FBI PTA: [redacted] b7E

_____ NO. ___X__ YES. Password and audit information may be retrieved by user name.

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

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

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

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

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

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

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

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

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

_____ YES.

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

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

_____ NO.

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

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

_____ YES. **Identify any forms, paper or electronic, used to request such**

FBI PTA: [redacted] b7E

information from the information subject:

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

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

__X___ YES. **If yes, provide date of last C&A certification/re-certification:** 02/14/2008

_____ Don't Know.

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

_____ NO. ___X__ 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. __X___ 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? 2002

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

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

3. Does a PIA for this system/project already exist? __X___ NO.
(But as noted above, an EOUSA PIA does exist for the main VNS system.)

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: Quickwins [redacted] b7E

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: IATU Division: SecD Phone: [redacted] Room Number: SpyB 5th Floor	**FBI OGC/PCLU POC** Name: [redacted] Phone: [redacted] Room Number: JEH 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Security Division	Signature: /s/ Date signed: 03/29/10 Name: [redacted] Title: Unit Chief, Information Assurance Technology Unit	Signature: /s/ Date signed: 03/29/10 Name: Michael J. Folmar Title: AD, Security Division
FBIHQ Division: Security Division	Signature: /s/ Date signed: 03/29/10 Name: [redacted] Title: Unit Chief, Information Assurance Technology Unit	Signature: /s/ Date signed: 03/29/10 Name: Michael J. Folmar Title: AD, Security Division

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)
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
1 - OGC\PCLU intranet
1 - PCLU UC
1 - PCLU Library
1 - PCLU Tickler

b6
b7C

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

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

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

__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). – The only PII are usernames/passwords and only the system administrator has access.
- ___ Other (describe):

Applicable SORN(s): 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 (indicate revisions needed):

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

No Privacy Act (e)(3) statement is necessary since the username/password do not say anything *about* the individual, particularly as an individual may choose anything as their username or have one assigned to them.

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:

David C. Larson, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 5/12/06

FBI PTA: Quickwins [redacted] b7E

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

Quickwins [redacted] is the proposed process to update the One Way Transfer (OWT) capabilities of Quickwins-OWT (see Quickwins OWT PTA dated 07/11/2008). This system automates the transfer of extensive and detailed SF-86 background clearance information from the Office of Personnel Management (OPM) to the FBI's Clearance Processing System (CPS). While OPM stores this information on an unclassified network, the FBI uses this information on a secret network to conduct background investigations. In order to transfer this information from an unclassified network outside the bureau to a classified network within the bureau, a Cross Domain Solution (CDS) is required. b7E

[redacted] that has the required capability to securely transfer information between domains of different classification levels. As with Quickwins-OWT, Quickwins [redacted] will automate the OWT of files [redacted] b7E - no changes will be made in the type of data that is transferred, the way that users receive the information, or who will have access to the information. As such, general users will continue to access the SF-86 information through CPS, not through Quickwins [redacted] The only users of Quickwins [redacted] will be privileged users, i.e. the system administrator and the security administrator. These privileged users will be the only ones with access to Quickwins [redacted]

Quickwins [redacted] The extensive and detailed SF-86 background clearance information [redacted] This information originates from prospective and current FBI employees who submit their SF-86 information to the Office of Personnel Management (OPM) through the Electronic Questionnaires for Investigative Processing (E-QIP) application. After collecting the SF-86 files, OPM sends the files [redacted] The files will first enter the Quickwins [redacted] system when they are transferred [redacted] to the Quickwins [redacted] passing first through the Quickwins-[redacted] Quickwins [redacted] the files will be transferred through the Quickwins [redacted] b7E

and high-side router and onto the Clearance Processing System (CPS) application residing on the FBI Secret Enclave.

The files that are transferred though Quickwins [redacted] will merely pass through the system -- no data will be stored on Quickwins [redacted] itself. [redacted] Quickwins [redacted] b7E

CPS application. No residual elements of the document will remain on [redacted]

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

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

__X__ YES [If yes, please continue.]

The only PII that will be stored on the system consists of the usernames and passwords of the system administrators and the security administrators.

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

_____ NO __X__ YES

The system administrators and security administrators will always be government employees or contractors, so only their PII would be stored. Information on non-government employees may pass through the system but that information is not collected, maintained or disseminated.

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

_____ NO __X__ YES

The system administrator and security administrators will always be U.S. citizens. The system administrator will be able to see the usernames on the [redacted] b7E Access Control List (ACL).

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

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

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

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

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

_____ 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.]

__X__ YES

Any system administrator will have the ability to control the [redacted] ACL and thus the usernames of other administrators. For the new administrators, a system administrator will be able to either make up a username for the new administrator or that individual may directly request a preferred username. b7E

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

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

__X__ 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)?

__X__ NO

No Privacy Act (e)(3) statement is necessary since the username/password do not say anything *about* the individual, particularly as an individual could choose anything as their username.

_____ 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)?

__X__ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date**: C&A is pending with an anticipated completion date of May 24, 2010.

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

_____ Don't Know.

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

__X__ NO _____ Don't know _____ YES **If yes, please provide the date and name or title of the OMB submission:**

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

__X__ NO _____ YES _____ Don't know

10. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

FBI PTA: Quickwins [redacted] b7E

1. When was the system/project developed?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FBI PTA: Quickwins [redacted] b7E

_____ 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

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

Total Deleted Page(s) = 1
Page 4 ~ b3 - National Security Act of 1947; b7E;

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b3 b7E

BIKR FBI Unique Asset ID: Proj2012-019-01

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [redacted] Program Office: CDIG Division: CJIS Phone: [redacted] Room Number: E-3	FBI OGC/PCLU POC Name: [redacted] Phone: [redacted] Room Number: C3

b6 b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [redacted] Date signed: 6/12/2013 Name: W. Jay Abbott Title: Chief - Global Operations Section Intelligence Program Manager	Signature: [redacted] Date signed: 7/12/13 Name: [redacted] Title: Supervisory IT Specialist
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6 b7C

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_____ PIA is required by the E-Government Act.

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

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

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

Applicable SORN(s): __ Data Warehouse SORN _____

Notify FBI RMD/RIDS per MIOG 190.2.3? _X__No ___Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? _X__No ___Yes:

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

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

Other:

[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 7-25-13
Christine M. Costello, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 7-25-13

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

(a) [redacted] b3 b7E

(b) [redacted] operational within an accredited Top Secret//Sensitive Compartmented Information (TS//SCI) Facility (SCIF) at the Criminal Justice Information Services (CJIS) Division. [redacted] Standards and procedures to ensure confidentiality, integrity and availability of the [redacted] data will be in place to support [redacted] b3 b7E

[redacted] This PTA addresses [redacted]

(c) The goal of developing [redacted] is to [redacted] b3 b7E

(d) The CJIS Division will [redacted] b3 b7E

[redacted] b3 b7E

[redacted] b3 b7E

[redacted] b3 b7E

(e) FBI employees from the following units and contractors supporting the various units will have access to the system:

[redacted] b7E

[redacted] will limit system access by utilizing user defined roles and access controls for [redacted] User groups have access only to those files necessary to complete a user's assigned task and nothing more. Users are divided into privileged and general users. User groups are role based in that they are defined by the specific type of duties assigned to the individual. For example, system programmers are in one group, whereas system administrators are a separate group. System administrators are assigned administrative type privileges based on the type of work performed by the user; different accounts are assigned for specific requirements. b3 b7E

[redacted] b3 b7E

All personnel must have active access [redacted] and have a FS clearance with SCI access to the appropriate levels. All personnel are required to have received training regarding the use and handling of classified information. Users are granted accounts by the system administrator with receipt of an approved user application and agreed to [redacted] Rules of Behavior form. b3 b7E

(f) The CJIS Division [redacted] b7E

[redacted] b3 b7E

[redacted] and must be used in accordance with applicable regulations. [redacted]

[redacted] CJIS will ensure that ability is covered by separate privacy documentation.

[redacted] b3 b7E

System administrators will have the ability to search [redacted]

[redacted] This search capability is designed for audit and control purposes as well as [redacted] b3 b7E

[redacted] b3 b7E

[redacted] b7E

b3
b7E

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

_____ NO

__X___ YES

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

__X__ The information directly identifies specific individuals.

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

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

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

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

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

__X__ NO _____ YES

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

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

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

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

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

_____ YES

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

_____ NO

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

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

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

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

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

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

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

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

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

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

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

8. Is the system operated by a contractor?

__X__ No.

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

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

__X__NO **If no, indicate reason; if C&A is pending, provide anticipated completion date**: Authority to Operate is pending anticipated date August 23, 2017

_____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)?

_X___ NO

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

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

_____ NO _X___ YES

12. Status of System/ Project:

_X___ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

_____ NO _____ YES

If yes:

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

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

____NO ____YES

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Secret Enclave/FBINet

BIKR FBI Unique Asset ID: NEN 0000010

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: N/A Division: ITID Phone: [redacted] Room Number: 9959	**FBI OGC/PCLU POC** Name: [redacted] Phone: [redacted] Room Number: 7350 JEH

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as [redacted]	Division Privacy Officer [redacted]
Program Division: **[insert division name]**	Signature: Date signed: 7/30/14 Name: [redacted] Title: Program Manager	Signature: Date signed: 8/14/2014 Name: [redacted] Title: IT ~~Specialist~~ Policy 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 7350).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

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

____ PIA is required by the E-Government Act.

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

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

__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 (describe):

Applicable SORN(s): _JUSTICE/FBI-002, Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998); DOJ-002, Department of Justice Computer Systems Activity and Access Records, 64 Fed. Reg. 73,585 (Dec. 30, 1999).

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 (indicate revisions needed):

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

Ernest J. Babcock, Deputy General Counsel, FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 9/19/14

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.**

FBI Secret Enclave (FBISE) provides infrastructure support to enterprise wide information systems operating up to the SECRET level throughout FBI. Beyond basic login information, FBISE does not process information; instead, it provides the transport mechanism for information that needs to be transferred, shared and distributed across the FBI. While some applications and systems that run on FBISE's transport may contain significant amounts of Personally Identifiable Information (PII) only user audit logs and login information rise to the level of PII, all other is accessed through the use of the above mentioned systems and applications. Privacy risks and mitigation strategies applicable to PII maintained in the various systems and applications will be analyzed as appropriate in separate documentation; this Privacy Threshold Analysis (PTA) is limited to FBISE itself.

Access to FBISE is restricted to FBI personnel to include contract support staff, task-force members, and detailees from other agencies. All individuals with access to FBISE hold a minimum of a TOP SECRET clearance. Upon request and approval through the System Access Request (SAR) process, end users are issued password controlled login accounts allowing the end user(s) to authenticate and login to FBISE from designated workstations authorized to operate at the SECRET level.

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

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

__X__ YES **[If yes, please continue.]**

Other than login identifiers and user audit log information, any PII contained on FBISE is accessed through various applications such as SharePoint. This PTA is limited in scope to FBISE alone and does not address these kinds of applications nor the information they contain.

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

__X__ The information directly identifies specific individuals.

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

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

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

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

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

_____ NO __X__ YES

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

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

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

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

__X__ NO **[If no, proceed to question 7.]** Except for login information and information contained in audit logs, information is not collected directly from the individual who is the subject of the information.

_____ 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.

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

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

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

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

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

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

8. Is the system operated by a contractor?

__X__ No.

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

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

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

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

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

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

FBISE was recertified on 14 MAR 2012 with an expiry of 13 MAR 2015. Case ID: 319U-HQ-A1487677-SECD Serial: 2709

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.

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)?

__X__ NO

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

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

_____ NO __X__ YES

12. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? July 11, 2003

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

__X__ NO _____ YES

If yes:

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

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

___ NO ___YES

[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.]

(Rev. 06/08/2010)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: Service Manager (SM) [formerly known as ServiceCenter]

BIKR FBI Unique Asset ID: SYS 000080

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: IT Specialist [redacted] Program Office: Information Technology Engineering Division (ITED) Division: Office of the Chief Information Officer Phone: [redacted] Room Number: GP 703	**FBI OGC/PCLU POC** Name: AGC [redacted] Phone: [redacted] Room Number: 7350 JEH

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title: [redacted]	Signature: Date signed: Name: Title: [redacted]
FBIHQ Division: Information Technology Engineering Division	Signature: [redacted] Date signed: 2-11-11 Name: [redacted] Title: Unit Chief, Directory Services and Systems Management Engineering Unit	Signature: [redacted] Date signed: 2-11-11 [redacted] Name: [redacted] Title: Division Privacy Officer, ITMD

b6
b7C

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

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

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

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

Applicable SORN(s): Bureau Personnel Management System (BPMS), Justice/FBI-008

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 __X__ Yes
PCLU will follow up with FBI help desks utilizing Service Manager regarding some form of Privacy Act statement to help desk callers whose PII is solicited in order to verify caller's identities.

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:

Service Manager (SM) is used for internal government operations (identifying personnel contacting internal help desks and identifying IT equipment inventory). Any PII contained in SM's Oracle database or contacts table pertains solely to FBI personnel, including contractors and task force officers with access to FBI IT equipment, and is used to support agency administrative functions. To the extent that a PIA may be deemed necessaary because the SM contacts table contains PII imported from BPMS, the contacts table constitutes a routine FBI database for which a PIA has already been completed. A copy of the routine database checklist for the SM contacts table is attached.

Elizabeth Ross Withnell Acting Deputy General Counsel & FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 3/11/20

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 FBI's existing IT Support application, ServiceCenter, is being upgraded to **Service Manager (SM).** SM is a Hewlett-Packard (HP) Windows application used by the FBI to record, monitor, report, and resolve Service Desk tickets (Incidents, Problems, and Changes). SM also tracks Bureau IT Acquisition Requests and IT Inventory using the Property Management Application (PMA)[1] in order to help manage the FBI's IT enterprise infrastructure.

The SM application resides on servers operating on the FBI's Secret Enclave and integrates with other enterprise management tools. Upgrading ServiceCenter to SM will consolidate technical and operational support activities in order to deliver support service more effectively and efficiently across the FBI IT infrastructure.

SM supports four separate help desk centers: (1) Enterprise Operations Center (EOC) Help Desk; (2) Human Resources Division (HRD) Help Desk; (3) Records Management Division (RMD) Help Desk; and (4) Financial Division (FD) Help Desk for Travel Transfer Payment Unit (TTPU). Whenever a service call is received by any one of the help desks, SM is used to create, and then monitor the status of, service request tickets. An Oracle database is used to store information about pending and closed IT service tickets so that the information may be readily retrieved by help desk personnel. The Oracle database also generates a contacts table displaying certain identifying information about FBI personnel. This information is used both to verify the identity of individuals contacting help desks as well as to create service tickets. The database is populated daily with current information imported from the Bureau Personnel Management System (BPMS), Justice/FBI-008.

SM enhancements to ServiceCenter are being deployed in phases. Phase one, currently underway, involves the EOC Call Center Module which will be pre-deployed for the Information Technology Branch (ITB) at four Field Offices (San Francisco, Washington, DC, Chicago and Tampa). Phase two, scheduled for deployment later in 2011, will include full deployment of the EOC Call Center as well as deployment of the HRD, RMD and FD Call Centers. Phase three, not yet scheduled, will include several

[1] PMA is one of the FBI's Administrative Mainframe Applications. PMA is a legacy application in service prior to April 17, 2003; no significant changes have been made to PMAS since that time affecting privacy risks.

other modules designed to facilitate either the resolution of IT issues or the acquisition or maintenance of IT assets.[2]

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

_____ NO

__X__ YES

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

__X__ The information directly identifies specific individuals.

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

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

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

FBI help desk personnel utilize the SM contacts table to confirm the identity of individuals requesting service as well as to create a service ticket documenting the interaction and assigning the issue for resolution. The employee data fields in the contacts table available to personnel assigned to all four help desks (see below) include name, telephone number, division to which assigned, unit cost code and office location.

In addition, personnel assigned to the HRD, RMD and FD help desks will be able to view employee Social Security Numbers (SSNs) in the SM contacts table. These particular employees require access to employee SSNs in order to perform their duties. HRD help desk personnel must include SSNs on HRD service tickets for personnel issues, since the SSN is used as a primary employee identifier. RMD help desk personnel require access to employee SSNs because they handle employment verification requests concerning on-board and former FBI personnel. FD help desk personnel must include SSNs on FD service tickets to resolve travel and relocation-related tax issues. EOC help desk personnel, in contrast, do not require access to SSNs and are therefore unable to view them in the contacts table.

[2] For convenience, this PTA also addresses the SM HRD and RMD help desk modules, although those help desks presently use the ServiceCenter legacy application.

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

_____ NO __X__ YES

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

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

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

As noted above, the SM database documents pending and closed service requests. While information about a service ticket is normally retrieved from the database by ticket number, the database can also be searched by employee name in the event a ticket number is unavailable.

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

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

__X__ YES

Help desk personnel ask individuals calling the help desk for identifying information and then compare the information provided with the information in the SM contacts table in order to verify the caller's identity. In addition, an individual's assignment information as contained in BPMS (and hence, in the SM contacts table) may not have be current in light of a TDY or permanent reassignment.

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

__X__ NO

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

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

__X__ NO

_____ YES

PCLU will follow up with help desk supervisors to determine whether an (e)(3) notice may be posted on the home page for each of the four SM help desks.

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

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

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

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

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

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

Personnel SSNs are imported daily from BPMS into the SM database and used to populate the contacts table. Those SSNs may be viewed by personnel assigned to the HRD, RMD or FD help desks with a need to verify the SSN. Developers and system administrators assigned to SM also have access to SSNs as they maintain the system. As noted above, EOC help desk personnel using SM are unable to view SSNs, since they do not require that information to carry out their duties.

The SM application, including its database, resides on the FBI's Secret Enclave. As a result, SM may only be accessed from the Bureau's secure classified network, which has an existing robust auditing capability.

In light of the continuing need to reduce use of SSNs, PCLU will coordinate with the appropriate help desk supervisors to attempt to limit the solicitation of SSNs by RMD, HRD and FD help desks to the four digits, which can then be compared to the full SSN contained in the SM contacts table. In the event that the last four digits do not match those contained in the Contacts Table, the caller may then be asked to provide a full SSN.

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

8. Is the system operated by a contractor?

__X__ No.

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

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

___ NO

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

ServiceCenter was certified/recertified on January 9, 2008.

Confidentiality:	**__Low**	**__Moderate**	**__X__ High**
Integrity:	**__Low**	**__Moderate**	**__X__ High**
Availability:	**__Low**	**__Moderate**	**__X__ High**

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

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

____ NO

__X__ YES

ServiceCenter is one of several systems subsumed in the FY 2011 OMB300 for the *FBI Administrative Systems Support*, UPI no. 011-10-01-03-02-2045-00.

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53?

__X__ NO

_____ YES

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

__X__ NO _____ YES

13. Status of System/ Project: Phase 1 of the SM application is being deployed; phase 2 is undergoing testing prior to deployment.

_____ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

SM is an enhancement to the existing ServiceCenter application currently used by the FBI. ServiceCenter was originally deployed in late 1999, with the addition of an EOC help desk in 2000.

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

__X__ 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?

__X__ NO ____YES

If yes:

a. **Provide date/title of the PIA:**
b. Has the system/project undergone any significant changes since the PIA?

___ NO ___ YES

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: _____

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Platform Support Unit Division: Information Technology Services Division (ITSD) Phone: [redacted] Room Number: QP-703	**FBI OGC/PCLU POC** Name: [redacted] Phone: [redacted] Room Number: 7350

b6
b7C

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

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: ITSD	Signature: [redacted] Date signed: 6/23/11 Name: [redacted] Title: Unit Chief	Signature: [redacted] Date signed: 6/24/11 Name: [redacted] Title: OGC Specialist
FBIHQ Division: ITSD	Signature: [redacted] Date signed: 6/23/2011 Name: [redacted] Title: SITS	Signature: Date signed: Name: SAME Title:

b6
b7C

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

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

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

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

__X__ PIA is not required for the following reason(s):
___ System does not collect, maintain, or disseminate PII.
___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
___ Information in the system relates to internal government operations.
___ System has been previously assessed under an evaluation similar to a PIA.
__X__ No significant privacy issues (or privacy issues are unchanged). [redacted] b7E
[redacted]
___ Other (describe):

Applicable SORN(s): _____N/A_____

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No ___Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? ___No ___Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? ___No ___Yes (indicate forms affected):

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

Other:

Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 7/5/11

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

This PTA covers the [redacted] b7E

[redacted] which was the subject of a previous PTA. The purpose of this tool is to [redacted]

[redacted] b7E

[redacted] b7E

[redacted] No data is stored within [redacted]

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

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

_____ YES **[If yes, please continue.]**

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

_____ The information directly identifies specific individuals.

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

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

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

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

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

_____ NO _____ YES

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

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

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

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

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

_____ YES

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

_____ NO

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

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

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

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

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

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

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

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

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

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

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

8. Is the system operated by a contractor?

_____No.

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

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

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

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

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

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

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

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

_____ NO

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

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

_____ NO

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

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

_____ NO _____ YES

13. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

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

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

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

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

(For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

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

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

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

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

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

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

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

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

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

_____ NO _____ YES

If yes:

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

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

___ NO ___ YES

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: [redacted] b3 b7E

BIKR FBI Unique Asset ID: SYS-0000074

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [redacted] Program Office: Technical Response Unit (TRU) Division: Operational Technology Division (OTD) Phone: [redacted] Room Number: ERF-3	FBI OGC/PCLU POC Name: [redacted] Phone: [redacted] Room Number: 7350 JEH

b6 b7C

FBI DIVISION INTERMEDIATE APPROVALS (complete as necessary consonant with Division policy)

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Technical Response Unit	Signature: [redacted] Date signed: 7/6/10 Name: SSA [redacted] Title: UC Acting	Signature: [redacted] Date signed: 08/5/10 Name: SC J. Clay Price 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 7350). (The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

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

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

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

1- DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov; 1 - OGC\PCLU Intranet
If classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530)
2- FBI OCIO / OIPP [redacted]
1- FBI SecD/AU (UC [redacted]
1- RMD/RMAU [redacted]
1- Program Division POC
1- Division 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 FBI.GOV (after any RMD FOIA redactions)? ___ Yes. ___ No (indicate reason):

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

Applicable SORN(s): DOJ-002, Department of Justice (DOJ) Computer Systems Activity and Access Records, DOJ-002, 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? __x_No ___Yes--See sample EC on PCLU intranet website here: https://home/DO/OGC/LTB/PCLU/Privacy Civil%20Liberties%20Library/form_for_miog190-2-3_ec.wpd

SORN/SORN revision(s) required? _x__No ____Yes (indicate revisions needed):

Prepare/revise/add Privacy Act (e)(3) statements for related forms? _x__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 records 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: 8/5/10

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

[redacted]

When a user logs onto the user's computer [redacted] the user first enters a user name and password in [redacted] then the user enters a separate user name and password [redacted] stores the username and password used to log onto [redacted] In addition, [redacted] creates audit logs used to monitor [redacted] activity for security purposes.

b3
b7E

[redacted]

b3
b7E

[redacted] and such information could be used to support a criminal, CT, or FCI investigation, this system is [redacted] such information and not the place where the information is stored or manipulated.

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

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

___x___ YES **[If yes, please continue.]**

The system maintains user names and passwords. In addition, the system creates and maintains audit logs. [redacted] b3 b7E

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

__x__ The information directly identifies specific individuals.

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

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

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

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

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

_____ NO ___x__ YES
The user names, passwords, and audit logs pertain to government employees, contractors, or consultants. [redacted] b7E

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

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

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

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

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

_X__ YES