

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

PIA is required by the E-Government Act. *Sup to this PIA will be part of an overall PIA for N91*
 PIA is to be completed as a matter of FBI/DOJ discretion.

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

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

Applicable SORN(s): Section 1 / FBI-009



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: *In progress*

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

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

Other:

<input type="checkbox"/> Unit Chief Privacy and Civil Liberties Unit	Signature:  Date Signed: <i>3/5/12</i>
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature:  Date Signed: <i>3/21/12</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.

The Global Operations Section (GOS) Global Initiatives Unit (GIU) of the Criminal Justice Information Services (CJIS) Division manages the mobile Biometric Identification Tools Program (B-iD) biometric collection devices. These devices, either Quick Capture Platforms (QCP) or Flyaway kits, are state-of-the-art biometric devices that allow investigators to collect fingerprint data, other identifying information, and available biographic data to validate a subject's identity through rapid identification services. The QCP and Flyaway kits enable instant access to federal fingerprint databases—the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System (IAFIS), the Department of Defense's Automated Biometric Identification System (ABIS), [REDACTED]

b7E

QCP and Flyaway devices consist of a laptop, fingerprint scanner, camera, military battery and cellular air card or satellite communication equipment. The devices have different laptops and the software is configured for different mission sets. [REDACTED]

b7E

Authorized FBI personnel are the only users permitted to access or operate the QCP and Flyaway devices. QCP devices are deployed both within and outside of the United States, on the Southwest border, and in maritime situations. They frequently are deployed to combat theatres such as Iraq and Afghanistan, other hostile environments, and remote areas where access to CJIS services would otherwise be impossible. The devices have assisted frontline FBI investigators with identifying terrorists and transnational criminals. They are also used by various FBI task forces, such as Crimes against Children, Safe Streets, and Violent Crimes.

Flyaway devices also are deployed both within and outside of the United States. Domestically, the devices support national special security events, humanitarian rescue and recovery, and mass arrest scenarios. In addition, the Flyaway or QCP devices may be used domestically by FBI agents during investigatory detentions, incident to arrests, and when the subjects provide consent. A February 2011 opinion from the FBI's Office

of the General Counsel provides guidance regarding the domestic use of these biometric collection devices.



b7E

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

NO

YES

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.

The information directly identifies specific individuals.

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

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

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

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

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

NO YES

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

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

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

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

NO [If no, proceed to question 7.]

YES

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

NO

YES [If yes, proceed to question 7.]

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

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

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

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

NO YES If yes, check all that apply: The software does not recognize SSN as a required field nor does it have an optional field for the SSN. However, an authorized user may place a SSN in the Remarks field. The software stores the information in the Remarks field but it is not searchable by SSN.

..... 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: Estimated December 31, 2011. The systems accessed by the devices (IAFIS, ABIS, IDENT) have independent C&A.

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.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 2007

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

UNCLASSIFIED

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

b7E

BIKR FBI Unique Asset ID: NEN-0000023

SYSTEM/PROJECT POC	ALTERNATE SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: <input type="text"/>	Name: <input type="text"/>	Name: <input type="text"/>
Program Office: Enclave Support Unit Customer Support Section	Program Office: Information Systems Security Unit	OGC/Privacy and Civil Liberties Unit
Division: Information Technology Services	Division: Security Division	Phone: <input type="text"/>
Phone: <input type="text"/>	Phone: <input type="text"/>	Room Number: JEH, Rm 7350
Room Number: JEH, Rm 9988	Room Number: SPYB F-601	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Enclave Support Unit	Signature: <input type="text"/> Date signed: 5/11/11 Name: <input type="text"/> Title: Enclave Program Manager	Signature: <input type="text"/> Date signed: Name: Title:
FBIHQ Division: Network Support Section	Signature: <i>Steve P. Shelton</i> Date signed: 5/11/11 Name: Name: Steve Shelton Title: Section Chief, Network Support Section, ITSD	Signature: <input type="text"/> Date signed: 5-13-11 Name: <input type="text"/> Title: ITB Division Privacy Office

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

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

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

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

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

Applicable SORN(s): DOJ-002, DOJ Computer Systems Activity & Access Records; JUSTICE/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

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

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

Other:

[Redacted]	Unit Chief	Signature:	[Redacted]
Privacy and Civil Liberties Unit		Date Signed:	1/15/11
James J. Landon, Deputy General Counsel		Signature:	[Signature]
FBI Privacy and Civil Liberties Officer		Date Signed:	6/16/11

b6
b7c

UNCLASSIFIED

UNCLASSIFIED

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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



b7E

UNCLASSIFIED

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

NO

YES

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.]

UNCLASSIFIED

..... 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:

UNCLASSIFIED

UNCLASSIFIED

_____ 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:
November 20, 2008.

Confidentiality: ___Low Moderate ___High ___Undefined

Integrity: ___Low ___Moderate High ___Undefined

Availability: ___Low ___Moderate High ___Undefined

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

UNCLASSIFIED

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?

b7E

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.

UNCLASSIFIED

_____ 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

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

Total Deleted Page(s) = 9

- Page 4 ~ b7E;
- Page 5 ~ b7E;
- Page 6 ~ b7E;
- Page 7 ~ b7E;
- Page 8 ~ b7E;
- Page 9 ~ b7E;
- Page 10 ~ b7E;
- Page 11 ~ b7E;
- Page 12 ~ b7E;

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


Unclassified

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Bureau Personnel Management System (BPMS)

BIKR FBI Unique Asset ID: SYS0000008

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [Redacted] Program Office: HRASU Division: ITSD Phone: [Redacted] Room Number: 1907	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number: JEH 7350
--	--	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: IT Services Division	Signature: [Redacted] Date signed: 7/26/2012 Name: [Redacted] Title: Supervisory IT Specialist (Unit Chief)	Signature: Date signed: Name: Title:
FBIHQ Division: Human Resources Division	Signature: Date signed: Name: David G. Bennett Title: Assistant Director	Signature: Date signed: Name: [Redacted] Title: Division Privacy Officer for ITB

b6
b7C

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS

PIA is required by the E-Government Act.

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

Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? Yes. No (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): Justice/FBI-008, Bureau Personnel Management System (BPMS), 58 Fed. Reg. 51,875 (Oct. 5, 1993), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001) and 72 Fed. Reg. 3410 (Jan. 25, 2007).

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): Revised system of records needed in order to accurately reflect increase in collection of information and the manner in which the information is stored and used.

Prepare/revise/add Privacy Act (e)(3) statements for related forms? No Yes (indicate forms affected): HRD should continue to work with OGC's PCLU to review new and existing forms to ensure that the requirements of 5 U.S.C. § 552a(e)(3) are met.

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	Signature: Date Signed:	7/26/12
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed:	7/27/12

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.

System Overview:

The Bureau Personnel Management System (BPMS) is an FBI system that supports integrated human resource and payroll functions. [REDACTED]

b7E

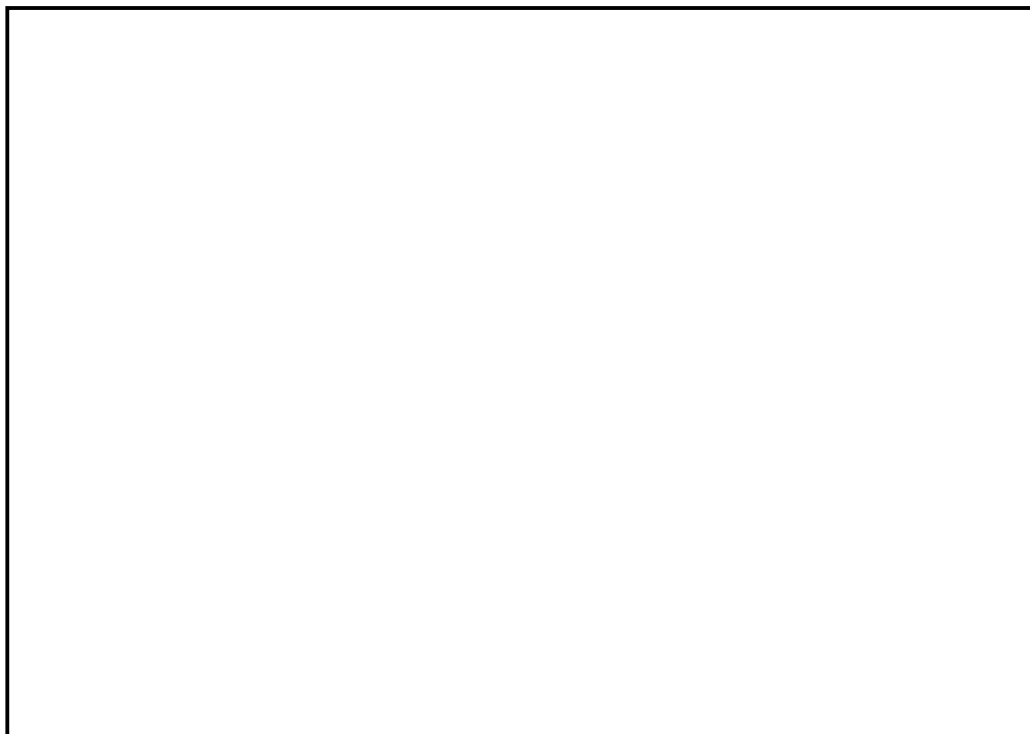
[REDACTED]

[REDACTED] The principal sponsor of BPMS is the Human Resources Division (HRD). Secondary sponsors include the Finance Division (FD), Director's Office (DO), and Security Division (SD).

BPMS is made up of many applications that support the management of personnel resources, applicant, security matters and the payroll system of the FBI. The scope of the System Security Plan (SSP) covers the following BPMS components and the accreditation boundary consists of the following applications:

[REDACTED]

b7E



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

NO [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.

Unclassified

___ 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

b7E

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: Multiple forms exist.

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:** Payroll and insurance matters; background investigations and reinvestigations

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 are encrypted during transmission and are available only to certain users.

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:**

Unclassified

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

12/04/2008

Confidentiality: Low Moderate High Undefined

Integrity: Low Moderate High Undefined

Availability: Low Moderate High Undefined

Not applicable – this system is only paper-based.

Unclassified

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? June 1989

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]:

b7E

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

NO YES (A PIA was published in 2006 for the Bureau Personnel Management System Security Clearance Subsystem; however, the PIA does not adequately define the system under current DOJ and FBI standards.)

If yes:

a. Provide date/title of the PIA:

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

NO YES

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Bureau IT Knowledge Repository (BIKR)

BIKR FBI Unique Asset ID: APP-0000240

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [Redacted] Program Office: Capital Planning Unit Division: IT Management Division / ITB Phone: [Redacted] Room Number: Crystal City 4 Floor	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number:
--	--	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: IT Management Division	Signature: [Redacted] Date signed: 4/26/2012 Name: [Redacted] Title: IT Specialist	Signature: [Redacted] Date signed: 4/26/2012 Name: [Redacted] Title: IT Specialist
FBIHQ Division: IT Management Division	Signature: [Redacted] Date signed: 6/16/2012 Name: [Redacted] Title: ASST. SEC. CHIEF	Signature: Date signed: Name: Title:

b6
b7C

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

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

___ 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. ___ X ___ 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).

X 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; the only PII in BIKR are names of system points of contact. BIKR is a repository of information about systems, not a means for retrieving information by name or personal identifier.

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): (N/A)

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] Unit Chief Privacy and Civil Liberties Unit	Signature: [Redacted] Date Signed: 4/27/12
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: [Redacted] Date Signed: 4/30/12

b6
b7c

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Bureau IT Knowledge Repository (BIKR) is the FBI's official on-line tool to manage, share, and report on IT projects, systems, and networks as well as other related IT information. BIKR resides on the [REDACTED]

[REDACTED] which, in turn, resides within the FBI [REDACTED] on the FBI SECRET Enclave.

b7E

Users from across the FBI regularly contribute data to the Capital Planning Unit for addition to BIKR to create for the entire FBINET community a continually-updated, common understanding of how the FBI is investing its IT resources.

BIKR is the authoritative, centralized source of information for all FBI IT projects, systems, networks and investments. For each of these, BIKR stores the information most critical to their effective management – such as capability descriptions, points of contact (POCs) and other stakeholder and compliance information, including Federal Information Security Management Act and privacy documentation. The POC information in BIKR is the only personally identifiable information in the system.

Access to the physical database, as well as the ability to enter data into BIKR, is restricted to members of the Data Entry Team within the Capital Planning Unit in the Information Technology Management Division.

BIKR data is electronically available on an unrestricted basis to all authorized FBINET users at <http://home/teamsites/BIKR>. Once logged into FBINET, no username or password is required to view BIKR data. In the future, the Bureau anticipates placing some additional information on BIKR that will only be accessible by certain members of the Finance and Security divisions.

Importantly, the information stored in BIKR does not “belong” to BIKR; rather, BIKR is a repository for 14 different data stewards¹ to manage the information they require to complete their individual missions. In addition to storing information, something the data stewards could do themselves, the unique service BIKR provides is in maintaining the crosswalks between the various data stewards' perspectives. For example, BIKR maintains the relationship between a system's name (the way the business owner knows a capability), that same system's C&A boundary (the way SecD knows the capability), the

¹ The data stewards are assigned by membership in the BIKR Advisory Group (BAG), which consists of representatives from the Customer Liaison Office, Finance Division, Office of General Counsel, Records Management Division, Security Division, Office of the Chief Knowledge Officer, Information Technology Engineering Division, and Information Technology Management Division.

UNCLASSIFIED/FOUO

system's PTA name (the way OGC initially evaluates privacy aspects), and the system's Investment name (the way the capability is reported out to OMB and Congress). With BIKR, users can view the information in the way that makes most sense to them, while remaining confident that their view of the data is reconciled with the views shown to other stakeholders.

BIKR not only stores information for open use, it also maintains relationships with outside data sets to enable deeper analysis and improve operations. For example, for commercial off-the-shelf systems or projects, users can determine whether the specific technologies a project or system employs (as stored in BIKR) are still supported by the original product manufacturer (as indicated by the Information and Technology Branch's Standard Product List), or users can use BIKR to determine whether the technologies they want to procure next are available via one of the FBI's enterprise-wide contract vehicles.

BIKR also contains links to the reference guides, handbooks, and templates most often used by Project, System, and Network Managers.

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

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

YES [If yes, please continue.]

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

The information directly identifies specific individuals.

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

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

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

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

UNCLASSIFIED/FOUO

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?

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

While it is possible that a user, knowing a POC, could retrieve information by the POC's name, the purpose of BIKR is to provide information about FBI systems, projects, networks and investments.

_____ 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.] While POCs may complete BIKR information, they are not the subject of the information.

_____ 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)?

 X 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:

UNCLASSIFIED/FOUO

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:

BIKR operates on the

received its latest C&A 3/14/2011.

b7E

UNCLASSIFIED/FOUO

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? 2005

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

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

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

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

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

A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed.

UNCLASSIFIED/FOUO

(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.]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Bureau Mailing List (BML)

BIKR FBI Unique Asset ID: _____

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [Redacted] Program Office: HRASU Division: ITSD Phone: [Redacted] Room Number: 1907	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number: 7350
--	--	---

b6
b7C

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

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Facilities & Logistics Services Division	Signature: [Redacted] Date signed: // 6/27/2011 Name: [Redacted] Title: Unit Chief	Signature: [Handwritten Signature] Date signed: 6/27/11 Name: Elton Wayne Thomas Title: SUPVY SECUR SPEC-CSO
FBIHQ Division: Facilities & Logistics Services Division	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

PIA is required by the E-Government Act.

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

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

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

System does not collect, maintain, or disseminate PII.

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

Information in the system relates to internal government operations.

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

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

Other (describe):

Although no PIA has been done in this, the system operates on Intranet and has not changed since inception. It is approved. Transparency provided by FBI-613

Applicable SORN(s): _____ *FBI-613*


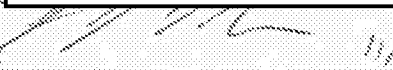
Notify FBI RMD/RIDS per MIOG 190.2.3? No Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCiviP%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

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 Privacy and Civil Liberties Unit	Signature:  Date Signed: 11/15/11
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature:  Date Signed: 11/15/11

b6
b7C

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. BML (Bureau Mailing List) – The BML is a system that supports the efforts of the Logistics Unit (LU) which, among other activities, is responsible for mail services. BML provides customers with the capability to enter, query, and report address information about FBI and non-FBI individuals and groups who are eligible to receive publications and wanted bulletins distributed by the FBI.
2. Data is not migrated into another system or used by any other systems. It is used to produce statistical reports and for address labels, which are utilized to mail Bureau publications, such as the Uniform Crime Report, the Law Enforcement Bulletin, and reports from the Bomb Data Center and National Academy. Address information of FBI individuals, non-FBI individuals, and law enforcement agencies scheduled to receive Bureau publications is entered into BML via an online data entry panel. Through various online functions on the BML main menu panel, customers granted access to BML can also query and report address information. The LU has the ability to print mailing addresses using BML; it is the only unit that can use BML for this purpose.
3. The data in BML is text information consisting of name and address. It is kept in a Natural/ADABAS relational database file. Since LU is the sponsor, LU is primarily responsible for the overall entry and maintenance of the data. However, groups supporting the Bomb Data Center, National Academy, and Law Enforcement Bulletin also enter data into the BML. These users have a group code that allows them to enter address data pertaining to their group.

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

YES [If yes, please continue.]

3. 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.

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

____ 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)? 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.

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

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

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

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

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 1986

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.

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

_____ 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.]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: CA Universal Job Management Agent & Workload Control Center System

BIKR FBI Unique Asset ID: SYS-0000215

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: IT Specialist [redacted]	Name: [redacted]
Reason:	Program Office: ITSD/ISS/OSSU	Phone: [redacted]
Declassify On:	Division: ITSD	Room Number: JEH 7350
	Phone: [redacted]	
	Room Number: JEH 1714	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: ITSD	Signature: [redacted] Date signed: 7/11/11 Name: [redacted] Title: Unit Chief, ITSD, Operating System Support Unit	Signature: [redacted] Date signed: 7-11-11 Name: [redacted] Title: IT Specialist, ITMD, Product Assurance Unit

b6
b7C

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

[UNCLASSIFIED]

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS

PIA is required by the E-Government Act.

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

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

<input type="checkbox"/> Unit Chief Privacy and Civil Liberties Unit	Signature:  Date Signed:
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature:  Date Signed: 10/12/11

b6
b7c

[UNCLASSIFIED]

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Computer Associate (CA) Universal Job Management Agent (UJMA) and Workload Control Center (WCC) are mainframe-hosted products designed to automate workloads and IT processes across the enterprise. UJMA and WCC work together as a subsystem to provide a graphical management user interface (GUI) to mainframe schedulers to manage the resources and background processes of the enterprise servers in order to balance workload on each partition in the server. This project is an online, real-time, interactive system that automatically controls, schedules, and initiates work according to time-driven and event-driven activities. The UJMA provides monitoring resources in real time to identify if the appropriate amounts of memory, disk, or CPU resources are available before allowing a job to execute. This will prevent failures and potential cleanup activities later. The WCC is a graphical interface that helps to coordinate, execute, and manage job schedules and triggered events from the mainframe hosted workload automation tool.

This project supports the Data Center Unit (DCU), Infrastructure Support Section. The system has been online since last year. The system will be migrated from production physical servers into the

b7E

The UJMA/WCC system will reside between the FBI's Mainframe and Windows Server 2003/2008 Environment, which is part of the "Secret" Enclave. Secret Enclave is the subject of an existing PTA.

Since the UJMA/WCC system is designed to track mainframe resources and schedule jobs, it does not contain the actual names of individual users or specific personally identifiable information (PII).

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 FLA is required.]

YES [If yes, please continue.]

[UNCLASSIFIED]

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. N/A
(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.]

[UNCLASSIFIED]

[UNCLASSIFIED]

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.

[UNCLASSIFIED]

[UNCLASSIFIED]

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.

[UNCLASSIFIED]

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.]

[UNCLASSIFIED]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

BIKR FBI Unique Asset ID:

[Redacted]

b7E

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC		FBI OGC/PCLU POC
	Name:	[Redacted]	Name: [Redacted]
	Program Office: ITB Division: ITSD Phone:	[Redacted]	Phone: [Redacted] Room Number: 7350
	Room Number: 8979		

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: DI	Signature: [Redacted] Date signed: 12-17-11 Name: [Redacted] Title: Acting Chief, [Redacted]	Signature: [Redacted] Date signed: 12/15/2011 Name: [Redacted] Title: Unit Chief, Supervisory MAPA
FBIHQ Division: ITSD	Signature: [Redacted] Date signed: 12/9/11 Name: [Redacted] Title: IT Specialist	Signature: [Redacted] Date signed: 1-6-12 Name: [Redacted] Title: Chief, Process Policy & Metrics Unit

b6
b7C
b7E