

UNCLASSIFIED/FOUO

FBI PTA:

b3
b7D
b7E

- 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:** January 9, 2006

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

NAME OF SYSTEM: Enterprise Directory Service (EDS)

FBI SYSTEM CONTACT PERSON Name: [Redacted] Program Office: IATI Division: SECD Phone: [Redacted] Room Number: Date PTA submitted for approval:	FBI OGC/PCLU POC Name: [Redacted] [Redacted] Phone: [Redacted] Room Number: JEH-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:	FBIHQ Division: SECD
Program Manager (or other appropriate executive as Division determines)	Signature: Date signed: Name: Title:	Signature: /s/ Date signed: Name: [Redacted] Title: SECD/iAS/IATU Unit Chief
Division Privacy Officer	Signature: Date signed: Name: Title:	Signature: /s/ Date signed: 9/26/07 Name: Jeffrey J. Berkin Title: SECD, 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: 9/29/07 Name: David C. Larson Title: Acting Deputy General Counsel
---	---

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

1 - Signed original to 190-HQ-C1321794

Copies:

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

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Enterprise Directory Service (EDS)

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:

Enterprise Directory Service (EDS) is a directory service that contains identity and access control attributes of FBI employees, contractors, detailees and integrees.

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:

Identity and access control attributes are the attributes needed to allow FBI mission critical applications to successfully authenticate and authorize users. Examples include user's name, X.509 certificate, citizenship, division, security clearance, cost code, squad, RA (Resident Agency) code, program code, functional title, role, group/COI (community of interest), etc. Attributes will be collected from authoritative data sources for users registered in the FBI PKI system.

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

The EDS objective is to support authentication, access control, and also workflow needs of the bureau. It collects specific attributes from the various legacy authoritative data sources and provides a unified view of those attributes to the clients (application systems or users).

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

EDS consists of [redacted]

b7E

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

EDS v1 can only be accessed by [redacted] It gets data attributes from the various data sources [redacted] depending on the source. It provides data attributes to clients [redacted]

b7E

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

EDS clients include: application systems, FBI/Net users, and administrative clients (directory administrator and application specific delegated administrators). EDS directory solution will enforce proper access control via privilege groups and Access Control Policy Point (ACP) which are used by Oracle directory. In addition, it also uses Access Control List (ACL) and Access Control Information (ACI) at the directory object, entry, or attribute level.

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:

Only FBI personnel with access to FBI/Net will have access to EDS v1.

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

EDS is currently going through its C&A process for both the prototype and production systems. We anticipate a full ATO for the production system on the FBI/Net.

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Enterprise Directory Service (EDS)

- 8 Is this system encompassed within an OMB-300? Yes No Don't Know
SECD/IATI Program - OMB 011-10-02-00-02-3231-00-404-140

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 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: Enterprise Directory Service (EDS)

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.)

FBI PRIVACY THRESHOLD ANALYSIS (PTA) (OGC/PCLU (Rev. 07/06/07))
NAME OF SYSTEM: Uniform Crime Reporting Program

FBI Privacy Threshold Analysis (PTA) Cover Sheet (OGC/PCLU (Rev. 07/06/07))

NAME OF SYSTEM: Uniform Crime Reporting (UCR) Program

FBI SYSTEM CONTACT PERSON Name: [Redacted] Program Office: Crime Statistics Management Unit (CSMU), Program Development Group Division: Criminal Justice Information Services (CJIS) Phone: [Redacted] Room Number: Module E-3 Date PTA submitted for approval: May 15, 2008	FBI OGC/PCLU POC Name: AGC [Redacted] Phone: [Redacted] Room Number: JEH 7338
--	---

b6
b7C

FBI DIVISION APPROVALS.

	Program Division:	FBIHQ Division: CJIS
Program Manager (or other appropriate executive as Division determines)	Signature: [Redacted] Date signed: [Redacted] Name: [Redacted] Title:	Signature: [Redacted] Date signed: 8/20/08 Name: [Redacted] Title: Unit Chief, CSMU
Division Privacy Officer	Signature: [Redacted] Date signed: [Redacted] Name: [Redacted] Title:	Signature: [Redacted] Date signed: 8-26-08 Name: [Redacted] 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: [Handwritten Signature] Date Signed: 8/22/08 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

2 - FBI OCIO / OIPP

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

2*- FBIHQ Division POC /Privacy Officer

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

1 - OGC/PCLU intranet website

1 - PCLU Unit Chief

1 - PCLU Library

1 - PCLU Tickler

NAME OF SYSTEM: Uniform Crime Reporting Program

A. General System Description: Please briefly describe:

The Uniform Crime Reporting (UCR) Program is a collective effort on the part of more than 17,000 federal, state, local, and tribal law enforcement agencies to present a nationwide statistical view of the volume and scope of crime and to enable analysis of crime trends. The UCR Program is managed by the FBI's Criminal Justice Information Services Division (CJIS), Crime Statistics Management Unit (CSMU).

In addition to general crime-related information, the UCR Program collects information about law enforcement officers killed and assaulted, hate crime, and police employee personnel. Most of this information is purely statistical and does not contain personally identifying information (PII) identifiable to individuals. However, once an initial report of a law enforcement officer killed by any means or assaulted and injured with a gun or knife is received, a more detailed form requesting uniquely identifiable data is provided to the victim officer's employing agency for completion. This personally identifiable data, which is maintained by the UCR Program offline in a Microsoft Access data base, is addressed in a separate PTA for the Law Enforcement Officers Killed and Assaulted (LEOKA) system.

1. Type of information in the system:

The UCR Program contains non-PII statistical data on specific criminal offenses such as murder, manslaughter, rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson. The system also contains clearance data for these offenses as well as statistics on persons arrested and police employees.

- 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 statistical information acquired through the UCR Program is used by the FBI to produce statistical reports that are disseminated to the public. These reports are:

Preliminary Semiannual Report
Preliminary Annual Report
Crime in the United States
Hate Crime Statistics
LEOKA
Preliminary LEOKA

These publications provide law enforcement with statistical data for use in operational and tactical studies and as an aid to allocate police resources. In addition, officer safety training may be reviewed in light of information contained in UCR data. This statistical information may also be accessed through the fbi.gov website.

The FBI also utilizes UCR statistics to prepare special studies and respond to questions from the public, government officials, and researchers. Data utilized for this purpose is retrieved via ad-hoc requests for information from the mainframe system and does not contain PII.

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

The current UCR Program is an application that shares resources hosted on an administrative mainframe computer operated by the FBI's Information Technology Operations Division located at FBI Headquarters in Washington, D.C. The current UCR Program collects crime information and stores it in flat-file architecture on a mainframe system within three separate databases -- Summary, National Incident-Based Reporting System, and Hate Crime. Efforts are underway through the UCR Redevelopment Project to replace the current UCR Program with a more efficient application that will facilitate statistical research of the UCR database. However, the information collected and disseminated by the UCR Program will remain the same.

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

Direct access to the UCR Program is limited to approximately [redacted] at the CJIS facility in West Virginia that are used for data entry and review. In order to accommodate the submission capabilities of various federal, state, local, and tribal contributors, the FBI receives statistical data in a variety of formats, including paper submissions, cartridges, and internet e-mail submissions via Law Enforcement Online (LEO). CJIS personnel copy the data into electronic files, check it for errors, and facilitate corrections as needed.

b7E

No information is transmitted directly from the UCR Program; however, data from the Program is extracted by CJIS personnel in order to perform data quality checks, retrieve raw data for preparation of reports, perform special statistical studies, and respond to questions from government officials and the public.

As noted *supra*, under the proposal for the redevelopment of the UCR System, a repository of non-personally identifiable data will be made available to law enforcement and the general public for direct query through the Internet.

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 the data contained within the UCR application is presently limited to personnel assigned to the CJIS Division's CSMU, Crime Analysis Research and Development Unit, and Training and Systems Education Unit, as well as designated staff within the Criminal Investigative Division and Training Division, all who require access to the data in order to perform their work in analyzing data and preparing reports. A limited number of personnel assigned to the CJIS Division's Information Technology Management Section (ITMS) and the Information Technology Operations Division also have access to the system to process data or perform system security functions.

NAME OF SYSTEM: Uniform Crime Reporting Program

The UCR application is accessed from an administrative mainframe computer; access to the administrative mainframe requires a valid user name and strong password (which must be changed on a regular basis). An access log is maintained for the administrative mainframe and is subject to audit.

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?

Currently, no one outside the FBI has direct access to the information within the UCR application.

Under the proposal for the redevelopment of the UCR system, a secondary, secured repository of non-personally identifiable data will be made available to law enforcement and the general public for direct query through the internet. As the system is being designed, ITMS and the Information System Security Officer will ensure through current security standards that only authorized persons will be able to access the master data base.

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

The UCR Program is a low risk application residing on the FBI's administrative mainframe computer and therefore does not require separate certification and accreditation.

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

The existing UCR system is not encompassed within an OMB-300. An OMB-300 for the UCR redevelopment project is under development, but has not yet been submitted to OMB.

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.)

I. 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.)

The UCR Program has not undergone any significant changes since April 17, 2003; however, the CJIS Division is seeking authorization for a redevelopment project to include an initiative that will improve the public availability of statistical data in the UCR system via the internet.

NAME OF SYSTEM: Uniform Crime Reporting Program

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

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

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

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

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

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

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

(FBI and DOJ reviewing officials reserve the right to require a PIA.)

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

II. For systems developed after April 17, 2003.

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

(Continue to Question 2.)

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

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

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

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

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

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.)

NAME OF SYSTEM: [insert name]

III. Full or Short-Form PIA

1. Is the system a major information system (as listed on OGC's FBINET website)?

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

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

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

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

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

FBI Privacy Threshold Analysis (PTA) Cover Sheet (Rev. 10/31/06)

NAME OF SYSTEM: Voice Recognition Software

FBI SYSTEM CONTACT PERSON

Name: [Redacted]
Program Office: none
Division: note: project for Associate Deputy Director Joseph Ford
Phone: [Redacted]
Room Number: 6026
Date PTA submitted for approval: 01/12/07

b6
b7C

FBI DIVISION APPROVALS:

Program Manager (or other appropriate executive as Division determines)	Signature: TWS [digital] Date signed: 01/12/07 [digital] Name: [Redacted] Title: Special Advisor to the Chief Financial Officer
Division Privacy Officer	Signature: Date signed: Name: Title:

b6
b7C

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

FINAL FBI APPROVAL:

FBI Privacy and Civil Liberties Officer	Signature: /s/ Date Signed: 5/10/07 Name: David C. Larson for Patrick W. Kelley Title: Deputy General Counsel
---	--

Upon final FBI approval, distribute as follows:

Original signed copy to 66F-HQ-C1321794

Copies:

- 1 - DOJ Privacy and Civil Liberties Office (Main Justice, Room 4259)
- 1 - FBI OCIO
- 1 - FBI SecD
- 2 - Division POC /Privacy Officer
(please reproduce as needed for Program/Division file(s))
- 1 - OGC\PCLU Intranet website
- 1 - PCLU Library

1 - PCLU Ticker

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: Voice Recognition Software

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:

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 Administrative Law Unit 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 Administrative Law Unit 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," please provide a brief explanation of a) the purpose of the system, and b) quantity and type of employee/contractor information:

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 Administrative Law Unit for review, approval, and forwarding to DOJ's Privacy and Civil Liberties Office.

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: Voice Recognition Software

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 and proceed to Question 2.)

Voice Recognition Software (VRS) has three primary areas of functionality. Dictation, whereby spoken language is transcribed to written text; commands that control, whereby spoken language is recognized as command to perform an action; and finally text-to-speech whereby written text is converted to synthesized audio stream.

The FBI project team assumes that the main usage at the Bureau will be the transcription of spoken language to written text.

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 Administrative Law Unit 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," please provide a brief explanation of a) the purpose of the system, and b) quantity and type of employee/contractor information:

a) the purpose of the system is to facilitate the transcription of documents that need to be created with or without voice recognition software (VRS). For example, without VRS agents need to complete 302's by typing from their rough case notes; with VRS agents could complete 302's by dictating their case notes into the software and then modifying the document as needed to ensure accurate capture of the information. In either case, the final product should be the same.

b) Information captured by VRS will include the same case and other administrative information already captured by 302's and other standard FBI documents.

The quantity and type of employee/contractor information should be the same with or without VRS.

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 Administrative Law Unit for review, approval, and forwarding to DOJ's Privacy and Civil Liberties Office. Unless you

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: Voice Recognition Software

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.)

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

NAME OF SYSTEM / PROJECT: Public Key Infrastructure (PKI)

BIKR FBI Unique Asset ID: SYS-0000066

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [Redacted] Program Office: ESS/DSSU Division: ITSD Phone: [Redacted] Room Number: 1388	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: ESS/DSSU	Signature: [Redacted] Date signed: 7/23/2010 Name: [Redacted] Title: Unit Chief	Signature: [Redacted] Date signed: 8-2-10 Name: [Redacted] Title: Privacy Officer
FBIHQ Division: ITSD	Signature: <i>Christina Kears, Acting</i> Date signed: 7/27/2010 Name: Gail Scavongelli / CSM Title: Section Chief	Signature: [Redacted] Date signed: [Redacted] Name: Title:

b6
b7C

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

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

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

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

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

b6
b7C

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 FBL.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): _____

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):

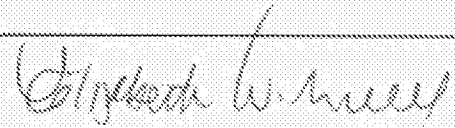
Prepare/revise/add Privacy Act (e)(3) statements for related forms? No Yes (indicate forms affected):

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 and FBI Privacy and Civil Liberties
Officer

Signature:
Date Signed: 8/23/2010



[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. The FBI PKI is an integrated suite of products, which meet and exceed the FBI's base requirements, to provide enhanced certificate management features for improved security services. Key elements of the designed solution are: integrated suites of COTS products that provide enhanced usability and key management; client software that fully meets the FBI's requirements for transaction validation; and scalable architecture that will grow to support the FBI's anticipated enterprise user community. Initially, the system facilitates secure electronic email, using digital signature and encryption, between two FBI locations. The system is scaled to support full deployment of PKI services of strong authentication, digital signatures, encryption/decryption services, and non-repudiation throughout FBI.

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

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

___X___ YES [If yes, please continue.]

3. 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 3.

_____ 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

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

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 But only as an Administration function for proper vetting

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: **The FBI Rules of Behavior form provides a Privacy Act notice for PKI registrants.**

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.

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

_____ 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:

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

Provide date of last C&A certification/re-certification:
12/10/07 Re-certification expect 12/14/2010

Confidentiality: ___ Low ___ Moderate **_X_** High ___ Undefined

Integrity: ___ Low ___ Moderate **_X_** High ___ Undefined

Availability: ___ Low ___ Moderate **_X_** High ___ Undefined

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

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

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: Exhibit 53 PKI Revitalization
5/2010

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?

NO

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

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

NO _____ YES

13. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 2003/2004

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

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

YES If yes, indicate which of the following changes were involved (mark all
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.

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS,
IF APPROPRIATE]

(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.

___X___ Other [Provide brief explanation]: Migrated to new hardware/operating System

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

_____ NO ___X___ YES

If yes:

a. Provide date/title of the PIA: 9/19/2006 PIA for the FBI Public Key Infrastructure

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

___X___ NO _____ YES other than described above.

[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: Reimbursable Agreement Management System (RAMS)

BIKR FBI Unique Asset ID: 2011-002-01-P-307-116-9999

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: [Redacted] Program Office: Accounts Receivable Unit Division: Finance Division Phone: [Redacted] Room Number: 6132	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: Finance Division	Signature: [Redacted] Date signed: 7/3/11 Name: [Redacted] Title: Unit Chief	Signature: [Redacted] Date signed: 8/10/11 Name: Luke Preus Title: Privacy SPO
FBIHQ Division: Finance Division	Signature: [Redacted] Date signed: 8/17/11 Name: MICHAEL MURPHY Title: DEPUTY SECTION CHIEF, PRIVACY	Signature: [Redacted] Date signed: 8-10-11 Name: [Redacted] Title: Unit 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:

____ 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 :

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.

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

____ Other :

Applicable SORN(s): Accounting Systems for the Department of Justice, DOJ-001; Central Records System, DOJ/FBI-002

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? ____ No ____ Yes

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

Other:

[Redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [Redacted] Date Signed: 3/15/10
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: [Redacted] Date Signed: 3/15/10

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 Accounts Receivable Unit (ARU) uses the Reimbursable Agreement Management System (RAMS) to manage the FBI's [redacted] annual reimbursable funding through billing, collecting, and reporting on Reimbursable Agreements. RAMS at FBI Headquarters is currently hosted through MS Access but will soon change to an Oracle-based system.

b7E

As the business requirements have evolved over time for the unit, RAMS has expanded in size, capacity, and function [redacted]. [redacted] Because of the ARU's critical financial management function for the FBI, RAMS is currently being transitioned to Oracle, which is supported by the FBI's technical support personnel [redacted]. Once RAMS moves to Oracle, it will be [redacted].

b7E

RAMS database batch uploads transactional data to the Financial Management System (FMS) and ARU reconciles the data [redacted] to ensure its accuracy. RAMS [redacted]

b7E

[redacted] will maintain their same functionality and remain [redacted] even after the ARU RAMS transitions to Oracle.

The information contained in RAMS is related to Reimbursable Agreements (RA) and the status of the billing or collections against those Agreements. The information will continue to be uploaded to FMS, which will remain as the official record. RAMS also contains Point of Contact (POC) information for each RA, which includes the contact's name, telephone number, and address of the RA customer as well as the FBI POC's name and telephone number. The customers include other federal government agencies, state/local government agencies, as well as a few private companies. The proposed solution will mirror the current capabilities in RAMS while providing a more sustainable and robust database.

The users will be personnel (both government employees and contractors) in ARU, Finance Division (FD), and Financial Applications Support Unit (FASU) who require access as part of their job function.

UNCLASSIFIED

The proposed application will be a web-based application only available to approved users on the FBI's secure classified Secret enclave.

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

NO

YES [If yes, please continue.]

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

The information directly identifies specific individuals.

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

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

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.]

UNCLASSIFIED

UNCLASSIFIED

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:

UNCLASSIFIED

UNCLASSIFIED

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:

A C&A will be completed as required, but has not yet been started due to not having a complete database to be tested at this time. The anticipated completion date is approximately September, 2011.

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

UNCLASSIFIED

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).]

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

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

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

X 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.)

RAMS is in transition from an Access database to an Oracle database. The Oracle environment, [redacted]

[redacted]

RAMS.

..... 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.

b7E

UNCLASSIFIED

_____ 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

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

NAME OF SYSTEM / PROJECT: Records Information System (RCI)

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [redacted] (Project Mgr)	Name: [redacted]
	[redacted] (System Admin)	Phone: [redacted]
	Program Office: [redacted] (Records Conversion Unit (RCU)) [redacted] (Business Operations Support Unit (BOSU))	Room Number: JEH 7350
	Division: Records Management Div (RMD)	
	Phone: [redacted]	
	Room Number: [redacted] ARC3, Bldg 917 [redacted] PA1001, Ste. 520	

b6
b7C

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

	Program Manager: [redacted]	Division Privacy Officer: David Hardy
Program Division: RMD/RCU	Signature: [redacted] Date signed: [redacted] 8/3/2010 Name: [redacted] Title: Project Manager	Signature: [Handwritten Signature] Date signed: 8/12/2010 Name: David Hardy Title: Division Privacy Officer
FBIHQ Division: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

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

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

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

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

b6
b7C

Unclassified

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

_____ PIA is required by the E-Government Act.

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

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

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

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

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

Information in the system relates to internal government operations.

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

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

_____ Other (describe):

Applicable SORN(s): DOJ-002, Department of Justice Computer Systems Activity and Access Records, 64 Fed. Reg. 73,585 (Dec. 30, 1999), 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):

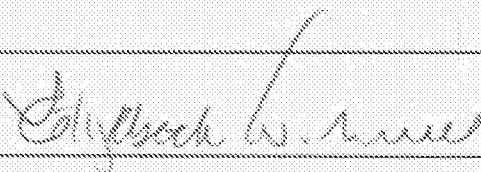
Prepare/revise/add Privacy Act (e)(3) statements for related forms? No _____ Yes (indicate forms affected):

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

Other:

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

Signature:
Date Signed:

 8/9/10

Unclassified

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.):

Before the development of TRIM Context, which is an inventory system used to manage records, the Records Management Division (RMD) records storage mission was handled primarily using manual processes. RMD processes did not provide an auditable chain of custody for records, nor did they provide the FBI with the ability to assert with certainty that all records relating to a subject have been located. In addition, the existing processes did not provide RMD a reliable method of tracking disposition dates for transferring of records to the National Archive and Records Administration or disposing of them. As a result, RMD was maintaining many records well beyond their disposition dates. Without a tracking system, the risk of loss of records, access to records, and the security of the records was increased. Thus, RMD developed RCI, which hosts the TRIM Context application, to solve this problem.

TRIM Context allows the Records Management Control Unit (RMCU) to have control of FBI records; complete the inventory of the records; maintain chain of custody; and properly dispose either by transferring ownership to National Archives and Records Administration (NARA) or by destruction. TRIM Context provides one location to account for all records in RMD's custody. The system maintains information up to and including the SECRET classification.

TRIM Context works in the following manner:

FBI records are assigned record numbers. In order to locate a record, a user logs into TRIM Context and types in the record number. TRIM Context then displays for the user where the record is currently located along with a history of the record's previous locations. The location data gives geographic information, such as building address and room number. The location data does not indicate which individuals, if any, may currently have the record. For example, TRIM Context may indicate that record 123 is at FBI Headquarters in the Office of General Counsel, but *will not* indicate that the record is with FBI specialist [REDACTED]

b6
b7c

TRIM Context does not search by record name or record content; thus, the system does not contain sensitive PII, which might otherwise be found in the actual records. This system merely tracks the record's location by identification number. If a user does not know the record number, the user may retrieve the number through searches in other systems. For example, to locate the record on [REDACTED] an individual could search for [REDACTED] in another database and learn that the record number associated with [REDACTED]

is 123. Then, the user will manually input the record number into TRIM Context and learn where the record is located.

Access to the system is limited to designated users, all of which are FBI employees or contractors. The system contains a list of users and the user's authorized roles. Further, the system contains audit logs that can be searched by the name of the user.

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

NO [If no, STOP. The 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.]

If an individual does not know the record number of the record that the individual desires to locate, the individual may look up the record number in another system by the name of the record, which could contain PII depending on the type of record, and then learn the record number. The record number is then manually entered into TRIM Context. Thus, the record number is potentially linkable to an individual.

The record number has a low risk of privacy as the only function one can perform in TRIM Context with the record number is to learn the location of the record. Further, the act of learning the location of the record serves an internal government function. Thus, since the risk of privacy is relatively low, and under M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, a Privacy Impact Assessment is not required for systems that are for internal government operations, a Privacy Impact Assessment is not required for this system. Moreover, a search by the record number does not retrieve information about an individual, but instead retrieves information about the physical location of the record. Therefore, a Privacy Act system of records does not exist for this portion of the system.

Although the system contains an audit log with the names of individual FBI users, which can be linked to an audit trail associated with an individual's activities on the system, such records are covered under DOJ-002. Further, under M-03-22, this portion of the system does not trigger a Privacy Impact Assessment, as this portion only contains non-sensitive information about FBI users and is used to carry out an internal government function.

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

NO YES

The audit logs contain information only on government employees and contractors. However, the record numbers are linkable to records maintained in other systems that are largely about non-government employees and contractors.

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

Audit log information, which is about FBI users, is retrieved by a personal identifier.

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

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

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

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

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

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

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

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

NO [If no, proceed to question 7.]

_____ YES

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

YES [If yes, proceed to question 7.]

NO

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

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

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

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

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

YES If yes, provide date of last C&A certification/re-certification:
January 29, 2006

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? The RCI system was developed in early part of 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 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]:

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.]

FBI Privacy Threshold Analysis (PTA) Cover Sheet (OGC/PCLU (Rev. 07/06/07))

NAME OF SYSTEM: Security Access Control System (SACS)

FBI SYSTEM CONTACT PERSON Name: [Redacted] Program Office: Security Operations Section Division: Access Control Unit Phone: [Redacted] Room Number: 1358 Date PTA submitted for approval: March 26, 2008	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number: JEH 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	FBIHQ Division: Security Operations Section
Program Manager (or other appropriate executive as Division determines)	Signature: Date signed: Name: Title:	Signature: /s/ Date signed: 04/17/08 Name: [Redacted] Title: Unit Chief
Division Privacy Officer	Signature: Date signed: Name: Title:	Signature: /s/ Date signed: 4/18/08 Name: Michael A. Morehart Title: DAD

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: 6/26/08 Name: David C. Larson Title: Acting Deputy General Counsel
---	---

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

1 - Signed original to 190-HQ-C1321794

Copies:

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

2 - FBI OCIO / OIPP

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

2* - Program Division POC /Privacy Officer

2*- FBIHQ Division POC /Privacy Officer

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

1 - OGC/PCLU intranet website

1 - PCLU Library

1 - PCLU Tickler

NAME OF SYSTEM: Security Access Control System (SACS)

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:

SACS contains a [redacted] of personal information containing Name, [redacted] [redacted] Also, data on security clearance issues are included.

b7E

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

SACS currently houses [redacted] and validates the following data: Name, [redacted] [redacted] Also, data on security clearance issues are included.

b7E

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

The purpose of SACS is to provide controlled access into the FBIHQ. The system issues and tracks identification badges for the FBI and monitors alarm systems. It performs database functions (granting/denying) on an isolated network which is used to assist in regulating physical access for the J. Edgar Hoover (JEH) F.B.I. building. The SACS identification access cards are programmed to grant/deny the holder access to the facility, or select rooms based upon access level granted by FBI security.

SACS is used to create and activate both permanent and temporary identification badges. SACS is programmed with information indicating which badge is authorized for access to specific areas and the timeframes for which that access is valid. To gain facility and office access, the Security Division must approve the request based upon background investigation and need to know. After being approved, all FBIHQ employees, contractors, visitors, and others requiring access to the facility are issued an identification badge. The type of photo badges issued may be permanent, temporary, or visitor, and each type utilizes a different color scheme. Everyone who is issued a badge falls under one of the three types. Each badge is a proximity access card. An activated proximity access card is required to activate card readers that control the facility perimeter turnstiles, access to offices, rooms, or Sensitive Compartmented Information Facilities (SCIFs). When a badge is placed next to (close proximity) a specific card reader, SACS determines if the badge is valid for access through that access point at that time. Based on that validation, the SACS either activates or does not activate the controlling mechanism (e.g., turnstile, door lock). Some card readers require the badge holder to enter a 5-digit personal identification number (PIN) in addition to swiping/reading of the badge, in which case both the badge and the PIN (dual factor

NAME OF SYSTEM: Security Access Control System (SACS)

authentication) must be a valid matching set and associated with that card reader at that time, in order to permit entry. The SACS logs all attempted accesses whether valid or invalid.

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

b7E

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

Log in directly into the SACS 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 SACS will be controlled by unique user accounts and system roles. Only users assigned to the FBI's Access Control Unit, SACS 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

--

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. SACS uses access control measures for providing authorized users access to SACS.

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

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

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

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

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

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

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

(Continue to Question 2.)

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

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA) (OGC/PCLU (Rev. 07/06/07))

NAME OF SYSTEM: Security Access Control System (SACS)

Unit (PCLU) for review, approval, and forwarding to DOJ's Privacy and Civil Liberties Office. Unless you are otherwise advised, no PIA is required.)

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

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

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

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

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

II. For systems developed after April 17, 2003.

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA) (OGC/PCLU (Rev. 07/06/07))

NAME OF SYSTEM: [insert name]

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.)

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Form Rev. 9/9/08

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

NAME OF SYSTEM / PROJECT: Vehicle Management Application (VMA)

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLE POC
Classified By:	Name: IT Specialist [redacted]	Name: AGC [redacted]
Reason:	Program Office: Financial Applications	Phone: [redacted]
Declassify On:	Support Unit	Room Number: 7350 JEH
	Division: ITSD	
	Phone: [redacted]	
	Room Number: 1302 JEH	

b6
b7C

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

A. Provide date checklist prepared: February 17, 2011

B. Provide a general description of the system or project that includes: name of the system/project, including associated acronyms; structure of the system/project, purpose; nature of the information in the system and how it will be used; who will have access to the information in the system and the manner of transmission to all users.

The Vehicle Management Application (VMA) is a legacy application residing on the FBI's Administrative Mainframe. [redacted]

[redacted] VMA records and tracks data relative to FBI automobiles and associated maintenance and depreciation costs. The VMA stores information on the entire FBI vehicle fleet [redacted]

b7E

[redacted] The VMA tracks automobile costs (direct and indirect), mileage readings, motor maintenance and bureau accident information. Each Field Division and LEGAT is responsible for entering all costs associated with operating each bureau vehicle into VMA.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

VMA interfaces with the Bureau Personnel Management System (BPMS) to obtain and verify information about Bureau personnel and with the Property Management Application (PMA) to obtain and verify information about Bureau vehicles. Information in VMA about individuals involved in traffic accidents with Bureau vehicles is derived from the Central Records System.

VMA is sponsored by the Fleet Management and Transportation Unit (FMTSU) at FBIHQ and is supported by Information Technology (IT) specialists in FASU. Access to VMA must be authorized through the Security Access Request (SAR) system before an individual may access the system. Upon approval, a VMA account is established for the individual and is then included in the user's Mainframe Applications menu.

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

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

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- * 9. The system was developed after April 17, 2003.²
- * VMA is a legacy application deployed in 1985, prior to the effective date of FISMA, and no significant changes affecting privacy have been made to VMA since that time. While a PIA is unnecessary for such a legacy application, the FBI has elected, as a matter of discretion, to prepare this PIA since VMA constitutes an FBI Routine Database.
- X 10. If the system maintains information about U.S. citizens or legal permanent residents, it is covered by a published Privacy Act System of Records Notice.
- X 11. Records retention issues have been discussed with the Records Management Division.
- X 12. Any personally identifiable information placed on a mobile device or on media that is transported outside FBI facilities must comply with the FBI policy on encryption and must be password protected.

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

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

APPROVING OFFICIALS

Program Manager (or other appropriate official as division determines)	Division Privacy Officer
Signature: [Redacted]	Signature: [Redacted]
Date signed: 2/22/2011	Date signed: 2-25-11
Name: [Redacted]	Name: [Redacted]
Title: Unit Chief, Financial Applications Support Unit, ITSD	Title: IT Specialist, ITSD

b6
b7C

DISTRIBUTION:

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

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Sensitive Compartmented Information Operational Network (SCION)

BIKR FBI Unique Asset ID: NEN-0000039

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [REDACTED]	Name: [REDACTED]
Reason:	Program Office: SCION	Privacy Civil Liberties Unit
Declassify On:	Division: Information Technology Services Division	Phone: [REDACTED]
	Phone: [REDACTED]	Room Number: JEH, 7350
	Room Number: JEH, 9988	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Information Technology Services Division	Signature: [REDACTED] Date signed: 1/9/13 Name: [REDACTED] Title: Enclave Program Manager	Signature: [REDACTED] Date signed: Name: Title:
FBIHQ Division: Customer Support Section (CSS)	Signature: [REDACTED] Date signed: 1-7-2013 Name: Naomi Singer Title: Section Chief, Customer Support Section, ITSD	Signature: [REDACTED] Date signed: 1/10/13 Name: [REDACTED] Title: IT Branch 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:

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: System is infrastructure and is being phased out.

Applicable SORN(s): DOJ-002 (DOJ Computer Systems Activity and Access Records)

Notify FBI RMD/RIDS per MIOG 190.2.3? No Yes--See sample EC on PCLU intranet website here:
http://home/DO/OGC/LTB/PCLU/Privacy/Civil%20Liberties%20Library/form_for_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:

System is being phased out and will be replaced by Next Generation SCION, which is due to be completed in 2012. No PIA is required because the system is infrastructure. The system of records notice for DOJ-002 would cover the PII of the FBI personnel who use the system (that is, their user names and encrypted passwords).

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

Signature:
 Date Signed: 1/11/2013
 Signature: *[Handwritten Signature]*
 Date Signed: 1-11-2013

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 Sensitive Compartmented Information Operational Network (SCION) provides the infrastructure allowing the FBI to interface with the national Intelligence Community (IC) through the Joint Worldwide Intelligence Communications Systems (JWICS). JWICS provides access to the IC, the Secure Automated Message Network, NCTC Online and other Communities of Interest (COI's). SCION utilizes the Trilogy Program-based network architecture to include the Trilogy approved lists of computers, hardware, and software.

SCION capabilities include:

- Enhanced access to IC databases & websites outside of FBI and FBI-wide share drives;
- Email capabilities with various levels of access, both internally and externally; and
- Advanced features to classify work.

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

_____ NO

YES [If yes, please continue.] However, the only personal information maintained are encrypted passwords as well as usernames contained within the audit logs (which are not accessible to general users).

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.