FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: Document Capture System Interim Central Records Complex (DCS-ICRC)
BIKR FBI Unique Asset ID: 2005-005-01-C-404-142-3284

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: RMD Division: 17 Phone: [redacted] Room Number: J-24	**FBI OGC/PCLU POC** Name: [redacted] Phone: [redacted] Room Number: JEH 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: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Records Management Division	Signature: Date signed: 8/5/2010 Name: John C. Krysa Title: RAS Section Chief	Signature: Date signed: 8/9/2010 Name: David Hardy Title: RIDS Section Chief

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): _N/A_____

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:

Elizabeth Withnell, Acting Deputy General Counsel Acting FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 8/9/10

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.):

The Document Capture System-Interim Central Records Complex (DCS-ICRC or DCS), is a system that allows users to scan documents, convert the image to the appropriate format, and then transfer the image to the appropriate medium, such as a compact disc, thumb drive, hard drive, and/or electronic storage space for use in FOIA processing or other applications, for storage. After scanning, the files may be converted to both a TIFF image and OCR text (OCR and TIFF are types of electronic files) for electronic storage. Information is only stored in the system for the period of time needed to complete the scan of the document and transfer the document to the appropriate medium or other applications. Since information is not stored within DCS beyond this period, the documents cannot be searched and information cannot be retrieved from the documents. Access to the DCS is limited to those individuals with a user ID and password.

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 only information about individuals collected, maintained, or disseminated by this system consists of user names and passwords of employees or contractors. Because this is a system that scans documents, one should assume that the system will contain information about individuals. However, as indicated above, this information is only stored for the period of time needed to transfer the document from paper to electronic format. Thus, the DCS is merely a conduit used to complete an interagency function.

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?

___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?

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

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

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

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

_____ YES

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

_____ NO

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

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

_____ NO **[The program will need to work with PCLU to develop/implement**

the necessary form(s).]

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

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

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

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

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

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

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

_x____ It is not feasible for the system/project to provide special protection to SSNs. **Explain:** DCS is a document scanning tool. The collection of social security numbers that may be contained in the documents scanned has already been deemed necessary to carry out the particular function. DCS *does not* maintain a copy of the document scanned once the scanning process is complete.

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: October 2007.

Confidentiality:__Low__Moderate _x_High __Undefined

Integrity: __Low _x_Moderate __High __Undefined

Availability: __Low _x_Moderate __High __Undefined

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

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

__x___ NO

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

11. Does the system conduct data mining as defined in Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (codified at 42 USC 2000ee-3)?
__x___ NO

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

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

__x___ 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?

DCS was developed in May 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.

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

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

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

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

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

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

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

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

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

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

__x___ NO _____ YES

**A PTA, entitled "Document Capture System – Interim Central Records Complex," was completed in 2007. The system has not undergone significant changes since the last PTA.

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.]

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Digital Collection System Network (DCSNET)

BIKR FBI Unique Asset ID: NEN-0000013

Derived From: **Classified By:** **Reason:** **Declassify On:**	**SYSTEM/PROJECT POC** Name: Electronics Egr. [redacted] Program Office: TICTU Division: OTD Phone [redacted] Room Number: 4A39 ERF-E	**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: **Operational Technology Division**	Signature: [redacted] Date signed: 02/12/14 Name: [redacted] Title: Acting Unit Chief, Telecom. Intercept and Collection Technology Unit (TICTU)	Signature [redacted] Date signed: 2/12/14 Name: SSA [redacted] Title: Assistant Section Chief, Technical Surveillance Section
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PIA 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).
- ____ Information in the system relates to internal government operations.
- ____ System has been previously assessed under an evaluation similar to a PIA.
- ____ No significant privacy issues (or privacy issues are unchanged).
- __X__ Other.

The DCSNET is the IT network used for transmission of electronic surveillance (ELSUR) data collected from telecommunications service providers (TSPS) between FBI IT data analysis systems, [redacted] The ELSUR data is encrypted while travelling through the DCSNet and cannot be decrypted. The only PII maintained by the DCSNET is system administrator access and activity information [redacted] b7E

Since the DCSNET functions as a pipeline between IT systems and store only access and activity data about system administrators, it constitutes IT architecture for which no PIA is required.

Applicable SORN(s): ___DOJ Computer Systems Activity and Access Records, DOJ-002, 64 Fed. Reg. 73585 (Dec. 30, 1999)

Notify FBI RMD/RIDS per MIOG 190.2.3? __X__ No ____Yes--See sample LC 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:

Monica E. Ryan Unit Chief, Privacy and Civil Liberties Unit FBI Privacy and Civil Liberties Officer	Signature: [signature] Date Signed: 6/18/14

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.**

The FBI's Telecommunications Intercept and Collection Technology Unit's (TICTU) mission is to ensure that ability to access and lawfully collect evidence and intelligence through the development, deployment and support of wire-line and wireless electronic surveillance (ELSUR) intercept capabilities, as well as the development and deployment of field office ELSUR information management and collection systems. In support of this mission, TICTU is responsible for providing equipment to the field, troubleshooting problems with equipment and systems, providing training to field office users, tracking needs of the field to identify new ELSUR requirements, and serving as the FBI's technical liaison with telecommunications service providers.

The TICTU manages, at the enterprise level, the Digital Collection System Network (DCSNET). The DCSNET is a fully meshed unclassified network [redacted] b7E [redacted] The DCSNET is a conduit transporting ELSUR data between operational IT systems; [redacted]

The digital information transported along the DCSNET is lawfully acquired through various ELSUR techniques, and includes [redacted] b7E [redacted] real-time data (such as telephone or e-mail routing information) provided by telecommunications carriers subject to the Communications Assistance for Law Enforcement Act (CALEA). The data travelling through the DCSNET is encrypted and cannot be accessed by end users (e.g., Special Agents and analysts) until after the data arrives at its destination point.

Because the data travelling through DCSNET does not remain in the system, the only personally identifiable information (PII) maintained in DCSNET are the names and user names [redacted] b7E all assigned to TICTU, who have been designated as system administers for DCSNET and therefore require direct access to the network in order to maintain it and provide network-related IT support. This information is contained in access and activity logs maintained online for ninety days and offline for ten years, in accordance with the DCSNET system security plan (SSP).

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.]**

As explained supra, the only PII maintained by DCSNET are the names and user names [redacted] all assigned to the TICTU, who have been designated as system administrators. b7E

_____ 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, CI, or FCI investigations or assessments?

_____ NO

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

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

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

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

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

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

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

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

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

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

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

8. Is the system operated by a contractor?

____No.

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

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

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

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

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

Confidentiality: __Low __Moderate __High __Undefined
Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

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

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

_____ NO

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

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

_____ NO _____ YES

12. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

__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.]

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: SYS-0000144

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [redacted] Program Office: Division: Counterintelligence Phone: [redacted] Room Number: 5989	FBI OGC/PCLU POC Name: [redacted] b6 b7C Phone: [redacted] Room Number: 7350

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: Counterintelligence	Signature: [redacted] Date signed: 6/27/2011 Name: SSA [redacted] Title: CD Program Manager	Signature: [redacted] Date signed: 6-27-11 Name: [redacted] b6 b7C Title: [illegible]
FBIHQ Division: (insert division name)	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 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: [This section will be completed by the FBI PCLU/PCLO following PTA submission. The PTA drafter should skip to the next page and continue.]

_X_ PIA is required by the E-Government Act. Deconfliction should be included in the CORE PIA revision.

_____ 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): _____CRS-DOJ/FBI-002; ultimately system should be covered by a separate SORN for CORE

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No _X__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 _X__Yes (indicate revisions needed): See above

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

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

Other:

[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 7/5/11
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 7/7/11

b6
b7C

UNCLASSIFIED

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

This PTA is intended to update [redacted] formerly known as the [redacted] PIA dated November 23, 2010. [redacted] was originally intended to help FBI Headquarters elements manage relationships with affiliates in industry, academia or other sectors who help the FBI identify risks and how to protect against them. The [redacted] is changing its name, but more importantly is also expanding coverage to Domain and Collection managers in the field, who will be provided read-only access to the tool in anticipation of [redacted] being integrated into the capabilities of [redacted] b7E

Domain and Collection Coordinators need to be able to review all interactions that have taken place as a result of outreach and interface initiatives in both the private and public sectors through such programs as Business Alliance, Academic Alliance, and Counterintelligence Working Groups. [redacted] will provide a shared liaison contacts database, which ultimately will be part of [redacted] that will enhance knowledge about where the FBI has liaison contacts and where such contacts need to be established. Users will be able to review relationships and the history of interactions with liaison contacts in a format that supports ongoing activities and planning. b7E

The privacy of information about domain liaison contacts will be protected because the personal information on such contacts will be viewable only with appropriate permission based on justification to a case agent who has entered the contact into the system. An email notification will be sent to the case agent when someone attempts to obtain information about a liaison contact. In addition, the information at issue is maintained only on internal FBI systems, thereby limiting the possibility of access outside the FBI.

When the PIA for [redacted] is revised to reflect additional functionality, [redacted] will be addressed as well, since the intent is to integrate these two data sources. b7E

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

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

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

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

__X__ The information directly identifies specific individuals.

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

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

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?

__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?

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

__X__ YES Domain liaison contact information is collected from individual who volunteer to be liaison contacts.

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

_____ NO

__X__ YES **(If yes, proceed to question 7.)**

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

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

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

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

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

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

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

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

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

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

8. Is the system operated by a contractor?

_____No.

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

imposed as a matter of Department of Justice policy. Consultations with the Office of the General Counsel may be required if a contractor is operating the system for the FBI.

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

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

SecD has stated that this does not need a separate C&A because it is part of SharePoint, and SharePoint is part of the Secret Enclave.

_____ 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)?

__X__ NO _____ YES

12. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 2009-10

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.

_____ 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.

__X__ 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 __X__ YES

If yes:

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

[redacted] approved November 23, 2010. b7E

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

___ NO __X_ 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.]

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Delta

BIKR FBI Unique Asset ID: SYS-0000138

Derived From: Not Applicable Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Domain Collection HUMINT Technical Unit Division: Directorate of Intelligence Phone: [redacted] Room Number: 11079X	**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: IT Management Division	Signature: [redacted] Date signed: 4/3/12 Name: [redacted] Title: Program Management Executive	Signature: [redacted] Date signed: 4/5/2012 Name: [redacted] Title: Information Technology Specialist
FBIHQ Division: Directorate of Intelligence (DI)	Signature: [redacted] Date signed: 4/30/2012 Name: Eric Velez-Villar Title: Assistant Director DI	Signature: [redacted] Date signed: 5/3/2012 Name: [redacted] Title: Privacy Officer for the Directorate of Intelligence

b6
b7C

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

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

_____ PIA is required by the E-Government Act.

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

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

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

Applicable SORN(s): _____

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:

[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 4/6/12
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 4/10/12

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

Name of the system/project: The name of the system is "Delta". "Delta" is not an acronym.

Structure of the system/project: The Delta system [redacted] data regarding Confidential Human Sources (CHSs). [redacted] Delta's users can also [redacted] b3 b7E

Purpose: In order to respond to a post-9/11 environment and to the recommendations from the 9/11 Commission and the Weapons of Mass Destruction Commission for changes in the Intelligence Community, significant changes in the FBI's Asset/Informant program were warranted. The Delta system was designed and executed in response to these recommendations and in response to directives from Congress and the Department of Justice (DOJ). It implements improvements for the management and administration of the FBI's CHSs and their intelligence. Delta addresses every aspect of handling information and intelligence derived from CHSs [redacted] Furthermore, Delta provides enhanced security to protect CHS identifying information and also leverages the existing security enhancements provided by the Public Key Infrastructure (PKI). b3 b7E

Nature of the information in the system: By policy, Delta contains information that [redacted] each CHS the FBI operates [redacted] is also captured and maintained in Delta. Intelligence information is shared among the operational divisions within the FBI. Intelligence Analysts also [redacted] Lastly, FBI Agents use the information for case investigation and management. b3 b7E

How information in the system will be used: Delta users are Special Agents, Supervisory Special Agents, Intelligence Analysts. [redacted] b3 b7E

[redacted] in the Delta system [redacted] a Case Agent for the CHS. Access to [redacted] information is highly controlled and strictly enforced by the system. b3 b7E

Who will have access to the information and the manner of transmission to all users:
Delta currently operates [redacted] Only users, such as Special Agents, Supervisory Special Agents, Intelligence Analysts, [redacted] who are enrolled in Delta [redacted] have access to Delta. Access to most of the information in Delta is through [redacted] although some forms require use of SharePoint forms using a software client on users' workstations. b3 b7E

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

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

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

Delta contains information identifying [redacted] a CHS [redacted] Although Delta contains the name(s) of CHSs, [redacted] Delta users [redacted] Delta, [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 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?

__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?

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

__X__ YES

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

_____ NO

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

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

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

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

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

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

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

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

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

__X__ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:** SSNs are considered sensitive information about a CHS. Consequently, access to this information is limited by a role-based access security feature in Delta. By policy, only a [redacted] will have access to this sensitive identifying information. b3 b7E

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

8. Is the system operated by a contractor?

_____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:

Authority to Operate (ATO) was granted on 05/19/2009
per EC 319U-HQ-A1487677-SECD Serial #1670

Confidentiality: __Low __Moderate _X_High __Undefined

Integrity: __Low __Moderate _X_High __Undefined

Availability: __Low _X_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:

_____ 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? **Response:** It was first deployed in a limited pilot to [redacted] Field Offices on May 14, 2008. **b3 b7E**

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.

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

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

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

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

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

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

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

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

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

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

_____ NO __X__ YES

If yes:

a. **Provide date/title of the PIA: Response:** EC dated [redacted] subject "[redacted] Privacy Impact Assessment (PIA)"; Case ID #: [redacted] b3 b7E

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

__X__ NO __YES

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Sentinel Release

BIKR FBI Unique Asset ID: SYS-000026

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

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: CID	Signature: [redacted] Date signed: 12-12-2011 Name: [redacted] Title: Program Manager	Signature: [redacted] Date signed: 12-13-2011 Name: [redacted] Title: CID Privacy Officer [redacted]
FBIHQ Division: ITSD	Signature: [redacted] Date signed: 12/12/2011 Name: [redacted] Title: IT Specialist	Signature: [redacted] Date signed: 12-15-11 Name: [redacted] Title: Chief, Process Policy and Metrics

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.
- ___ No significant privacy issues (or privacy issues are unchanged).
- ___ Other (describe):

Will be covered by the FBI's PIA for entire database.

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

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No _x__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): Information is not collected by the FBI directly from the individual; however, PCLU may consult with DOJ about adding a Privacy Act statement to its USM 3A form.

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:
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 12-5-12

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The database contains the task force names for each of the FBI's field offices, the program that has oversight of the task force, the type of deputation requested (Title 18 or Title 21), case file number, task force officers names, social security numbers, and dates of deputation. The database is holding historic and current information concerning the FBI's task force officers. This information is used to provide the Director with the number of deputized officers and the types of deputations they are holding. The information is also used to remind field offices to deputize officers whose deputations are getting ready to expire. The information is collected as a way to track all deputized task force officers and to provide information concerning the officers to the Director and the FBI's field offices.

The Deputation Database consists of [redacted] utilizes [redacted] utilizes [redacted] b7E

The database has a nightly backup to the data center [redacted] to be used in the event of a COOP.

The Deputation Database is only available on FBI workstations, accredited to the SECRET level. It is accessed through an internal web browser. Users must be authenticated before viewing or modifying data. [redacted] b7E ensures the user's identification (i.e. user ID) is stored in the application's User Table. Deputation Database Developer accounts are created by the [redacted] database administrator and require a unique id and password for login.

Access is limited to the Criminal Investigation Division Operational Support Section Administrative Unit at Headquarters and to employees responsible for the processing the deputation candidates in the Field Offices. The application has a role based security matrix for access and manipulation of the data. The application has a System Administrator (ITSD) and an Owner (Criminal Investigation Division) who will have access to the User Table. 1 Tthe Owner is responsible for granting access to the database for the following roles: Reports Only, Read Only, Modify, and Owner. The Owner is the only one who

grants access to the field offices. The System Administrator is responsible for granting access for the Admin and Owner roles. No one outside the FBI will have access to the application. All categories of Users who no longer require access to the Deputation Database will be removed from the User Table. Once removed, users are unable to login; however, their account transaction records will be retained in the Deputation Database for reference purposes.

The Deputation Database audits seven types of user activities: successful login, unsuccessful login, authentic user-but no valid role (users without a valid role are not allowed past the login screen), data created, data modified, data deleted and data accessed. Audit logs will be reviewed by the Information Systems Security Officer (ISSO) as required. All audit records are accessible only by the ISSO and system developers; they are not accessible by General Users or Owners. The audit logs are read-only and may not be modified or deleted.

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

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

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

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

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

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

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

_____ NO __X__ YES

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

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

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

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

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

__X__ YES

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

__X__ NO

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

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

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

__X__ YES **Identify any forms, paper or electronic, used to request such information from the information subject:** The subjects fill out USM 3A (Application for Special Deputation) – this is a US Marshal's form for Title 18 Deputation. The Field Office Supervisor's fill out the FD-815 for Title 21 Deputation.

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:**

_____ 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**: The Deputation Database is a minor application, and so it is not separately C & A'd but rather it is reviewed by Security Division as part of the [redacted] and so it falls under the accreditation of the Enterprise Servers. The Deputation Database is registered within the Bureau IT Knowledge Repository (BIKR). Security Division issued its approval for use of the system in 2009. b7E

____ YES **If yes, please indicate the following, if known: Not 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)?

__X__ NO _____ YES

12. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 11/05/2001

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.

Original database was an MS Access housed on a division's shared drive. Use of the [redacted] permits access and use controls to be employed [redacted] with the Access version. [redacted] therefore creates a more secure environment than the earlier

b7E

Access version. In addition, [redacted] Demutation Database [redacted] is backed up nightly to the FBI's data center [redacted] while the previous Microsoft Access environment was backed up on Division servers. b7E

_____ 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.]

1 - Signed original to file 190-HQ-C1321794 (send to [redacted])

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) (PIAs
and PTAs are not sent in all cases, please discuss first with [redacted] if you are unsure.)
1- FBI OCIO / OIPP ([redacted]) (attachment via email)
1- FBI SecD/AU (UC [redacted] & [redacted] & [redacted]) (send
SharePoint link from website)
1- RMD/RMAU ([redacted]) (attachment via email)
1- Program Division POC
1- Division Privacy Officer
1-OGC\PCLU intranet

b6
b7C

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

Total Deleted Page(s) = 2
Page 1 ~ Duplicate;
Page 2 ~ Duplicate;

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

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

Total Deleted Page(s) = 6
Page 1 ~ Duplicate;
Page 2 ~ Duplicate;
Page 3 ~ Duplicate;
Page 4 ~ Duplicate;
Page 5 ~ Duplicate;
Page 6 ~ Duplicate;

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Document Capture System Headquarters (DCS-HQ) System

BIKR FBI Unique Asset ID: SYS-000269

Derived From: **Classified By:** **Reason:** **Declassify On:**	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: RMD - BOSU Division: 17 Phone: [redacted] Room Number: BOSU	**FBI OGC/PCLU POC** Name: Phone: Room Number:

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:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Records Management Division	Signature: [redacted] Date signed: 4-3-12 Name: [redacted] Title: Acting RAS Section Chief	Signature: [signature] Date signed: 4/11/2012 Name: David Hardy Title: RIDS Section Chief

b6
b7C

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

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ 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):

DCS-HQ is merely for converting paper records to electronic copies for use by the relevant submitter. The submitter has the responsibility for completing privacy documentation, if appropriate.

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? __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:

James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 4/30/12

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 Document Capture System-Headquarters (DCS-HQ) system is a complementary system to DCS-Interim Central Records Complex, described in a separate PTA. http://home.fbinet.fbi/DO/OGC/LTB/PCLU/PrivacyCivil%20Liberties%20Library/DCS-ICRC%20%20%20%20%20(pdf).pdf . DCS-HQ will allow [redacted] b7E personnel at FBI Headquarters to scan documents, convert the image to the appropriate format, and then transfer the image to removable medium, such as a compact disc or thumb drive for use by requesting personnel, other applications, or for storage by other systems.

This system will support Scan on Demand (SOD), a program that facilitates walk-in requests for scanning conversion from FBI Headquarters. Other areas that the DCS-HQ will support are:

Special Access Projects through RAS Management and Logistics Unit (M&L)
The Directors Executive staff requests and from the AD
263 classification files from the Special File Room (SFR)

At times requests may come in from the field offices. These are usually small requests. In addition, the system may be used to help with overflow of FOIA requests.

The output of the DCS-HQ provides a digital representation of documents that can rapidly and efficiently be retrieved, searched, and analyzed by other systems or personnel. In some cases, these electronic images will become official FBI files and will be managed under appropriate policies and directives.

[redacted] b7E The scanned documents are stored in the system for the period of time needed to complete the scan request and the transfer of the output to the appropriate medium, then removed from the system. Since the documents will not be stored within DCS-HQ beyond this period, the documents will not be searchable or information retrievable once the scan job is complete and the customer has accepted the digital media.

[redacted] b7E

b7E

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

_____ 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.]**

This system contains user names and passwords of employees or contractors for logon purposes and system auditing only. Because this is a system that scans documents, one should assume that the system will contain information about individuals. However, as indicated above, this information is only stored for the period of time needed to convert documents from paper to electronic format. DCS-HQ is merely a conduit used to complete an interagency function.

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?

__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?

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

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

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

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

_____ YES

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

_____ NO

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

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

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

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

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

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

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

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