

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

NAME OF SYSTEM: HumRRO FBI SBU Laptops System

FBI SYSTEM CONTACT PERSON

Name: Acting Unit Chief [REDACTED]
Program Office: Career Path Unit
Division: HRD - (D-3)
Phone: [REDACTED]
Room Number: 1B-233, Bldg. 9, FBI Academy
Date PTA submitted for approval: 03-16-2007

b6
b7C

FBI DIVISION APPROVALS

	Program Division: EDSP	FBIHQ Division: HRD (D-3)
Program Manager (or other appropriate executive as Division determines)	Signature: Date signed: Name: [REDACTED] Title: Assistant Section Chief	Signature: Date signed: Name: Timothy D. Cox Title: Section Chief
Division Privacy Officer	Signature: Date signed: Name: Title:	Signature: Date signed: Name: [REDACTED] Title: Division Privacy Officer

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: [Signature] Date Signed: 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 [REDACTED]
- ✓ 2* - FBIHQ Division POC /Privacy Officer [REDACTED]
- 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) Cover Sheet (OGC/PCLU (Rev. 1/17/07))

NAME OF SYSTEM: HumRRO FBI SBU Laptops System

FBI SYSTEM CONTACT PERSON

Name: Acting Unit Chief [REDACTED]
Program Office: Career Path Unit
Division: HRD - (D-3)
Phone: [REDACTED]
Room Number: 1B-233, Bldg. 9, FBI Academy
Date PTA submitted for approval: 03-16-2007

b6
b7C

FBI DIVISION APPROVALS.

	Program Division: EDSP	FBIHQ Division: HRD (D-3)
Program Manager (or other appropriate executive as Division determines)	Signature: [REDACTED] Date signed: 5/16/07 Name: [REDACTED] Title: Assistant Section Chief	Signature: [REDACTED] Date signed: 5/14/07 Name: Timothy D. Cox Title: Section Chief
Division Privacy Officer	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]	Signature: [REDACTED] Date signed: 5/7/07 Name: [REDACTED] Title: Division Privacy Officer

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

FINAL FBI APPROVAL:

FBI Privacy and Civil Liberties Officer	Signature: Date Signed: Name: 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 10-23-2014 BY NSICG/C32W33B91

EPIC-333

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: HumRRO FBI SBU Laptops System

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

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: The Human Resources Research Organization (HumRRO) FBI Sensitive But Unclassified (SBU) Laptop System processes For Official Use Only (FOUO), SBU, and Law Enforcement Sensitive (LES) information.

1. Type of information in the system: Non-personally identifiable information consisting of minutes from contractor-held focus group meetings with FBI employees who are Subject Matter Experts (SMEs) regarding the tasks performed and the knowledge, skills and abilities required in their area of specialization, information generated from the analysis of the results of those meetings, and information related to the preparation of reports to the FBI by HumRRO as deliverables under the contracts. The currently identified contract task orders to be supported by this system are: FBI Job Analysis (JA) - Special Agents - focuses on counterintelligence, counterterrorism, intelligence, cyber and criminal divisions, and FBI JA - Intelligence Career Service (ICS) - focuses on intelligence analysts, language analysts, surveillance specialists.

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: N/A

2. Purpose for collecting the information and how it will be used: The HumRRO contracts (OPM Project Codes: 02EA3TS218 and 02EA3TS251) provide analysis of multiple job series. The purpose of this analysis is to determine program-specific competencies and their associated developmental opportunities. Program-specific competencies reflect specialized knowledge, skills or abilities that are required to perform the critical job tasks. For each program-specific competency developed, HumRRO must identify proficiency levels, measurable behavioral indicators and related development opportunities. This system is used to record minutes from focus groups, analyze the recorded information, and prepare reports for the FBI. The goal is to describe what personnel in various internal FBI departments do and how they do it in order to improve training. Each task addresses a different focus group. In addition, the data gathered from the questionnaires will be analyzed by a statistical software package to facilitate the identification of the important tasks and knowledge-skills-and-abilities (KSAs). Finally, this information system will be used to produce various deliverables associated with the generation of the tasks, KSAs, and then ultimately competencies. These deliverables include lists, as well as the final report.

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

b7E

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: HumRRO FBI SBU Laptops System

4. Means of accessing the system and transmitting information to and from the system: All users are authorized system access based on a minimum of a Secret security clearance or Limited Background Investigation (LBI). The uncleared users are specifically authorized to access the system based on an LBI conducted by the FBI Security Division. The system owner or program manager determine need-to-know and authorize specific HumRRO personnel for SBU Laptop system accounts. Each person authorized to access this information system is briefed on their system responsibilities and has agreed to the user rules of behavior for this system. The ISSO retains signed acknowledgement forms for each authorized person. Each person has a unique login to the information system. Upon change in access or termination, the specified user's login will be disabled.

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: Acting Unit Chief [REDACTED]

b6
b7C

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] HumRRO Project Manager.

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: HumRRO FBI SBU Laptops System

By EC dated 03/07/2007, file/serial number 319U-HQ-A1487677-SECD-523, a separate system, the HumRRO FBI Classified Laptop System, received Approval to Operate (ATO). ATO for the *HumRRO SBU Laptops System* is pending, and expected in due course.

HumRRO has been awarded a facility clearance at the Secret level and has been approved for closed storage safeguarding of Secret material. The assumption is made that HumRRO will maintain, as a minimum, the Secret facility clearance and safeguarding approval throughout the period of performance. Failure on HumRRO's part to maintain this minimum level of facility clearance and safeguarding will result in the recovery by the FBI of all material entrusted to HumRRO to include the HumRRO FBI SBU Laptop system hard drives, printouts, and other system media containing FBI data (e.g. system backups, deliverables, reference material and work in progress information).

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

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

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

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

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

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

(Continue to Question 2.)

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

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

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

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

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

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

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

☐ No. (If "no," the PTA is complete and should be sent to FBI OGC's Privacy and Civil

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: HumRRO FBI SBU Laptops System

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 above. See Question A.2, *supra*.

(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.)

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

~~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: PENDING

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

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Access Control	Signature: Date signed: 7/11/11 Name: Title: Acting Unit Chief	Signature: Date signed: Name: Title: Assistant General Counsel
FBIHQ Division: Security Division	Signature: Date signed: 7/11/11 Name: Colleen Cortyngnam Title: Section Chief	Signature: Date signed: Name: Title: Assistant General Counsel

b6
b7C

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

~~SECRET~~

~~SECRET~~

~~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 :
This is a national security system, it will not be published on fbi.gov.

☐ 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): Security Access Control System (SACS), DOJ/FBI-013 and Intelligence Community Security Clearance and Access Approval Repository, ODNI-12

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

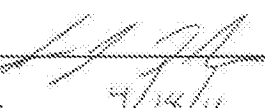
SORN/SORN revision(s) required? ☒ No ☐ Yes :

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

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

Other:

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

Signature: 
Date Signed: 4/14/11

~~UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

~~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.

[Redacted]

b3
b7E

[Redacted]

b3
b7E

[Redacted]

b3
b7E

[Redacted]

b1
b3
b7E

(S)

[Redacted]

b3
b7E

~~UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

~~UNCLASSIFIED~~

b3
b7E

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 [If yes, please continue.]

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

___X___ The information directly identifies specific individuals.

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

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

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

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

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

_____ NO ___X___ YES

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

~~UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

~~UNCLASSIFIED~~

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

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

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

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

 X YES

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

 X NO

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

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

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

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

Privacy Act (e)(3) statements are posted in the Visitor's Center, the Escort Desk, and

b3
b7E

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

_____ NO X YES If yes, check all that apply:

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

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

~~UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

UNCLASSIFIED

_____ SSNs are important for other reasons. Describe:

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

b3
b7E

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

8. Is the system operated by a contractor?

 X No.

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

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

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

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

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

December 2, 2010

Confidentiality: Low Moderate X High Undefined

Integrity: Low X Moderate High Undefined

Availability: X Low Moderate High Undefined

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

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

 X NO

UNCLASSIFIED

~~SECRET~~

~~SECRET~~

~~UNCLASSIFIED~~

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

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

 X NO

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

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

_____ NO X YES

13. Status of System/ Project:

 X This is a new system/ project in development.

b3
b7E

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.)

~~UNCLASSIFIED~~

~~SECRET~~

~~SECRET~~

~~UNCLASSIFIED~~

_____ 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

~~UNCLASSIFIED~~

~~SECRET~~

~~SECRET//NOFORN~~

COVER SHEET IS UNCLASSIFIED//FOR OFFICIAL USE ONLY WHEN DETACHED FROM PTA

(OGC/PCLU (Rev. 06/08/2010))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: [REDACTED] b7E

BIKR FBI Unique Asset ID: N/A

FBI INFO

CLASSIFIED BY NSICG/C32W33B91

REASON: 1.4 (C)

DECLASSIFY ON: 01-27-2040

DATE: 01-27-2015

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: SSA [REDACTED]	Name: AGC [REDACTED]
Reason:	Program Office: CPIU	Phone: [REDACTED]
Declassify On:	Division: WMDD	Room Number: 7350 JEH
	Phone: [REDACTED]	
	Room Number: 6387 JEH	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]
FBIHQ Division: Weapons of Mass Destruction Directorate (WMDD)	Signature: [REDACTED] Date signed: 10/17/10 Name: SSA [REDACTED] Title: Unit Chief, WMDD, Counter-Proliferation Initiatives Unit	Signature: [REDACTED] Date signed: 10/17/10 Name: [REDACTED] Title: Management & Program Analyst

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.)

~~SECRET//NOFORN~~

COVER SHEET IS UNCLASSIFIED//FOR OFFICIAL USE ONLY WHEN DETACHED FROM PTA

~~SECRET//NOFORN~~

COVER SHEET IS UNCLASSIFIED//FOR OFFICIAL USE ONLY WHEN DETACHED FROM PTA

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):

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

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

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

_____ 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).

X Other:

[REDACTED]

b7E

Applicable SORN(s): CRS-FBI-002 will cover any resulting FBI information derived from this activity.

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? X No _____ Yes

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 &
FBI Privacy and Civil Liberties Officer

Signature:
Date Signed:

Elizabeth Ross Withnell
10/7/10

~~SECRET//NOFORN~~

COVER SHEET IS UNCLASSIFIED//FOR OFFICIAL USE ONLY WHEN DETACHED FROM PTA

~~SECRET//NOFORN~~

FBI PTA: [REDACTED]

b7E

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.

(S)

b1
b3
b7E

~~SECRET//NOFORN~~

EPIC-518

~~SECRET//NOFORN~~
FBI PTA:



b7E

(S)

(S)

b1
b3
b7E

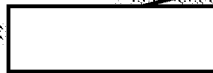
2. Does the system/project collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person)?

..... NO

~~SECRET//NOFORN~~

EPIC-519

FBI PTA:



b7E

~~SECRET//NOFORN~~

X YES [If yes, please continue.]

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

X The information directly identifies specific individuals.

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

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

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

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

X NO _____ YES

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

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

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

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

X 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.]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FBI PTA: [REDACTED]

b7E

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)? N/A

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

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

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

_____ NO X YES If yes, check all that apply:

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

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

_____ SSNs are important for other reasons. Describe:

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

~~(S)~~ (NF) [REDACTED]

(S) [REDACTED] will be restricted to FBI personnel [REDACTED] with a "need to know." In the event that information [REDACTED] is relevant for other [REDACTED] matters, access will still be restricted to appropriate personnel in the appropriate FBI investigative programs with a "need to know."

(S)

b1
b3
b7E

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

8. Is the system operated by a contractor?

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

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FBI PTA:

[Redacted]

b7E

Office of the General Counsel may be required if a contractor is operating the system for the FBI.

[Redacted]

(S) b1
b3
b7E

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

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

(U) ~~(S/NF)~~ [Redacted] does not constitute an information technology system and is therefore not subject to C&A.

b7E

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

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

Confidentiality: Low Moderate High Undefined

Integrity: Low Moderate High Undefined

Availability: Low Moderate High Undefined

 Not applicable – this system is only paper-based.

10. 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

[Redacted]

(S) b1
b3
b7E

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FBI PTA:

b7E

b1
b3
b7E

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

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

X NO _____ YES

~~(S/NF)~~

(S)

b1
b3
b7E

13. Status of System/ Project:

X This is a new system/ project in development. [If you checked this block, STOP. The PTA is now complete and after division approval(s) should be submitted to FBI OGC/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 (IL3).]

_____ 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.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FBI PTA:

b7E

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

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

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

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

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

_____ Other [Provide brief explanation]:

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

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

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

_____ NO _____ YES

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

~~SECRET//NOFORN~~

~~SECRET~~**FBI Privacy Threshold Analysis (PTA) Cover Sheet**

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

NAME OF SYSTEM: ISRAA

Derived From: Classified By: Reason: Declassify On:	SYSTEM POC Name: <input type="text"/> Program Office: ITB Division: ITOD Phone: <input type="text"/> Room Number: 1302	FBI OGC/PCLU POC Name: <input type="text"/> <input type="text"/> Phone: <input type="text"/> 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: RPO	FBIHQ Division: ITOD
Program Manager (or other appropriate executive as Division determines)	Signature: _____ Date signed: _____ Name: <input type="text"/> Title: Unit Chief, Resources Analysis Unit	Signature: /s/ _____ Date signed: 5/29/2008 Name: <input type="text"/> Title: Acting UC- FSU
Division Privacy Officer	Signature: _____ Date signed: _____ Name: _____ Title: _____	Signature: /s/ _____ Date signed: 5/29/2008 Name: <input type="text"/> Title: Division Privacy Officer

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: 6/26/2008 Name: David C. Larson Title: Deputy General Counsel
---	--

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

1 - Signed original to 190-HQ-C1321794

Copies:

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

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

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

~~SECRET~~

~~SECRET~~

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: ISRAA

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:

ISRAA reposes Subject Names, Agent Names and to include all of the Agent Accomplishments to FBI Cases registered in ACS.

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:

N/A.

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

Primary Purpose: ISRAA allows FBI metrics to workload analysis and Agent Accomplishments.

Secondary Purpose: ISRAA allows qualitative and quantitative analysis

b7E

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

b7E

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

ISRAA operates at the Secret Level and is only accessible via FBINET. ISRAA receives data

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:

Access to ISRAA is granted via the SAR process and its approvals are governed by Management Analysts, DO/RPO/RAU.

b6
b7C

~~SECRET~~

~~SECRET~~

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: ISRAA

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:

ISRAA information does get disseminated outside the FBI to include DOJ, Congress at the direction of the Congressional Affairs Office, and other entities at the direction of the OGC.

7. Has this system been certified and accredited by the FBI Security Divisions? ☒_X_Yes ☐_No
8. Is this system encompassed within an OMB-300? ☐_Yes ☐_No ☐_X_Don't Know
(if yes, please attach copy of latest one.)

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

☒_X_YES (If "yes," proceed to Question 1.)

☐_NO (If "no," proceed to Section II.)

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

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

(Continue to Question 2.)

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

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

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

☒_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.)

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,

~~SECRET~~

~~SECRET~~

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: ISRAA

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)?:

___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?

~~SECRET~~

~~SECRET~~

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: ISRAA

☐ **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.)

~~SECRET~~

FBI Privacy Threshold Analysis (PTA) Cover Sheet

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

NAME OF SYSTEM: Integrated Video Imaging System (IVIS)

FBI SYSTEM CONTACT PERSON Name: <input type="text"/> Program Office: Financial Systems Unit, Systems Support Section Division: ITOD Phone: <input type="text"/> Room Number: 1302 Date PTA submitted for approval:	FBI OGC/PCLU POC Name: <input type="text"/> Phone: <input type="text"/> 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: Security Operations Section (SOS)	FBIHQ Division: Security
Program Manager (or other appropriate executive as Division determines)	Signature: /s/ Date signed: 10/31/07 Name: <input type="text"/> Title: Unit Chief	Signature: /s/ Date signed: 10/22/07 Name: <input type="text"/> Title: Management & Program Analyst
Division Privacy Officer	Signature: Date signed: Name: Title:	Signature: [not signed] Date signed: Name: Jeffrey J. Berkin Title: Deputy Assistant Director

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: 05/16/08 Name: David C. Larson Title: Deputy General Counsel
---	---

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

1 - Signed original to 190-HQ-C1321794

Copies:

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

2 - FBI OCIO / OIPP

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

2* - Program Division POC /Privacy Officer

2*- FBIHQ Division POC /Privacy Officer

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

1 - OGC/PCLU intranet website

1 - PCLU Library

1 - PCLU Tickler

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Integrated Video Imaging System (IVIS)

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:

IVIS contains an Access Database file of personal information from the Bureau Personnel Management System (BPMS), and the photos and signature files are stored on the Security Division's unit shared drive.

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:

IVIS currently houses 113,000 records and validates the following data from BPMS: Name, Social Security Number, Clearance, File Number, Phone Number, Extension, Home Telephone Number, Address, Retirement Date, and Cost Code.

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

IVIS is used to create identification badges and credentials for Bureau employees, background investigators, chaplains, contractors and task force personnel.

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

IVIS consists of standard FBI workstations configured to connect to the Access database through the Trilogy domain and have the IVIS client software installed.

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

Login through the Trilogy domain, then login through the IVIS application.

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:

Access to IVIS will be controlled by unique user accounts and system roles. Only users assigned to the FBI's Access Control Unit, and IVIS Administrator and ISSO roles will have access to user account data. Only the Privileged User and system administrators will have access to the server's desktop. Total number of users within the ACU is there are system administrators, and ISSO.

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:

No other agencies outside of the FBI use or will have access to the system or to the information in the system. IVIS uses the existing access control measures within the Secret Enclave's Active Directory for providing authorized users access to the IVIS.

7. Has this system been certified and accredited by the FBI Security Divisions? ☐_X_Yes ☐_No

8. Is this system encompassed within an OMB-300? ☐_Yes ☐_No ☐_X_Don't Know

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Integrated Video Imaging System (IVIS)

(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:

The current system is described in Part A above.

(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.)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Integrated Video Imaging System (IVIS)

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.)

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.)

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

Total Deleted Page(s) = 1
Page 4 ~ b3; b7E;

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

UNCLASSIFIED // ~~FOR OFFICIAL USE ONLY~~

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED]

BIKR FBI Unique Asset ID: [REDACTED]

Derived From: Classified By: Reason: Declassify On:	LEAD BUSINESS ANALYST Name: [REDACTED] Program Office: TSC IT Division: TSDC Phone: [REDACTED] Room Number: 31651	FBI OGC/PCLU POC Name: [REDACTED] Phone: [REDACTED] Room Number: 3346
--	---	---

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

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: TSC IT	Signature: [REDACTED] Date signed: 9/10/2012 Name: [REDACTED] Title: Program Manager	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: [REDACTED]
FBIHQ Division: TSC IT	Signature: [REDACTED] Date signed: [REDACTED] Name: [REDACTED] Title: IT Branch Chief	Signature: [REDACTED] Date signed: 9/10/12 Name: [REDACTED] Title: TSC Privacy Officer

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~~

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 FBLGOV (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 (described):

Applicable SORN(s): To the extent a SORN is required for this information, the TSC SORN is applicable, Justice/FBI-019.

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
FBI Privacy and Civil Liberties Officer

Signature:

Date Signed:

Elizabeth Withnell 9/23/12

b3
b7E

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.

b3
b7E

PROCESS

b3
b7E

b3
b7E

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?

☐ 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 ____X____ 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:

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

--

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

8. Is the system operated by a contractor?

☒ No.

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

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

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

--

b3
b7E

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

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

Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

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

10. 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 PLA and/or other actions are required.]

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? July 2008.

2. 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.

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

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

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

_____ Other [Provide brief explanation]:

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

☒ NO ☐ YES

If yes:

a. Provide date/title of the PIA:

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

☐ NO ☐ YES

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Laboratory Network (LabNet)

BIKR FBI Unique Asset ID: 2012-004-01

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: [REDACTED] Program Office: eLAB Division: Laboratory Phone: [REDACTED] Room Number: 5 th Floor	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: ITMD	Signature: Date signed: Name: [REDACTED] Title: Program Manager	Signature: Date signed: Name: [REDACTED] Title: IT Specialist, ITMD Privacy Officer
FBIHQ Division: Laboratory	Signature: Date signed: Name: Title:	Signature: Date signed: Name: John J. Behun Title: Forensic Science Support Section Chief

b6
b7C

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

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

☐ PIA is required by the E-Government Act.

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

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

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

☐ System does not collect, maintain, or disseminate PII.

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

☒ Information in the system relates to internal government operations.

☐ System has been previously assessed under an evaluation similar to a PIA.

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

☐ Other (describe):

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

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

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

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

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	Signature: <input type="checkbox"/>	Date Signed: 8/8/13
Privacy and Civil Liberties Unit	Signature: <i>[Handwritten Signature]</i>	Date Signed: 8/9/13
Christine M. Costello, Acting Deputy General Counsel		
FBI Privacy and Civil Liberties Officer		

b6
b7C

1. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Laboratory Network (LabNet) is a sensitive but unclassified information system that is a subnet of UNet. LabNet provides access to the Laboratory Information Management System (LIMS) [REDACTED] as well as other unclassified Laboratory Division (LD) applications, all of which are separately accredited.

b7E

This Privacy Threshold Analysis is limited to LabNet itself as an infrastructure system and not the various applications residing on LabNet. The scope of the information contained in LabNet is restricted to Active Directory user login identifiers and basic profile information, such as job title, supervisor, email address and phone number. The identifiers allow for access to various applications hosted on LabNet, and are tracked on audit logs. Separate privacy documentation will be prepared for the various applications, including LIMS, that access LabNet.

Access to LabNet is restricted to FBI personnel including contractors, task force members, and detailees to the FBI from other agencies. Upon request and approval through the LabNet network administrator, end users are issued password controlled logon accounts, which allow users to log into LabNet from FBI workstations.

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

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

☒ X YES [If yes, please continue.]

(As noted above, the only PII collected is logon and profile information.)

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.)

b7E

☒ X The information directly identifies specific individuals.

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

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

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

☐ None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. **[If you checked this item, STOP here after providing the requested description.]**

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

☐ NO ☒ X YES

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

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

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

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

☐ NO **[If no, proceed to question 7.]**

☒ X YES

Comment: User login information as well as information contained in audit logs is collected directly from the individual user.

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

☐ NO

☒ X 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.

___X___ NO _____ YES If yes, check all that apply:

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

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

_____ SSNs are important for other reasons. Describe:

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

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

8. Is the system operated by a contractor?

_____ 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: new system; C&A anticipated completion 09/24/2013

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

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

Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

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

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

☒ NO

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

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

☒ NO ☐ YES

12. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

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

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

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

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

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

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

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

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

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

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

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

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

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

_____ Other [Provide brief explanation]:

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

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

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

_____ NO _____ YES

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

UNCLASSIFIED

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Laboratory Information Management System (LIMS)

BIKR FBI Unique Asset ID: 2012-004-01

	SYSTEM/PROJECT POC Name: <input type="text"/> Program Office: eLAB Division: Laboratory Phone: <input type="text"/> Room Number: 5 th Floor	FBI OGC/PCLU POC Name: <input type="text"/> Phone: <input type="text"/> Room Number: JEH 7350
--	--	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: ITMD	Signature: <input type="text"/> Date signed: <input type="text"/> Name: <input type="text"/> 6/19/13 Title: Program Manager	Signature: <input type="text"/> Date signed: <input type="text"/> 6/21/13 Name: <input type="text"/> Title: IT Specialist, ITMD Privacy Officer
FBIHQ Division: Laboratory	Signature: <input type="text"/> Date signed: <input type="text"/> Name: <input type="text"/> Title: <input type="text"/>	Signature: <input type="text"/> Date signed: <input type="text"/> 6/17/13 Name: John J. Behun Title: Forensic Science Support Section Chief

b6
b7C

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

UNCLASSIFIED

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

<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> <p><input type="checkbox"/> System does not collect, maintain, or disseminate PII.</p> <p><input type="checkbox"/> System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).</p> <p><input type="checkbox"/> Information in the system relates to internal government operations.</p> <p><input type="checkbox"/> System has been previously assessed under an evaluation similar to a PIA.</p> <p><input type="checkbox"/> No significant privacy issues (or privacy issues are unchanged).</p> <p><input checked="" type="checkbox"/> Other (describe): System meets the requirement for a "routine database," and is covered by the PIA which covers those systems.</p>	
<p>Applicable SORN(s): FBI-002 (Central Records System)</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 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><input type="checkbox"/> Unit Chief</p> <p>Privacy and Civil Liberties Unit</p> <p>Jacqueline F. Brown, Acting Deputy General Counsel</p> <p>FBI Privacy and Civil Liberties Officer</p>	<p>Signature: <input type="checkbox"/></p> <p>Date Signed: 6/25/13</p> <p>Signature: <i>[Signature]</i></p> <p>Date Signed: 6/25/13</p>

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.

The Laboratory Information Management System (LIMS) is a Commercial Off the Shelf (COTS) product with minor customization to include an interface with STaCSDNA¹. LIMS provides a web-based system for the Laboratory Division (LD) to track evidence, maintain forensic analysis case notes, and generate reports of examination at the unclassified level. Case Notes are defined as the documentation of procedures, standards, controls, instruments used, observations made, results of tests performed, charts, graphs, photos, and other documents generated which are used to support the examiner's conclusions. Reports of Examination are the official report that presents case-related information to a contributor regarding FBI Laboratory activity. Evidence is defined as an item submitted for examination(s). Chain of Custody records all transfers of evidence over which the FBI Laboratory has control.

LIMS is accessible via the Laboratory Network (LabNet), a subnet of UNet, to authorized LD employees, contractors, task force members, and detailees to the LD. The system is not accessible to other FBI Divisions or to the general public. End users will be issued password-controlled logon accounts by the system administrator, which will allow users to log into the LIMS from FBI workstations.

User groups² are established by LD management based on a defined need to know and an appropriate role requiring access to the data. The integrity of the data is preserved through the pre-defined user groups with varying levels of modification privileges. Oversight is provided through the initial grant of access and through the ability to audit system use. (Audits are performed upon request of the FBI Lab.) The system also allows the restriction of case submissions to individual, authorized users to hide sensitive information from improper access or modification.

The LIMS includes personally identifiable information (PII) contained in the LIMS audit log (e.g., user name) and user login identifiers. The system also includes PII that the FBI has legally collected and maintains in other FBI systems, such as Automated Case Support (ACS) and Sentinel, or that is publically available.

¹ Sample Tracking and Control System for Deoxyribonucleic Acid, which is a DNA-specific LIMS used by the LD Nuclear DNA Unit.

² The current user groups are: Administrator, Clerical User, DNA Analyst, Examiner, Examiner Assistant, Firearms Administrator, Firearms User, Resource Administrator, Resource User, Security User, and Supervisor. It is possible that others will be added later.

LIMS captures evidence-related information in database tables. Information inputted by LIMS users includes, but is not limited to:³

- Name, agency, and address of contributor requesting LD services;
- Subject of crime to include name, race, sex, date of birth, and FBI number;
- Victim of crime to include name, race, sex, and date of birth;
- Assigned LD examiners.

The FBI currently manages the flow of evidence through the laboratory in a largely paper-based process, with a limited "in-and-out" database that shows when an item enters the laboratory for testing, when analyses are performed, and when the item leaves the laboratory. There is no division-wide or enterprise capability available. Use of ad-hoc databases and manual stovepipe processes remain the only means of evidence tracking. LIMS is intended to update and improve the current tracking process.

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.]

³ The categories listed herein account for the vast majority of categories of information inputted into the system. It does not preclude the possibility that, on occasion, other information will be provided.

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

Comment: User login information as well as information contained in audit logs is collected directly from the active directory listing and activity of the individual user and is the only information in the system collected directly from subjects.

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 X YES If yes, check all that apply:

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

_____ SSNs 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:**

X It is not feasible for the system/project to provide special protection to SSNs. **Explain:** SSNs are needed to verify the identity of a subject/victim (e.g., ensure correct fingerprint card retrieved from file). Work products provided to contributors, such as Laboratory reports of examination, may include SSNs. Not all users in the system will have access to SSNs.

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. The contractors are operating under the direction of the FBI lab, which has final decision making authority over the system.

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

X NO If no, indicate reason; if C&A is pending, provide anticipated completion date: new system; C&A anticipated completion 08/01/13

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

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

UNCLASSIFIED

Confidentiality: ___Low___Moderate___High___Undefined

Integrity: ___Low___Moderate___High___Undefined

Availability: ___Low___Moderate___High___Undefined

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

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

☒ NO

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

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

☒ NO

☐ YES

12. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

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

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

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

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

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

UNCLASSIFIED

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

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

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

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

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

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

_____ Other [Provide brief explanation]:

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

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

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

___ NO ___ YES

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Medgate

BIKR FBI Unique Asset ID: SYS-0000162

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [REDACTED] Program Office: Office of Medical Services Division: Human Resources Phone: [REDACTED] Room Number: 10909	FBI OGC/PCLU POC Name: [REDACTED] Phone: [REDACTED] Room Number: 7350
--	---	--

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: HCPU Paula Carter or Diane Vogelet	Signature: [REDACTED] Date signed: 6/11/12 Name: [REDACTED] Title: <i>Supervisory Occupational Nurse</i>	Signature: [REDACTED] Date signed: 6/25/2012 Name: [REDACTED] Title: <i>DC, PAMO</i>
FBIHQ Division: Human Resources/ Office of Medical Services (OMS)	Signature: <i>[Signature]</i> Date signed: 6/15/12 Name: <i>DAVID S. WATKINS</i> Title: <i>Section Chief, Office of Medical Services</i>	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.)

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):

If the unclassified version (UHD) is deployed, a PIA will be conducted.

Applicable SORN(s): CRS- FBI-002 & FBI-011 Employee Mailbox Search

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:

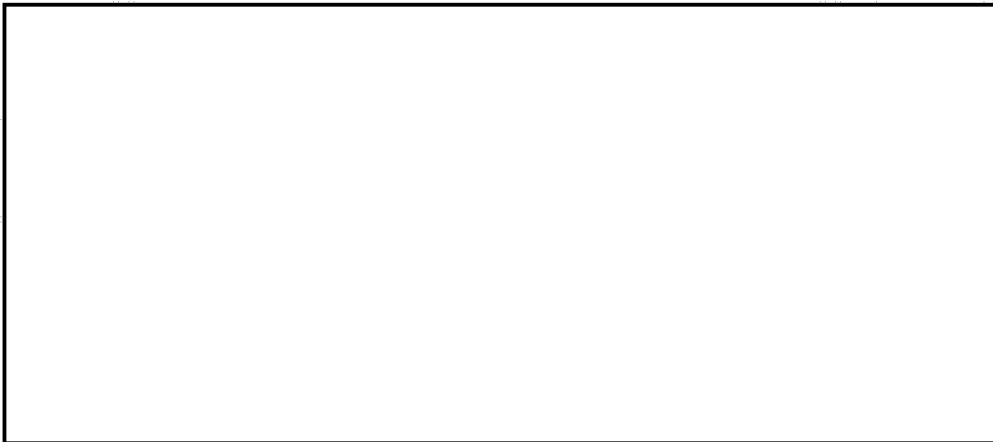
<div style="border: 1px solid black; width: 150px; height: 20px;"></div> Unit Chief	Signature: <div style="border: 1px solid black; width: 150px; height: 20px;"></div>	
Privacy and Civil Liberties Unit	Date Signed: <i>6/25/12</i>	
James J. Landon, Deputy General Counsel	Signature: <i>[Signature]</i>	
FBI Privacy and Civil Liberties Officer	Date Signed: <i>7/5/12</i>	

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.

Medgate is a commercial off-the-shelf (COTS) software application designed for managing and reporting occupational health, safety, and environmental data. The application is used by the Office of Medical Services (OMS) Healthcare Program Unit (HCPU) to support HCPU's clinical record-keeping operations, including mission readiness statistics. It is also used by FBI medical professionals (Occupational Health Nurses and Physicians), industrial hygienists, safety managers, and Drug Deterrence Program (DDP) coordinators to track employee-related health events such as: required Fitness for Duty physicals (FFD); FBIHQ clinic visits and services rendered; immunizations given; lab tests received; and results of safety equipment testing. Additionally, DDP personnel track employee drug screening test types, test dates, and results.



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 The information collected on employees comes from the FBI's Bureau of Personnel Management System (BPMS) and not directly from the employee; however, to the extent that medical information is obtained from the individuals via the forms listed below in 6.b., these forms have Privacy Act notices. These forms are submitted by the employee at the time of their physical to the physician, then mailed to the FBI and the relevant information is entered into Medgate.

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

☒ NO This system supports personnel matters, including Fitness for Duty examinations, DDP testing and other health related issues.

☐ 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: The forms that are filed in Medgate include the FD-1065 (Report of Medical History); used for a FFD physical, the FD-839 (Authorization for Disclosure of Medical Information), FD-789 (Influenza Vaccine) and FD-960 (General Vaccine Consent Form). Privacy Act and/or GINA information notices are included on these forms or will be added as appropriate.

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:** Currently SSNs come from BPMS to Medgate as a Primary ID. The FBI will be replacing the use of SSN by a Unique Employee ID (UEID) in the future.

_____ 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. It is a COTS product but is operated by FBI personnel. There are contract nurses who enter information into Medgate.

_____ 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:

b7E

Provide date of last C&A certification/re-certification: 1/13/11

Confidentiality: ☐ Low ☐ Moderate ☒ High ☐ Undefined

Integrity: ☐ Low ☒ Moderate ☐ High ☐ Undefined

Availability: ☒ Low ☐ Moderate ☐ High ☐ Undefined

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

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

☒ NO

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

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

☒ NO

☐ YES

12. Status of System/ Project:

☐ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 2008

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

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

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

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

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

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

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

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

Privacy Threshold Analysis

NAME OF SYSTEM: **Name Check Litigation Database**

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 changes since April 17, 2003?

☐ YES

☐ NO

(If "yes," please explain the nature of those changes and continue to Question 2.)

(If "no," the PTA is complete and should be sent to the PCLO.)

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 the PTA to the PCLO.)

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

☐ YES

☐ NO

(If the answer to Question 3 is "yes", please provide a brief explanation of the

purpose of the system, the quantity and type of employee/contractor information collected, and whether the system is a Major Information System. If the system is a Major Information System, a full PIA is required. If the system is not a Major Information System, PCLO reserves the right to require a component to conduct a PIA for a system that only collects information on employees/contractors. In either case, please forward the completed PTA to the PCLO.)

(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.)

The Name Check Litigation Database (NCLD) is a limited purpose Microsoft Access database, limited to the collection and storage of name check litigation-specific data. NCLD automates the tracking of civil litigation that alleges a plaintiff’s application for naturalization or adjustment of status has been delayed by the United States Customs and Immigration Service (USCIS), and that this delay is caused in whole or in part by the FBI’s failure to complete plaintiff’s name check. The NCLD thus assists FBI OGC attorneys in defending against allegations that the FBI has not completed Plaintiff’s name check, including litigation where the FBI or other DOJ components are named defendants. The database allows attorneys at the FBI’s Office of the General Counsel (FBI OGC) to monitor the status of FBI’s Records Management Division (FBI RMD) in completing plaintiff’s name check, thus eliminating the need for FBI RMD and FBI OGC personnel to engage in inefficient, time-consuming plaintiff-specific correspondence. The NCLD supplements FBI OGC plaintiff-specific paper case files and is thus subject to any and all attorney-client privileges that attach to FBI OGC work product.

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 the PTA to the PCLO.)

The NCLD collects Plaintiff’s First Name, Last Name, Middle Name, Alien Number, and Date of Birth (if available); the named Defendant (i.e., FBI, FBI & Others, Non-FBI), the FBI OGC Case Number (e.g., the LCMS Number), the OGC Attorney assigned the case, the Date FBI OGC received the Complaint, the name of the FBI RMD Analyst assigned plaintiff’s name check, the Date FBI RMD received the name check Request from USCIS, the Date USCIS Expedited the request (if applicable), the Status of the name check (i.e., complete, pending, or petitioner

unknown), and the Date the name check was Completed.

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

☒

YES

☐

NO

(If the answer to Question 3 is “yes”, please provide a brief explanation of the purpose of the system, the quantity and type of employee/contractor information collected, and whether the system is a Major Information System. If the system is a Major Information System, a full PIA is required. If the system is not a Major Information System, PCLO reserves the right to require a component to conduct a PIA for a system that only collects information on employees/contractors. In either case, please forward the completed PTA to the PCLO.)

(If the answer to Question 3 is “no” go to subsection III to determine if a full or short-form PIA is required.)

The purpose of the system is described at II.1 above. The information is being collected in support of the work of the FBI unit(s) that will use the database for litigation support. Access to the NCLD is limited to FBI OGC attorneys and paralegals tasked with the relevant litigation, and to FBI RMD personnel tasked with completing name check requests from USCIS. The NCLD is protected by user-level passwords, and access is controlled by the Unit Chiefs of the FBI OGC Civil Litigation Units (CLU) by granting or denying access to the CLU computer network drive on the FBI’s internal network system.

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.)

☐

NO

(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.)

(If “no”, a full PIA is required.)

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

[UNCLASSIFIED]

(OGC/PCLU (Rev. 01/05/09))

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

NAME OF SYSTEM / PROJECT: Next Generation Identification Network (NGINet)

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [REDACTED]	Name: [REDACTED]
Reason:	Program Office: Biometric Development Office/ Implementation and Transition Unit	Phone: [REDACTED]
Declassify On:	Division: Criminal Justice Information Services	Room Number: JEH 7338
	Phone: [REDACTED]	
	Room Number: Module D-2	

b6
b7C

FBI DIVISION INTERMEDIATE 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 Manager	Division Privacy Officer
Program Division: CJIS	Signature: [REDACTED] Date signed: 6-11-09 Name: [REDACTED] Title: Assistant Section Chief - Biometric Development Office	Signature: [REDACTED] Date signed: 6-11-09 Name: [REDACTED] Title: CJIS Division Privacy Officer
	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

After all division approvals, forward signed hard copy + 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.)

[UNCLASSIFIED]

[UNCLASSIFIED]

FBI PTA: Next Generation Identification Network (NGINet)

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

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

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

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

- [redacted]
- 1 - RMD/RMAU (attn: [redacted])
 - 2 - Program Division POC /Privacy Officer
 - 2 - FBIHQ Division POC /Privacy Officer

b6
b7C

[UNCLASSIFIED]

[UNCLASSIFIED]

FBI PTA: Next Generation Identification Network (NGINet)

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): FBI-009 (FIRS); DOJ-002 (DOJ Computer Systems Activity and Access Records)

SORN/SORN revision(s) required? ☐ No ☒ Yes (indicate revisions needed): Include test data and test data subjects in pending revision to FBI-009.

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.

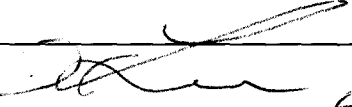
Other:

[Redacted area]

b7E

Under these circumstances, NGINet relates to internal government operations, and completion of a PIA is not required.

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

Signature: 
Date Signed: 6/27/09

★ Approved conditional on

[Redacted area]

b7E

[UNCLASSIFIED]

[UNCLASSIFIED]

FBI PTA: Next Generation Identification Network (NGINet)

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.):

Next Generation Identification Network (NGINet)

The NGINet is the infrastructure supporting the collaboration between the FBI and its contractor Lockheed Martin (LM) on the Next Generation Identification (NGI) project.¹ NGINet [REDACTED]

[REDACTED]

b7E

[REDACTED]

b7E

[REDACTED]

b7E

[REDACTED]

b7E

[REDACTED]

b7E

[REDACTED]

b7E

¹The NGI development and integration contract was awarded in FY 2008 and consists of a base year for development with nine option years. The contract included Privacy Act clauses 52.224-1 and 52.224-2.

[UNCLASSIFIED]

[UNCLASSIFIED]

FBI PTA: Next Generation Identification Network (NGINet)

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

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

[Redacted]

b7E

[UNCLASSIFIED]

[UNCLASSIFIED]

FBI PTA: Next Generation Identification Network (NGINet)

PII will be minimal

b7E

b7E

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

____ NO. X YES.

As indicated, the system is used for testing pursuant to the contract.

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

 X NO (mostly). X YES (in some instances).

For the most part, information in the system will not be retrieved by personal identifiers.

b7E

b7E

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

 X NO. ____ YES. **If yes, check all that apply:**

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

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

____ SSNs are important for other reasons. **Describe:**

[UNCLASSIFIED]

[UNCLASSIFIED]

FBI PTA: Next Generation Identification Network (NGINet)

_____ 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?

 X 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:

 X YES. If yes, provide date of last C&A certification/re-certification: 04/28/2009

_____ Don't Know.

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

 X 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)?

 X NO.

_____ YES.

_____ Don't know.

[UNCLASSIFIED]

[UNCLASSIFIED]

FBI PTA: Next Generation Identification Network (NGINet)

10. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

 YES. If yes, indicate which of the following changes were involved **(mark all boxes that apply):**

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

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

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

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

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

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

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

 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]:**

[UNCLASSIFIED]

[UNCLASSIFIED]

FBI PTA: Next Generation Identification Network (NGINet)

3. Does a PIA for this system/project already exist? _____ NO. _____ YES. If yes:

a. Provide date/title of the PIA:

b. Has the system/project undergone any significant changes since the PIA? ____ NO. ____ YES.

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

[UNCLASSIFIED]

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

Total Deleted Page(s) = 1
Page 4 ~ b7E;

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: National Name Check Program (NNCP)

BIKR FBI Unique Asset ID: SYS-0000061

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [REDACTED]	Name: [REDACTED]
Reason:	Program Office: SSS/CMSU	Phone: [REDACTED]
Declassify On:	Division: IT Services	Room Number: JEH 7350
	Phone: [REDACTED]	
	Room Number: JEH 8998	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Records Management	Signature: <i>Edward W. Reinhold</i> Date signed: 1/2/2013 Name: Edward W. Reinhold Title: Section Chief, NNCP	Signature: <i>David M. Hardy</i> Date signed: 1/3/2012 Name: David M. Hardy Title: Section Chief, Record / Information Dissemination Section
FBIHQ Division: IT Services	Signature: <i>Leslie J. Smith</i> Date signed: 12/17/2012 Name: Leslie J. Smith Title: Acting Section Chief, Systems Support	Signature: [REDACTED] Date signed: 12/17/12 Name: [REDACTED] Title: IT Services Privacy Officer

b6
b7C

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

☒ PIA is required by the E-Government Act. ** A PIA will be drafted for the National Name Check Program, which will describe the NNCP system and the Name Check Dissemination Database (NCDD), which is part of a larger system known as RMD Document Processing System (RDPS).

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

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

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

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Applicable SORN(s): FBI-002, The FBI Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. 17,200 (Mar. 29, 2001), 66 Fed. Reg. 33,558 (June 22, 2001), 70 Fed. Reg. 7513, 17 (Feb. 14, 2005), 72 Fed. Reg. 3410 (Jan. 25, 2007).

Notify FBI RMD/RIDS per MIOG 190.2.3? X 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? X No Yes :

Prepare/revise/add Privacy Act (e)(3) statements for related forms? X 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:

 Acting Unit Chief
 Privacy and Civil Liberties Unit
 Christine M. Costello, Acting Deputy General
 Counsel and Acting FBI Privacy and Civil Liberties
 Officer

 Signature
 Date Signed: 1/14/2013
 Signature: [Signature]
 Date Signed: 1-14-2013

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.

The National Name Check Program (NNCP) Section is part of the Records Management Division (RMD) of the FBI. The mission of the NNCP Section is to disseminate information from FBI files for the purpose of protecting the United States from espionage and terrorism, in response to name check requests received from offices within the FBI, other Federal agencies or components thereof, offices from the Legislative and Judicial branches of the Federal Government [REDACTED]

b7E

[REDACTED] Executive Order 10450 authorizes the NNCP Section to conduct National Agency Checks as part of the pre-employment vetting process and background investigation. Under Executive Order 12333, the FBI coordinates counterintelligence activities, by members of the Intelligence Community, necessary for the conduct of foreign relations and the protection of the national security of the United States.

To accomplish its mission, the NNCP Section uses an automated information technology system called the NNCP system to process name check requests submitted by a variety of customers.

In order to provide information to meet customer needs, the NNCP system electronically searches data [REDACTED]

b7E

[REDACTED] which include records from FBI Headquarters, FBI Field Offices, and Legal Attache Offices. Records accessed from these locations contain FBI investigative, administrative, personnel, and general files.

Name check requests are submitted by customer agencies [REDACTED]

b7E

b7E

b7E

b7E

The NNCP system is accessible to authorized FBI personnel (including contractors) via the Secret Enclave, the FBI's secure internal network which is accredited to contain information classified at or below Secret. Within the FBI, access to the NNCP system is generally restricted to RMD personnel involved in the name check process or to IT specialists responsible for system administrative functions. On a very limited basis, access to the NNCP system is granted to personnel in other FBI units, such as the Security Division and Office of General Counsel, for the purpose of reviewing name check results.

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, please stop.]

X YES [If yes, please continue.]

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

X The information directly identifies specific individuals.

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

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

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

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

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.] However, the submitter of the name check request obtains the information directly from the person who is the subject of the request, and that person has provided consent in most cases.

☐ 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.

 X SSNs are important for other reasons. **Describe:**

SSNs are initially submitted as part of a name check request and used as a search element. Further, as the technology currently exists, SSNs may be included in responses back to the requester.

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

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

8. Is the system operated by a contractor?

 X NO

____ YES. Information systems operated by contractors for the FBI may be considered Privacy Act systems of records. The Federal Acquisition Regulation contains standard contract clauses that must be included in the event the system collects, maintains or disseminates 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:

May 27, 2012 (as part of the Investigative Mainframe Applications C&A)

Confidentiality: ____Low ____Moderate X High ____Undefined

Integrity: ____Low ____Moderate X High ____Undefined

Availability: ☐ Low ☐ Moderate ☒ High ☐ Undefined☐ Not applicable -- this system is only paper-based.

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

☒ NO☐ YES If yes, please provide the date and name or title of the OMB submission:

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

☒ NO☐ YES If yes, please describe the data mining function:

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

☒ NO ☐ YES

13. Status of System/ Project:

☐ This is a new system/project in development.**II. EXISTING SYSTEMS / PROJECTS**

1. When was the system/project developed?

Development of the current NNCP system architecture began in the mid-1990s. The application was deployed in September 2000.

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.

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

b7E

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

_____ Other [Provide brief explanation]:

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

 X NO _____ YES

A PIA for the NNCP system was previously completed on April 27, 2007. Because the NNCP system was in existence prior to the enactment of FISMA, no PIA was completed.

If yes:

a. Provide date/title of the PIA:

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

..... NO YES

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: Personnel Recovery Isolated Personnel Reports (ISOPREPs)

	SYSTEM/PROJECT POC Name: <input type="text"/> Program Office: Personnel Recovery Division: DO Phone: <input type="text"/> Room Number: Aquia	FBI OGC/PCLU POC Name: <input type="text"/> Phone: <input type="text"/> Room Number: 7438
--	--	---

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager	Division Privacy Officer
Program Division: Personnel Recovery Coordination Group (PRCG)	Signature: Date signed: approved 8/5/2009 Name: <input type="text"/> Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Director's Office	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

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

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

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

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

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

1 - DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov)

(if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)

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

1 - FBI SecD/AU (electronic copy: via e-mail to UC)

1 - RMD/RMAU (attn:)

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

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 type="checkbox"/> PIA is not required for the following reason(s):</p> <p style="padding-left: 40px;"><input type="checkbox"/> System does not collect, maintain, or disseminate PII.</p> <p style="padding-left: 40px;"><input type="checkbox"/> System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).</p> <p style="padding-left: 40px;"><input checked="" type="checkbox"/> Information in the system relates to internal government operations. <i>Information relates only to FBI personnel. PTA completed out of abundance of caution, but information will be maintained on a DOD database rather than on an FBI system.</i></p> <p style="padding-left: 40px;"><input type="checkbox"/> System has been previously assessed under an evaluation similar to a PIA.</p> <p style="padding-left: 40px;"><input type="checkbox"/> No significant privacy issues (or privacy issues are unchanged).</p> <p style="padding-left: 40px;"><input type="checkbox"/> Other (describe):</p>		
<p>Applicable SORN(s): CRS</p> <p>Notify FBI RMD/RIDS per MIOG 190.2.3? <input type="checkbox"/> No <input checked="" type="checkbox"/> Yes (see sample EC on PCLU intranet website).</p> <p>SORN/SORN revision(s) required? <input type="checkbox"/> No <input type="checkbox"/> Yes (indicate revisions needed):</p>		
<p>Prepare/revise/add Privacy Act (e)(3) statements for related forms? <input 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>		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;">David C. Larson, Deputy General Counsel</td> <td style="width: 50%; padding: 5px;">Signature: David C. Larson</td> </tr> </table>	David C. Larson, Deputy General Counsel	Signature: David C. Larson
David C. Larson, Deputy General Counsel	Signature: David C. Larson	

FBI Privacy and Civil Liberties Officer

Date Signed: 9/25/2009

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. FBI personnel who deploy to theaters of war are required to complete Isolated Personnel Reports (ISOPREPs) prior to their deployment. This form solicits general information such as

[redacted] that a recovery team would need to plan a recovery as well as information that only the person completing the form would know. The information can be used by a recovery team to authenticate missing personnel. The ISOPREP form is needed in order to quickly leverage the recovery architecture that the Department of Defense (DoD) has in the theater. The ISOPREPs are classified CONFIDENTIAL once they are completed and transmitted to the Personnel Recovery Coordination Group (PRCG) via FBINET. The PRCG then electronically imports the forms into the DoD's classified database. Only approved ISOPREP managers and Rescue Coordination Centers have access to the ISOPREPs via the database. [redacted]

b7E

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

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

☒ YES. [If yes, please continue.]

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

☐ NO. ☒ YES.

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

☐ NO. ☒ YES.

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

☐ NO. ☒ YES. If yes, check all that apply:

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

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

☒ SSNs are important for other reasons. **Describe:** DoD has determined that the SSN is the most unique identifier for all personnel. Therefore, the SSN is used to create the ISOPREP account.

☐ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:** The database is maintained on the DoD's Secret Internet Protocol Router. This is their classified system that is used to process information up to the SECRET level. Additionally, only vetted ISOPREP managers and Rescue Coordinators may retrieve the data.

☐ 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 statement (either on the collection form or via a separate notice)? Privacy Act (e)(3)

☐ 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: A C&A has not been done on this project because the information collected will be maintained on a Department of Defense database.

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

☐ Don't Know.

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

☒ NO.

☐ Don't know.

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

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

☒ NO.

☐ YES.

☐ Don't know.

10. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? It was developed by the DoD in 2000.

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):

 X 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.

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

_____ Other. [Provide brief explanation]:

3. Does a PIA for this system/project already exist? X NO. _____ YES. If yes:

a. Provide date/title of the PIA:

b. Has the system/project undergone any significant changes since the PIA? _____ NO. _____ YES.

FBI PTA: Personnel Recovery Isolated Personnel Reports

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

Unclassified//FOUO

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

NAME OF SYSTEM / PROJECT: Professional Flight Management (PFM)

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [REDACTED] Program Office: Aviation Surveillance Branch Division: CIRG Phone: [REDACTED] Room Number: N/A	FBI OGC/PCLU POC Name: [REDACTED] Phone: [REDACTED] Room Number: 7458

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Division: Critical Incident Response Group (CIRG)	FBIHQ Division: CIRG
Program Manager	Signature: /s/ Date signed: Name: [REDACTED] Title: Supervisory Special Agent, Aviation Support Unit	Signature: /s/ Date signed: Name: J. Britt Johnson Title: Section Chief, Surveillance and Aviation Section (SAS)
Division Privacy Officer	Signature: Date signed: /s/ Name: Kenneth R. Gross, Jr. Title: SSA/CDC	Signature: Date signed: Name: Title:

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

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

PIA required: ____No ____X_Yes: _____		SORN/SORN revision required: ____No ____X_Yes: _____	
Applicable SORN(s):			
Notify FBI RMD/RID5 per MIOG 190.2.3: ____No ____Yes			
Consult with RMD to identify/resolve any Federal records/electronic records issues: ____No ____Yes:			
Prepare/revise/add Privacy Act (e)(3) statements for related forms? ____No ____Yes-forms affected:			
Other:			
David C. Larson, Deputy General Counsel FBI Privacy and Civil Liberties Officer		Signature: /s/ Date Signed: 11/25/2009	

Unclassified//FOUO

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Professional Flight Management (PFM)

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 Ticker

b6
b7C

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Professional Flight Management (PFM)

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Name of the system/project. Provide current name, any previous or anticipated name changes, and any associated acronyms:
Professional Flight Management (PFM)

2. Briefly describe the system's/project's structure (including identification of any components/subsystems or parent system, if applicable).

This database is a proprietary database [redacted] and is hosted on a server connected to the FBI Net Secret Enclave.

b7E

3. What is the purpose for the system/project?

This project is in development to replace the Bureau Aviation and Operations (BAO) mainframe computer program for scheduling, tracking and recording operational flight data. This effort is mandated by 41 CFR Section 102-33. This Government Management Regulation requires that all Federal Agencies maintain aviation records in the GSA's FAIRS (Federal Aviation Information and Records System), the intelligence agencies of the U.S. are not required to report to FAIRS but, "must maintain" records in accordance with FAIRS. The PFM Program will accomplish this. PFM collects data from all FBI Divisions with Aviation Programs as well as the Special Flight Operations, Field Flight Operations and the Tactical Helicopter Units within the Critical Incident Response Group (CIRG).

PFM is a Windows based application intended to be the long term replacement for BAO. BAO had limited functionality and did not meet all the requirements mandated by OMB A-126, A-123, A-76 and 41 CFR Section 102-33. PFM was identified as meeting the record keeping requirements set forth via OMB A126, A123, A76 and 41 CFR §§ 102-33. It also meets an FBI Enterprise requirement to move to Windows and Web based applications. All FBI flight operations are now using PFM for flight record keeping purposes.

4. Please provide a general summary of the nature of information in the system/project and how it will be used: PFM will be primarily used to [redacted] record data on the flights and process reports for analysis and official reporting requirements. There are other features in the database that can maintain [redacted] concerns of aircraft.

b7E

5. 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. **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.

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Professional Flight Management (PFM)

b7E

6. Access

- a. Describe the means of accessing the system/project and transmitting information to and from the system/project:

b7E

This database is currently operating in a limited capacity; however, it is intended, once technical/security concerns are resolved, to be accessible across the FBI Net Secret Enclave by all FBI entities with an Aviation Program.

- b. Describe who within the FBI will have access to the information in the system and the controls for ensuring that only authorized persons can access the information:

The information in this system is specifically part of the FBI's Aviation Mission and its responsibilities. Those individuals who meet all the requirements to maintain their FBI Net Secret Enclave user account, with a need-to-know and authorized by the Field Flight Operations (FFO) Unit, ASB, will be granted access to the actual database.

b7E

- c. Describe who outside the FBI will have access to the information in the system/project and the controls for ensuring that only authorized persons can access the information:

This system is not accessible outside of the FBI Net Secret Enclave. This system is only accessible by FBI personnel, cleared contractors or JTTF.

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

 X NO

 YES. If yes, provide a brief explanation of the quantity and type of information:

8. 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

9. Are Social Security Numbers collected, maintained or disseminated from the system/project?

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Professional Flight Management (PFM)

 X NO

 YES. If yes, for systems/projects **other than** those supporting law enforcement or intelligence activities:

- What is the purpose for the collection, maintenance or dissemination of SSNs?

- Is it feasible to eliminate SSNs from the system/project (please indicate why or why not)?

- In light of Federal policy to reduce the use of SSNs, is it feasible to minimize system/project-user access to SSNs in the system/project (why or why not)?

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

 NO

 X YES. If yes, for systems/projects **other than** those relating to criminal investigations, CT, or CI:

- Indicate how such information is collected:

Only data related to

b7E

- Identify by name and form number any forms used to request such information from the information subject (this includes paper or electronic forms):

No specific forms, recorded in unique electronic data base.

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

No

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

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

This project is currently a part of the FBI/Net Secret Enclave; however, the application may have to be placed under a separate C&A. There is no effort to do that at this time or currently required by the Security Division.

b7E

 YES. If yes, please:

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

 Don't Know

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Professional Flight Management (PFM)

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

☒ NO ☐ Don't know

☐ YES. If yes, if the name of the OMB 300 is not the same as the name of the system/project, please provide OMB name:

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

☒ NO ☐ YES ☐ Don't know

14. Status of System/ Project:

☒ This is a new system/ project in development. [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.]

☐ This is an existing system/project. [Continue to Section II.]

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

☐ YES. If yes, indicate which of the following changes were involved {mark all boxes that apply}:

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Professional Flight Management (PFM)

- _____ 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. [Please provide brief explanation]:

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

_____ NO

_____ YES. If yes, please provide date/title of the PIA:

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 .

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED] b7E

BIKR FBI Unique Asset ID: NEN-0000076

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [REDACTED] (ITSD)(CON) Program Office: Sentinel Division: ITED/EES/CMEU Phone: [REDACTED] Room Number: Sentinel Facility Hernden, VA	FBI OGC/PCLU POC Name: [REDACTED] (OGC)(FBI) Phone: [REDACTED] Room Number: FBIHQ – JEH – 7350
--	---	--

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Case Management Engineering Unit (CMEU)	Signature: [REDACTED] Date signed: 1/27/14 Name: [REDACTED] (ITED) (FBI) [REDACTED] Title: SSA / Acting Unit Chief	Signature: [REDACTED] Date signed: Name: Title:
FBIHQ Division: Information Technology Engineering Division (ITED) Enterprise Engineering Section (ESS)	Signature: [REDACTED] Date signed: 1-30-2014 Name: [REDACTED] (ITED) (FBI) Title: Unit Chief	Signature: [REDACTED] Date signed: 1/28/2014 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.)

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): N/A

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

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

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

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

Other:

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

Signature: 

Date Signed: 2/5/2014

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. (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.):

b7E

b7E

Users
 are FBI personnel and contractors. To facilitate user-to-user communications their full names are stored on the system, but no other data about users is collected, stored or maintained on the system.

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)?

 X 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.]

- Other than the collection of names of employees and contractors who have access to the system, the system does not collect, maintain, or disseminate any information about individuals.

 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 SecD)?

_____ NO

_____ YES

12. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

_____ NO _____ YES

If yes:

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

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

_____ NO _____ YES

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

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

FBI PRIVACY/ACCESS/ETC. (PAC) (OGC/PCLU) (PTA)

NAME OF SYSTEM / PROJECT: Provisioning and Access Control (PAC) System

BIKR FBI Unique Asset ID: 2010-011-01-P-404-140-9999

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [REDACTED]	Name: [REDACTED]
Reason:	Program Office: ITPMS/APU	Phone: [REDACTED]
Declassify On:	Division: ITMD	Room Number: HQ-7350
	Phone: [REDACTED]	
	Room Number: Crystal City #400	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: ITMD	Signature: [REDACTED] Date signed: 11/26/12 Name: [REDACTED] Title: APU Unit Chief	Signature: [REDACTED] Date signed: 11/26/12 Name: [REDACTED] Title: IT Specialist
FBIHQ Division: ITED	Signature: [REDACTED] Date signed: 11/26/12 Name: [REDACTED] Title: ISMEU Unit Chief	Signature: [REDACTED] Date signed: 11/26/12 Name: William Searcy Title: Enterprise Engineering Section Chief

b6
b7C

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

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [This section will be completed by the FBI PCLU/PCLO following PIA 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 Computer Systems Privacy & Access Records - 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_es.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:

	Signature:	
Privacy and Civil Liberties Unit	Date Signed:	3/6/12
James J. Landon, Deputy General Counsel	Signature:	
FBI Privacy and Civil Liberties Officer	Date Signed:	3/7/12

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description 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.

Provisioning and Access Control (PAC) System

The Information Technology Branch's implementation of the Provisioning and Access Control (PAC) system will fulfill an immediate need to modernize and expedite access processes across the organization. Central to these efforts is the utilization of a primary technology tool (Oracle Identity Manager Suite) which deliver access improvement solutions to all employees no matter where they are located, providing "one-stop shopping" for user access needs.

The overall objective of PAC is to provide an enterprise level identity management solution for the FBI. To address this complex endeavor, the ITB has developed an incremental strategy that involves the execution of individual task orders. The initial task order will establish a foundational identity management framework to support the capability to provision/de-provision basic access privileges with future task orders focusing on the more advanced features of identity management on the main FBI network (FBINET). The FBI plans to execute additional task orders to implement the advanced capabilities over the next couple of years pending availability of funding. Additional privacy documentation will be prepared as necessary.

In the initial task order, Oracle Identity Manager (OIM) will function as a backend service that will interface with the mainframe to allow for a self-service mainframe [REDACTED] is currently a manual process that must be performed by the Enterprise Operations Center (EOC) help desk administrator. Also, as part of the first task order, PAC will interface with the Enterprise Process Automation System (EPAS) to receive those Security Access Request (SAR) provisioning tickets specifically for access to the core set of systems and applications for all new employees. Once PAC receives the SAR tickets, it will automate the provisioning process to establish accounts for new employees and the de-provisioning of accounts once employees leave the Bureau. To provide the core IT system components, the PAC system will interface with the following systems and applications: EDS, Microsoft Active Directory, Microsoft Exchange, Microsoft Office Communications Server, WebTA, Microsoft SharePoint/MySite and User Home Drive. Once the PAC System is fully implemented, it will connect with the following networks, systems, and applications:

b7E

- FBINET (potentially UNET and NGSCION)

UNCLASSIFIED

- Mainframe
- Bureau Personnel Management System (BPMS)
- PKI Shadow Directory
- Active Directory (AD)
- Enterprise Directory Services (EDS)
- Microsoft Exchange
- Microsoft Office Communications Server
- WebTA
- Microsoft SharePoint/MySite
- User Home Drive

PAC will function as an enterprise system and be available to all users on FBINet, including full-time, part-time, and contract personnel, as well as any other persons requiring access. Supervisory personnel (Authoritative Users) and system administrators will have role-based authority to approve access requests and conduct system maintenance, respectively. For example, upon an employee's EOD, separation from employment, or assumption of new roles within the FBI, supervisors will be able to use a PAC dashboard to electronically authorize or revoke an employee's system access rights across FBINet. In addition, all users will be able to utilize a self-service interface to request access to desired applications and specific software packages, and subsequently track the status of those requests online.

A limited amount of personally identifiable information (PII) will be needed by PAC in order to correlate a proposed user with his/her digital identity in the desired IT application or system. PII contained in the Bureau Personnel Management System (BPMS) will be imported to PAC to facilitate processing access requests. PII contained in PAC includes the user's name, FBI unique identifying number, and social security number (SSN), which is the universal identifier in BPMS. Other than the information necessary to complete a specific task, such as the proposed user's name, no other PII will be visible to the individual approving the request. Further, other than that approving authority, no other users of the system will be able to see any PII relating to any other user. PAC user screens will not display user SSNs. SSNs are used by PAC only for electronic matching of access records in the various FBI systems that currently still use the SSN as the primary identifier. Moving forward, it is expected that, wherever possible, other less sensitive attributes, such as the FBI unique ID, will be used to maintain these accounts throughout its lifecycle.

PAC will reside in the Distributed Application Virtual Environment (DAVE), and will assume physical security constraints inherent to that environment. All access to and activities conducted within the PAC system by users and administrators are logged and auditable. In addition, PAC provides the Bureau with audit and reporting capabilities that reflect who has access to what systems and how that access was granted.

2. Does the system/project collect, maintain, or disseminate any information about individuals (e.g., identifying or natural person)?

UNCLASSIFIED

UNCLASSIFIED

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

 X YES [If yes, please continue.]

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

 X The information directly identifies specific individuals.

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

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

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

 None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. [If you checked this item, STOP here after providing the requested description.]

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

 NO X YES

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

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

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

The information about individuals contained within PAC will pertain only to FBI personnel (including contractors and task force officers); no information about non-FBI personnel will be contained in PAC.

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

UNCLASSIFIED

EPIC-205

UNCLASSIFIED

☒ 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 PCILU to develop/implement the necessary form(s).]

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

Notice to individuals is provided by the following published System of Records Notices (SORNs): Bureau Personnel and Management System, Justice/FBI-008, 58 Fed. Reg. 51846, 51874; and DOJ Computer Systems and Activity and Access Records, DOJ-002, 64 Fed. Reg. 73585.

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:

While PAC itself will use the Unique Employee Identifier (UEID) for personnel identification purposes, SSN is the common attribute that will be used to link identities to

UNCLASSIFIED

accounts in other legacy systems that have not yet implemented the UEID in place of the SSN. SSNs will not be exposed to the system user.

☒ 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:

SSNs in PAC will not be viewable by any system user. In addition, SSNs will be placed in protected status. The SSN field will be hidden from the user profile dashboard view. The SSN field will also be encrypted.

☐ 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.

Describe:

The PAC System will reside within the DAVE environment and Operations and maintenance (O&M) performed by FBI and contractor personnel. Fundamental platform and environment O&M will become the responsibility of the DAVE facility administrators, with specific system function O&M the responsibility of the Information Technology Services Division (ITSD) Directory Services Support Unit. A comprehensive transition plan will provide required training and facilitate appropriate knowledge transfer to the O&M group. The ITSD organization that will be responsible for PAC will be identified early in the development process and be involved throughout the development cycle so that transfer of knowledge is conducted properly. Contractor support for second or third level resolution will be determined at a later date.

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:

UNCLASSIFIED

UNCLASSIFIED

Anticipate Release of Information (AR) and/or other appropriate certification for the Application Server Environment (AVE) and/or other Environment (DAVE). When completed, it is expected to rate at the same levels of DAVE: High Confidentiality, High Integrity, and High Availability.

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

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

Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined

Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

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

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

☒ 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. 110-537?

☒ NO

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

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

☒ NO

☐ YES

Note: It is anticipated that during Phase 3 of its implementation, PAC will ultimately replace EDS. EDS is currently a FISMA system, and thus at that time it is possible PAC will be determined to be a FISMA system.

13. Status of System/ Project:

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

UNCLASSIFIED

UNCLASSIFIED

submitter. The submitter must provide a rationale for the request and determination if PII. Project descriptions are:

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

_____ YES If yes, indicate which of the following changes were involved (mark all boxes that apply):

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

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

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

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

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

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

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

_____ 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.

UNCLASSIFIED

UNCLASSIFIED

_____ Changes do not involve a change in the type of records maintained,
the frequency of collection, or the retention period.

_____ Other [Provide brief explanation]:

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

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

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

_____ NO _____ YES

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

UNCLASSIFIED

EPIC-210