FBI Privacy and Civil Liberties Officer	Signature: /s/ Date Signed: 11/13/07 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

- 1 - OGC\PCLU intranet website
- 1 - PCLU Library
- 1 - PCLU Tickler

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM:

[Redacted]

b7E

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

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

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

A. General System Description: Please briefly describe:

This site does not exist anymore..cant find anything on Google

1. Type of information in the system:

[Redacted]

[Redacted]

b7E

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:

[Redacted]

[Redacted]

b7E

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

[Redacted]

b7E

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

[Redacted]

b7E

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM:

[Redacted]

b7E

[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?

The Directorate of Intelligence is the program owner [Redacted] The DI will develop standard operating procedures [Redacted]

[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:

[Redacted]

b7E

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

NOTE: This is not an FBI system so FBI C&A is not pertinent.

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

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

YES (If "yes," proceed to Question 1.)

NO (If "no," proceed to Section II.)

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

YES If "yes," please explain the nature of those changes:

(Continue to Question 2.)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM:

[Redacted]

b7E

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

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

___YES (If "yes," please proceed to Question 3.)

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

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

___YES If "yes," is this a Major Information System (as listed on OGC's FBINET website)?:

___Yes. (If "yes," a full PIA is required.. PTA is complete.)

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

___NO (If "no," go to section III to determine if a full or short-form PIA is required.)

II. For systems developed after April 17, 2003.

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

See A. 2.

(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.)

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

NOTE: As discussed above, this is not an FBI IT system and none of the PII in the system is maintained by the FBI. Names and contact information for some FBI personnel are contained in the system [Redacted]

[Redacted]

b7E

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)

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

NAME OF SYSTEM:

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.)

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.)

2. Does the system involve routine information AND have limited use/access?

YES A short-form PIA is required. (I.e., you need only answer Questions 1.1, 1.2, 2.1, 3.1, 4.1, 5.1 (if appropriate), 6.2, 6.3, and 8.9 of the PIA template.) Please note that FBI and DOJ reviewing officials reserve the right to require completion of a full PIA. (PTA is complete---forward with PIA.)

NO (If "no," a full PIA is required. PTA is complete.)

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

NAME OF SYSTEM / PROJECT: Printing Unit General Support Systems (PU GSS)

BIKR FBI Unique Asset ID: SYS-0000064

	SYSTEM/PROJECT POC Name: [Redacted] Program Office: Print Shop Division: 21 FLSD Phone: [Redacted] Room Number: 1B-973	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number: JEH, 7350
--	--	--

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Facilities and Logistics and Services Division	Signature: [Redacted] Date signed: [Redacted] Name: [Redacted] Title: Unit Chief	Signature: [Handwritten Signature] Date signed: 12/3/10 Name: Elton Wayne Thomas Title: CSO
FBIHQ Division:	Signature: [Redacted] Date signed: [Redacted] Name: [Redacted] Title: Unit Chief	Signature: [Handwritten Signature] Date signed: 12/3/10 Name: Elton Wayne Thomas Title: CSO

b6
b7C

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

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

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

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

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

b6
b7C

UNCLASSIFIED

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): The only PII collected and/or maintained by this system pertain to internal government operations (such as username/password) or information that has previously been published.

Applicable SORN(s): CRS, FBI-002

Notify FBI RMD/RIDS per MIOG 190.2.3? No Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/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:

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

Signature:
Date Signed:

Elizabeth Withnell
10/10

UNCLASSIFIED

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Printing Unit General Support Systems (PU GSS) enhances the capabilities of the Facilities Logistic Services Printing Unit (FLSD/PU) to provide professional-quality, graphic-laden FBI, DOJ, and other agencies' reports, charts, and other printed media for public and government consumption. PU GSS is owned, operated and strictly controlled by FBI employees. PU GSS currently processes information up to and including Secret, but is expected to have the capability for Top Secret and/or Sensitive Compartmented Information added this fiscal year. PU GSS consists of both Automated Information Systems (AIS) and manual hard copy systems.

The AIS are comprised of the Digital Pre-Press (DPPS) network, the Xerox Copy Center network, the Digital Press (DP) network, the standalone CD replicator and the stand alone Engineer Copier. The DPPS, DP and Xerox systems [REDACTED] [REDACTED] PU GSS is designed to ingest unclassified to highly sensitive electronic data and hardcopy information from multiple sources and generate complete high-quality documents, reports, and publications. The systems are set up in a workgroup configuration that consists of multiple print servers and workstations. All users must log in and be authenticated at the workstations. Only system administrators can access network print servers, which also require user id and password for access. The AIS will maintain this information as well as any personally identifiable information contained within the documents, reports, and publications. PU GSS also contains a job tracking system which allows print shop employees to track the progress of an individual's print shop job.

b7E

Data ingestion currently occurs through manually entered hard copy data and any data uploaded from external media, such as zip, floppy, and/or compact disk. All jobs are logged in the Print Unit job tracking system which assigns a number and maintains the customer's name, a contact phone number for the customer, title of the print job, cost code, quantity desired, number of pages, and delivery date for each job.

On the manual system side, PU GSS consists of a host of hard copy manipulation systems (Binders, Paper Presses, Laminators, Staplers, Folders, Grinders, Wrappers, Cutters, and Shredders). These systems are limited in regard to automated processing and logical/standard data storage. Unlike the AIS part of PU GSS, the manual systems of PU GSS do not collect, maintain, store, or disseminate any personally identifiable information.

PU GSS is operated and maintained only by trained and cleared individuals who are authorized access to the system. PU GSS operates as a closed stand alone networked environment that does not connect logically or physically to any outside networks or systems. Maintenance, upgrades to software, and new installations are accomplished through FBI directed "air gap" procedures. An air gap procedure involves manually transferring data on approved compact disks or memory sticks instead of connecting via a network.

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

..... NO

X YES [If yes, please continue.] The only PII maintained by the system is username/password for the automated information systems, information in the job tracking system, and information that will be or has previously been published in the public domain.

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

(Check all that apply.)

X The information directly identifies specific individuals.

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

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

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

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

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

X NO YES

Usernames, passwords, and information in the job tracking system will only pertain to government employees, contractors, or consultants. However, information maintained by the graphic artists may include names or other identifiers of government employees, contractors or consultants as well as non-

governmental employees, contractors, or consultants who have appeared or will appear in various FBI publications throughout the years.

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.] Both the job tracking system and the audit logs would have the ability to retrieve information by name or other personal identifier (in this case, an individual's username).

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 However, the majority of personally identifiable information is not collected directly from the person who is the subject of the information. For example, the customer name used for tracking a job may not be the name of the person who actually dropped off the job. The only other information that could be collected directly from the person is the username/password when the person inputs it into the workstation. The administrator assigns the usernames and individuals create their own password.

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 X 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?

X NO

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

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

_____ NO X YES

13. Status of System/ Project:

_____ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? January, 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 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. Since 2004, PU GSS has changed its ability to ingest data. PU GSS changed from paper and film for printing to using scanners and computers. PU GSS is now able to ingest electronic data from CDs, emails, and thumb drives, thus enhancing the versatility of printing capabilities without a change in how it maintains records, individuals on whom records are maintained or the use/dissemination of information from the system.

_____ 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

~~SECRET~~ ATTACHED (THIS PAGE UNCLAS) WSM

FBI Privacy Threshold Analysis (PTA) Cover Sheet (OGC/PCLU (Rev. 05/02/08))

NAME OF SYSTEM: [REDACTED] b7E

Derived From: Classified By: Reason: Declassify On:	SYSTEM POC Name: [REDACTED] Program Office: ITB Division: ITOD Phone: [REDACTED] Room Number: 8977	FBI OGC/PCLU POC Name: [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: RMD	FBIHQ Division: ITOD
Program Manager (or other appropriate executive as Division determines)	Signature: <i>Debra Anne O'Clair</i> Date signed: 7/3/08 Name: Debra Anne O'Clair Title: Acting Section Chief	Signature: [REDACTED] Date signed: 6/26/08 Name: [REDACTED] Title: IT Specialist
Division Privacy Officer	Signature: <i>David M. Hardy</i> Date signed: 6/26/08 Name: David M. Hardy Title: Section Chief	Signature: <i>Jennifer R. Sanchez</i> Date signed: 6/26/08 Name: Jennifer R. Sanchez Title: 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: <i>David E. Larson</i> Date Signed: 7/14/08 Name: David E. Larson Title: Deputy General Counsel
---	---

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

1 - Signed original to 190-HQ-C1321794

Copies:

- 1 - DOJ Privacy and Civil Liberties Office-Main Justice, Room 4259
 - 1 - OGC/PCLU intranet website
 - 2 - FBI OCIO / OIPP
 - 1 - PCLU UC
 - 1 - FBI SecD (electronic copy via e-mail)
 - 1 - PCLU Library
 - 2* - Program Division POC /Privacy Officer
 - 1 - PCLU Tickler
 - 2*- FBIHQ Division POC /Privacy Officer
- (*please reproduce as needed for Program/Division file(s))

~~SECRET~~ ATTACHED (THIS PAGE UNCLAS) WSM

2008 JUL 9 2008

~~SECRET~~

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM:

b7E

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

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

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

A. General System Description: Please briefly describe:

1. Type of information in the system:

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

(U)

(u) ~~(S)~~

b7E

allows authorized users to enter, query, retrieve, maintain, modify, and delete index data

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

The units to which these personnel are assigned provide direct tactical, programmatic, and strategic analytical support

(U)

~~(S)~~

allows these authorized personnel to

are specifically designated for this purpose. Authorized users of allow for processing reports, including printing, and backing up the system without interaction with any other system.

b7E

~~7-25-2008~~
~~Classified by 4922 ugw/stp/jce~~
~~Declassify on: 1-25-2028~~

~~ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
EXCEPT WHERE SHOWN OTHERWISE~~
epic.org

~~SECRET~~

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: [REDACTED]

b7E

3. The system's structure (including components/subsystems): The system is [REDACTED]

[REDACTED]

b7E

4. Means of accessing the system and transmitting information to and from the system: The system can only be accessed from [REDACTED]

[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: The system administrator makes sure that only authorized persons access the system. There are approximately [REDACTED] authorized users that have access to the system.

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: Nobody outside of the FBI has direct access to the system [REDACTED]

[REDACTED]

b7E

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

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

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

YES (If "yes," proceed to Question 1.)

NO (If "no," proceed to Section II.)

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

YES If "yes," please explain the nature of those changes:

(Continue to Question 2.)

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

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED] b7E

BIKR FBI Unique Asset ID: SYS-0000175

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: Sr. Electronics Eng'r [REDACTED]	Name: AGC [REDACTED]
Reason:	Program Office: Data Intercept Tech. Unit (DITU)	Phone: [REDACTED]
Declassify On:	Division: Operational Technology (OTD)	Room Number: 7350 JEH
	Phone: [REDACTED]	
	Room Number: 4C05 - ERF	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Operational Technology Division	Signature: [REDACTED] Date signed: 5/16/12 Name: SSA [REDACTED] Title: Unit Chief, DITU	Signature: [REDACTED] Date signed: 5/17/12 Name: SSA [REDACTED] Title: Assistant Section Chief, OTD
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: [REDACTED] Date signed: 5/17/12 Name: [REDACTED] Title: Division 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:

[Redacted] End users cannot access data within [Redacted] Data remains in [Redacted] [Redacted] for up to twenty eight days before automatic deletion.

b7E

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

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:

[Redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [Redacted] Date Signed: [Redacted]
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: [Redacted] Date Signed: 6/3/12

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.

[Redacted]

b7E

[Redacted]

b7E

Access to [Redacted] is restricted to DITU personnel; end users cannot access or view data within [Redacted]. Collected data remains available in [Redacted] [Redacted] for no more than twenty-eight days before automatic purging.

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 PLA 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)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:


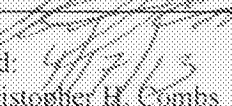
b7E

BIKR FBI Unique Asset ID: Not Assigned-pending

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: SSA 	Name:
Reason:	Program Office: SIOC	Phone:
Declassify On:	Division: 22	Room Number: 7350
	Phone: 	
	Room Number: 5712	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature:  Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: [CIRG]	Signature:  Date signed: 4/19/13 Name: Christopher H. Combs Title: Section Chief	Signature: Date signed: 4/19/2013 Name: Title: SSA/CDC

b6
b7C

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 :

PIA may contain Law Enforcement Sensitive information.

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

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

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



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

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

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

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

Other:

<input type="checkbox"/> Unit Chief Privacy and Civil Liberties Unit Brian F. Binney Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature:  Date Signed: 5/17/13 Signature:  Date Signed: 5/17/13
--	--

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.

A. Name of the system/project, including associated acronyms:

Strategic Information and Operations Center (SIOC) [redacted]
[redacted]

b7E

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

As a strategic asset of the FBI, the Strategic Information and Operations Center (SIOC) operates a command center on a 24/7/365 basis to maintain enterprise-wide situational awareness and provide FBI executives with timely notification and dissemination of strategic information. SIOC is the central operations center for FBI communications and operations worldwide. The command center is typically referred to as SIOC Watch. The SIOC Watch is locked to when critical events are breaking. Possessing a vast inventory of capabilities and network, SIOC maintains a constant state of readiness to support any crisis or major event, and provides a secure venue to support crisis management, special event monitoring, and significant operations. It is critical to its mission that SIOC be able to receive and disseminate information about such incidents in a timely manner. SIOC currently relies primarily on open source news resources for notification of critical breaking events. On occasions, this means that SIOC will not know a critical event is occurring until well after the fact, in situations where fast response time is necessary. [redacted]

[redacted]

b7E

[redacted] "standalone" system that will not connect to any other FBI information systems. [redacted]

[redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

To the extent that that FBI intends to use the system for purposes beyond that associated with the special event pilot, another PTA and PIA will be conducted prior to initiating that use.

C. Purpose of the system/project:

The purpose of [Redacted] in order to give the SIOC Watch the ability to notify FBI offices in the United States and around the world of critical incidents in their area of responsibility (AOR) as they are occurring. [Redacted] will improve overall FBI situational awareness and will enable SIOC to perform its mission in a timelier manner. [Redacted] should reduce response times and enable the FBI to more effectively deploy assets and mitigate crisis events.

b7E

The FBI will assess the privacy risks associated with the [Redacted] in phases. The first phase is a pilot [Redacted] The FBI is considering other uses for [Redacted] but those will be assessed in separate privacy documentation prior to any implementation. During the pilot phase, the FBI will [Redacted] will be required to articulate an authorized purpose as required under the FBI's Domestic Investigations and Operations Guide (DIOG); [Redacted]

b7E

[Redacted] and is in accordance with the Attorney General Guidelines (AGG) for Domestic Operations. Piloting the [Redacted] will allow the FBI to ensure that the system operates as expected and to identify any changes that need to be made to the system prior to expanding the possible uses of the system.

D. Nature of the information in the system/project and how it will be used:

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

[Redacted] must be approved at the supervisory level within the FBI.

SIOC is working with Records Management Division to determine whether a retention schedule is required. SIOC will request a 30 day retention schedule for [Redacted] to make a relevancy determination. Under the proposed retention schedule [Redacted]

[Redacted] Any information deemed to be relevant [Redacted] will be purged from [Redacted] and transferred to the FBI's case management system for retention and will take on the schedule of that case file. SIOC will take all necessary precautions to protect [Redacted] by ensuring that any information stored is pertinent [Redacted]

b7E

E. Who will have access to the information in the system/project:

[Redacted] will only be used by approximately 20-25 SIOC personnel who are trained to use [Redacted]. Approved SIOC personnel will have access to the [Redacted] user account while the project's computer engineer will have full system access. All user accounts will be password protected. Users will be trained [Redacted] that may be performed and their use will be audited to ensure that they are using the system in accordance with the [Redacted]. Users will also be trained on identifying personally identifiable information (PII) [Redacted] and how to mitigate the risks associated with that information. These steps will ensure appropriate use of incoming information. The training will be provided by the program manager, the [Redacted] developer, and the Privacy and Civil Liberties Unit of OGC.

b7E

F. The manner of transmission to all users:

An important function of [Redacted] will be the ability to send alerts to

b7E

SIOC personnel [redacted]
[redacted]

[redacted] At that point the [redacted] user will receive an alert indicating an event requiring SIOC attention. The alerts will be sent via email to a designated SIOC mailbox on the FBI's unclassified network (UNET). This will notify the user to look at [redacted] to determine if there is actionable information. The alert email will not contain any [redacted] PII. SIOC users will review the [redacted] stored on the [redacted] to determine if the information is credible (and must do so within 30 days). If the event is deemed credible and actionable, SIOC will follow its normal protocol for dissemination of information and notifications. SIOC uses [redacted]
SIOC uses [redacted]
[redacted]
[redacted] is deemed relevant to the investigation, SIOC will provide that information to the requestor.

b7E

In the event the [redacted] alerts [redacted] [redacted] are deemed relevant to a threat, [redacted] will then become part of the [redacted] file and will be stored in the FBI's Central Records System (CRS). This will be accomplished by [redacted] and uploading that information into the CRS on the FBI's secret network. Standard protocol will be to [redacted] [redacted] be relevant to the investigation, that information will be copied as well. This information will be deleted [redacted] once it has been uploaded to the CRS.

b7E

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

_____ NO

 X YES (If yes, please continue.)

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

(Check all that apply.)

_____ 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 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: The Project is in the preliminary development stages and has not been tested by Security Division.

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

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

b7E

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

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: Program Office: Special Technologies and Applications Office Division: 24 Phone: Room Number: CH-102	FBI OGC/PCLU POC Name: Phone: Room Number: 7350 <i>6172</i>
--	--	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Special Technologies and Applications Office	Signature: Date signed: <i>8-12-10</i> Name: Title: Unit Chief, Computer Engineering Unit	Signature: <i>Marcie Nagel</i> Date signed: <i>8/12/10</i> Name: Marcie Nagel Title: CSO (Acting)
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 7350).
(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)

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

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

b6
b7C

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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): *Infrastructure only - Applications all/will be analyzed separately*

Applicable SORN(s): *DOO 002*

Notify FBI RMD/RIDS per MIOG 190.2.3? No ___ Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/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):

FD-889, FBI Rules of Behavior for General Users, provides a SA where for PIA IT systems

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:

Barbara W. Muel

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

Signature:
Date Signed:

Signature: [Handwritten Signature] 8/23/10

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.

(U) [redacted] is an information system owned by the Special Technologies and Applications Office (STAO).

b7E

(U) [redacted] originally received an Approval to Operate (ATO) on July 16, 2004. The most recent Approval to Operate for [redacted] was granted on April 14, 2009 and expires on April 13, 2012.

b7E

(U//FOUO) [redacted] is an Unclassified network providing public Internet connectivity for approximately [redacted] staff, to include the following FBI Offices, Divisions, Units, and Joint-Task Force activities:

b7E

> STAO:

[redacted]

b7E

> Operational Technology Division (OTD):

[redacted]

> National Cyber Investigative Joint Task Force (NCIJTF)

(U//FOUO) [redacted] supports technical and investigative analysts, investigative application development staff, STAO management, and support staff, which includes personnel supporting engineering, logistics, finance, and security activities. The network provides [redacted]

b7E

connectivity for up to [redacted] authorized staff on field deployment. It supports counter-terrorism, counter-intelligence and criminal investigative missions by providing Unclassified data connectivity [redacted]


[redacted] also includes a [redacted] that provides STAO with an alternate Unclassified communications method.

(U//FOUO) [redacted] provides infrastructure support to the below listed major applications. Each application will have its own PTA/PIA; these are outside the scope of this PTA. This PTA is for the [redacted] core infrastructure, which only includes user credential information, e.g., username and password.

b7E

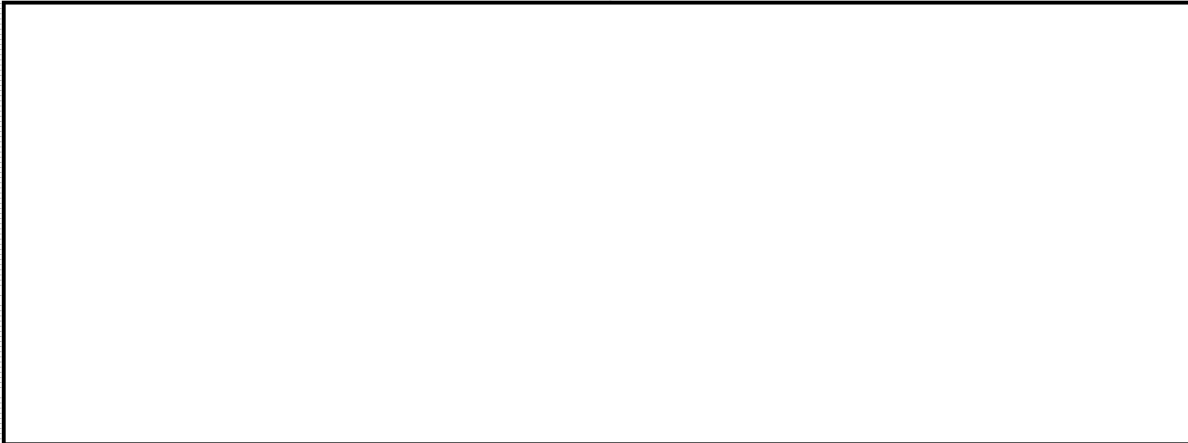


b7E

(U) The following is a high-level conceptual schematic of the data flows within 

b7E

UNCLASSIFIED//FOUO



b7E

UNCLASSIFIED//FOUO

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 PLA 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

User credentials only, e.g., username and password

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 Username and password, not a data collection system

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:
14 April 2009

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 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).]

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]: New applications are being added to

b7E

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

NO YES

underwent a PIA in 2007. This is the 3 year update.

b7E

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [Redacted]

b3
b7E

BIKR FBI Unique Asset ID: Pending

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [Redacted] Program Office: [Redacted] Division: CTD Phone: [Redacted] Room Number: 2500-TSC	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number: 7350-JEH
--	--	---

b6
b7C
b7E

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: [Redacted] Title: [Redacted]	Signature: Date signed: Name: Title:
FBIHQ Division: CTD	Signature: Date signed: [Redacted] 2/26/14 Name: [Redacted] Title: UC	Signature: Date signed: [Redacted] Name: [Redacted] Title: UC

b6
b7C

(LAW ENFORCEMENT SENSITIVE)

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

PIA is required by the E-Government Act.

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

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

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 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:

03/13/14

b6
b7c

(LAW ENFORCEMENT SENSITIVE)

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

(a) Name of the system/project – [redacted]

b3
b7E

(b) Structure of the system/project, including interconnections with other projects or systems – [redacted] is housed on a standalone system that is currently being used by 14 field offices within the FBI and is likely to expand to other offices in the future. It is anticipated that [redacted] data will be housed in an FBI database and fully integrated into the FBI's [redacted]

b3
b7E

(c) Purpose of the system/project – The purpose of [redacted] is to [redacted]
[redacted]

b3
b7E

(d) Nature of the information in the system/project and how it will be used – [redacted]

[redacted]

b3
b7E

(e) Who will have access to the information in the system/project – Only FBI entities with an articulable need to know and those associated with specific predicated subjects/investigations will have access to the information.

(f) Manner of transmission to all users – [redacted]

[redacted]

b3
b7E

[redacted] To ensure compliance with the Privacy Act, [redacted] will be based on predicated investigations to ensure that the information collected is relevant to a law enforcement activity.

Product Overview

[redacted] that assists analysts/agents' [redacted] ultimately helps the analyst/agent [redacted]

b3
b7E

[Redacted]

b3
b7E

Benefits

[Redacted] benefits the [Redacted] analyst/agent by:

- Saving time and resources by [Redacted]
[Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- Automatically collecting and storing [Redacted]
- [Redacted]
- [Redacted] to be used in other analytical software applications
- Receiving automatic software updates [Redacted]

b3
b7E

Architecture

[Redacted]

b3
b7E

[Redacted]

Data Collection

[Redacted]

b3
b7E

[Redacted]

The analyst/agent can delete from the database when it is no longer needed or can export for use in reports or in other software.

b3
b7E

supports which can be changed at any time, to give the analyst/agent a maximum amount of control over what is stored in the database:

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 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).

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?