

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT:

b7E

BIKR FBI Unique Asset ID: APP-0000256 (BIKR number for unclassified system pending)

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: SSA <input type="text"/>	Name: AGC <input type="text"/>
Program Office: Geospatial	Phone: <input type="text"/>
Division: DI	Room Number: JEH, Rm 7350
Phone: <input type="text"/>	
Room Number: 11100	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Records Management Division	Signature: <input type="text"/> Date signed: 2/18/13 Name: <input type="text"/> Title: Unit Chief	
Security Division:	Signature: <input type="text"/> Date signed: <input type="text"/> Name: <input type="text"/> Title: Assistant Section Chief	
Directorate of Intelligence:	Signature: <input type="text"/> Date signed: <input type="text"/> Name: <input type="text"/> Title: Unit Chief	Signature: <input type="text"/> Date signed: <input type="text"/> Name: <input type="text"/> Title: Management & Program Analyst

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:

PIA is required by the E-Government Act.

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

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

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

System does not collect, maintain, or disseminate PII.

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

Information in the system relates to internal government operations.

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

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

Other :

Applicable SORN(s): Central Records System, DOJ/FBI-002, 63 Fed. Reg. 8671 (Feb. 20, 1998) and Department of Justice Computer Systems Activity and Access Records, DOJ-002, 64 Fed. Reg. 73585 (Dec. 30, 1999)

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

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

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

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

Other:

Acting Unit Chief
Privacy and Civil Liberties Unit

Signature:
Date Signed: 1/13/12

Jacqueline F. Brown, Acting Deputy General Counsel
FBI Privacy and Civil Liberties Officer

Signature: *J. Brown*
Date Signed: 1/11/12

b6
b7c

UNCLASSIFIED//FOR OFFICIAL USE ONLY

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

b7E

b7E

b7E

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

Access to the unclassified version of [Redacted] will be limited to [Redacted] and direct support personnel, and the system is encrypted (https) and password protected to prevent unauthorized access. Usage logs will be maintained to provide audit tracking for user activity. FBI personnel in the [Redacted]

b7E

[Redacted]

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

will not contain any PII [Redacted]

[Redacted]

Information contained in the unclassified [Redacted] will be covered by the Central Records System system of records notice (SORN), as appropriate. Any information will be shared only in accordance with the routine uses in that published SORN and the FBI's Blanket Routine Uses, as published in the Federal Register. Any sharing outside of the [Redacted] will be on a case by case basis. No other entities will have direct access to input information in the tool.

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)?

[Redacted]

b7E

NO

YES [If yes, please continue.]

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

The information directly identifies specific individuals.

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

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

[Redacted] will not contain the names of FBI personnel. No other PII will be included in the data. [Redacted]

[Redacted]

b7E

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

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

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

NO YES

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

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

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

[Redacted]

b7E



b7E

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:

Since this is part of a pilot project, it has not undergone C&A at this point, but it will go through C&A at the appropriate stage. However, Security Division has reviewed and approved the use of this tool under the circumstances described above.

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

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

Confidentiality: Low Moderate High Undefined

Integrity: Low Moderate High Undefined

Availability: Low Moderate High Undefined

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

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

NO

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

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

NO YES

12. Status of System/ Project:

This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

NAME OF SYSTEM: Innocent Images Case Management (IICMS) (TECHNICAL REFRESH)

FBI SYSTEM CONTACT PERSON Name: [Redacted] Program Office: Division: IT Operations Phone: [Redacted] Room Number: 1334 Date PTA submitted for approval: 3/12/2008	FBI OGC/PCLU POC Name: Phone: Room Number:
--	--

b6
b7C

FBI DIVISION APPROVALS. A PIA (and/or PTA) should be prepared/approved by the cognizant program management in collaboration with IT, security, and end-user management and OGC/PCLU. (PIAs/PTAs relating to electronic forms/questionnaires implicating the Paperwork Reduction Act should also be coordinated with the RMD Forms Desk.) If the subject of a PTA/PIA is under the program cognizance of an FBIHQ Division, prior to forwarding to OGC the PTA/PIA must also be referred to the FBIHQ Division for program review and approval, if required by the FBIHQ Division.

	Program ID: [Redacted]	FBIHQ Division: IT Operations
Program Manager (or other appropriate executive as Division determines)	Signature: [Redacted] Date signed: 3/23/08 Name: [Redacted] Title: Acting Asst. Section Chief	Signature: [Redacted] Date signed: 3/24/2008 Name: [Redacted] Title: IT Specialist
Division Privacy Officer	Signature: [Redacted] Date signed: 3/26/2008 Name: [Redacted] Title: UNIT CHIEF	Signature: JM Sanchez Date signed: 3/24/08 Name: Jennifer R. Sanchez Title: Section Chief

b6
b7C

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

FINAL FBI APPROVAL:

FBI Privacy and Civil Liberties Officer	Signature: [Signature] Date Signed: 6/27/08 Name: David C. Larson Title: Acting Deputy General Counsel
---	---

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

1 - Signed original to 190-HQ-C1321794

Copies:

- 1 - DOJ Privacy and Civil Liberties Office-Main Justice, Room 4259
- 2 - FBI OCIO / OIPP
- 1 - FBI SecD (electronic copy via e-mail)
- 2* - Program Division POC /Privacy Officer
- 2*- FBIHQ Division POC /Privacy Officer
- (*please reproduce as needed for Program/Division file(s))
- 1 - OGC/PCLU intranet website
- 1 - PCLU Library
- 1 - PCLU Tickler

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Innocent Images Case Management (IICMS)

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

Whether or not a PIA is required, the system owner/program manager should consult with the FBI Records Management Division (RMD) to identify and resolve any records issues relating to information in the system.

A PTA contains basic questions about the nature of the system in addition to a basic system description. The questions are as follows:

A. General System Description: Please briefly describe:

1. Type of information in the system:

The IICMS contains copies of the FBI's 305 classification case and serial information that has been extracted on a daily basis from the Automated Case Support (ACS). Once loaded into the IICMS, analysts will attach other files collected as part of the undercover investigations pertaining to the on-line sexual exploitation of children. These attachments can be, at a minimum, chat room logs, web site captures, and images of minors of a sexually explicit nature.

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

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

To store evidentiary materials related to Sexual Exploitation Of Children (SEOC) cases that will be used as exhibits for trials, if necessary, by the Innocent Images National Initiative (IINI) staff.

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

The IICMS consists of [redacted] located at the II site in Calverton, MD. The IICMS consists of the [redacted]

b7E

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

There are two main methods for data to be entered into the IICMS. First, the IINI performs undercover investigations of online child predation. The data collected from these sessions is prepared by the undercover agent and delivered to an IINI analyst. The analyst [redacted] [redacted] The analyst will place the data files into the IICMS [redacted] [redacted] Second, all 305 case and serial data is extracted and sent [redacted] from ACS on a daily basis. The data is then stored within the IICMS.

b7E

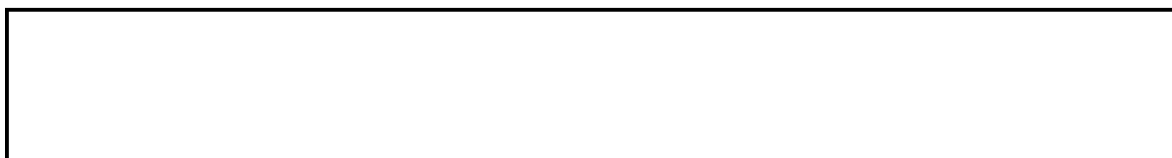
All customers of the IICMS [redacted] are located at the Calverton, MD site. [redacted]

b7E

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Innocent Images Case Management (IICMS)



b7E

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

All access to the IICMS will be approved by the IINI Program Manager at Calverton, MD. Accounts into the database, once approved, will be added by the on-site database administrator.

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

No one outside the FBI will have access to the IICMS.

7. Has this system been certified and accredited by the FBI Security Divisions? Yes No
The latest Authority to Operate dated 2/07/2006.

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

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

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

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

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

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

(Continue to Question 2.)

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

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

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Innocent Images Case Management System (IICMS)

BIKR FBI Unique Asset ID: SYS-0000043

	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [Redacted] Program Office: Division: IT Services Phone: [Redacted] Room Number: JEH 1339	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: Cyber	Signature: [Handwritten Signature] Date signed: 10/16/11 Name: Timothy Gallagher Title: Section Chief	Signature: [Redacted] Date signed: 9/20/2011 Name: [Redacted] Title: Supervisory Special Agent
FBIHQ Division: IT Services	Signature: [Redacted] Date signed: 10/17/11 Name: [Redacted] Title: Acting Section Chief	Signature: [Redacted] Date signed: 10-26-11 Name: [Redacted] Title: IT Specialist

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:
Due to the sensitive nature of this system, the PIA will not be published.

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): Central Records System (CRS), DOI/FBI-002

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

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

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

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

Other:

[Redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [Redacted] Date Signed: 10/27/11
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: [Handwritten Signature] Date Signed: 10/21/11

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.

(U//~~FOUO~~) The Innocent Images Case Management System (IICMS) is a centralized data warehouse residing on the FBINET Intranet. The purpose of IICMS is to store copies of evidentiary materials related to Sexual Exploitation of Children cases that will be used as exhibits for trials, if necessary, by the Innocent Images National Initiative staff.

(U//~~FOUO~~) IICMS contains copies of the FBI's 305 classification case (child pornography) and serial information that has been extracted on a daily basis. [redacted]

[redacted]

[redacted] Once loaded into the IICMS, analysts attach other files collected as part of the undercover investigations pertaining to the online sexual exploitation of children. These attachments can be, at a minimum, chat room logs, web site captures,

[redacted]

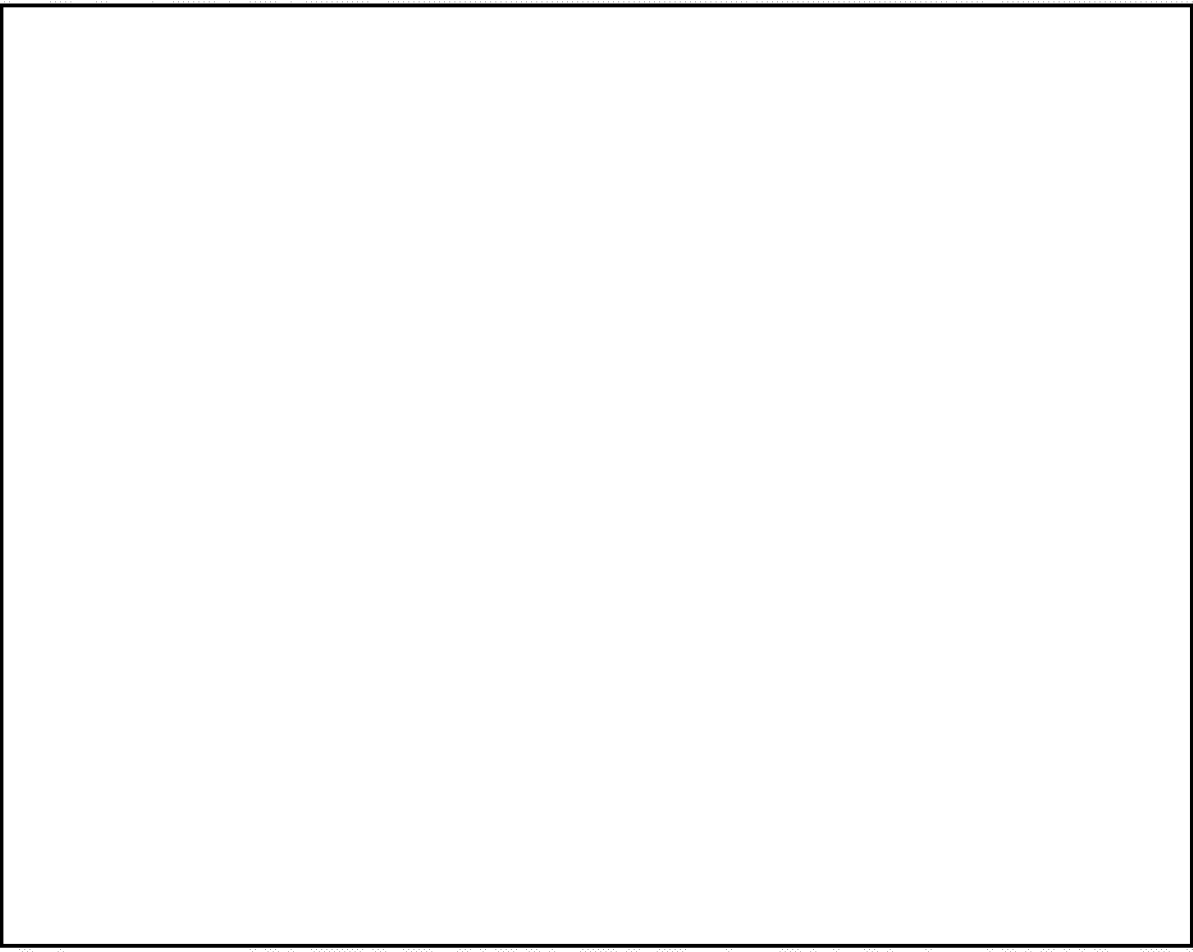
[redacted]

[redacted]

b7E

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

X YES (If yes, please continue.)

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

(Check all that apply.)

X The information directly identifies specific individuals.

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

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

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

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

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

NO YES

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

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

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

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

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

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:** IICMS data consists of unstructured data, such as text files, WordPerfect documents as well as official FBI documents. This data does not specifically identify SSNs as much of the data is free text. Thus, it is not realistically feasible to identify all occurrences of SSNs in the system. Additionally, SSNs are necessary to properly identify a subject within the system.

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: C&A received February 8, 2011.

Confidentiality: Low Moderate 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.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? October 1, 2002

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.)

The IICMS has added the Innocent Images Field Query (IIFQ) web application, allowing authorized field users access to the IICMS dataset. Additionally, IICMS has undergone a full technical refresh, upgrading server hardware and software. These hardware and software upgrades provide greater security, access control, and encryption of the IICMS data.

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

~~Sensitive But Unclassified//For Official Use Only~~

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

NAME OF SYSTEM / PROJECT: INTELPLUS

BIKR FBI Unique Asset ID: SYS-0000048

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: <input type="text"/> Program Office: ITSD Division: ITSD Phone: <input type="text"/> Room Number: 1333B	FBI OGC/PCLU POC Name: <input type="text"/> Phone: <input type="text"/> 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: Information Technology Services Division (ITSD).	Signature: /s/ Date signed: 9/13/2010 Name: Daniel D. Dubree Title: Assistant Director	Signature: /s/ Date signed: 9/21/2010 Name: <input type="text"/> Title: Information Technology Specialist
FBIHQ Division: Information Technology Services Division (ITSD).	Signature: /s/ Date signed: 9/13/2010 Name: Daniel D. Dubree Title: Assistant Director	Signature: /s/ Date signed: 9/21/2010 Name: <input type="text"/> Title: Information Technology Specialist

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)):

~~Sensitive But Unclassified//For Official Use Only~~

~~Sensitive But Unclassified//For Official Use Only~~

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

~~Sensitive But Unclassified//For Official Use Only~~

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):

IntelPlus file rooms have been added to IDW and the privacy implications of using the information were assessed at that the time of ingest.

Applicable SORN(s): DOJ/FBI-002

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

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

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

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

Other:

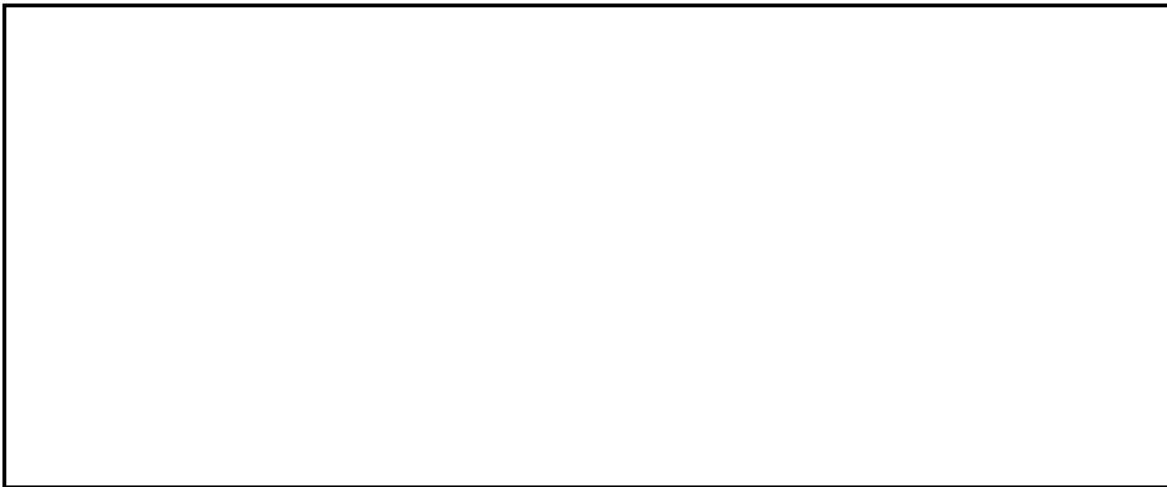
Elizabeth R. Withnell
Acting Deputy General Counsel
FBI Privacy and Civil Liberties Officer

Signature: /s/
Date Signed: 9/24/2010

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.

IntelPlus is a client/server Graphical User Interface (GUI) document management application accessible by authorized users in all FBI offices. It provides a complete set of full text searching capabilities and permits the electronic maintenance and retrieval of images of evidentiary materials in PDF and/or HTML format for ease of information sharing and use in connection with FBI mission activities.



b7E

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

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

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.

- X** The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.
- X** The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

If you marked any of the above, proceed to Question 3.

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

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

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 (in some cases)

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.

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: 05/02/2008

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: FY2010. Field Investigative
Systems Support**

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

NO

YES

If yes, please describe the data mining function:

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

NO

YES

13. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 1995

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

NO [If no, proceed to next question (II.3).] (Although new databases has been created in IntelPlus, there have been no significant changes to the structure of the system that would have an effect on privacy.

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

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

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

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

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

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

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

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

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

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

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

Other [**Provide brief explanation**]:

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

NO **YES**

If yes:

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

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

NO YES

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED]

b7E

BIKR FBI Unique Asset ID: SYS-0000174

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: SSA [REDACTED]	Name: AGC [REDACTED]
Reason:	Program Office: Internet Crime	Phone: [REDACTED]
Declassify On:	Complaint Center (IC3)	Room Number: 7350 JEH
	Division: Cyber	
	Phone: [REDACTED]	
	Room Number:	

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: Cyber	Signature: [REDACTED] Date signed: 01-22-2014 Name: [REDACTED] Title: Unit Chief, IC3	Signature: [REDACTED] Date signed: 1-21-14 Name: [REDACTED] Title: Supervisory Special Agent, CyD

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~~

FBI PIA: [redacted]

b7E

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 reductions)? 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): Some of the information contained in [redacted] is also contained in the FBI Central Records System, Justice/FBI-002. Because [redacted] also contains information that does not reside in the CRS, a separate SORN is being prepared for [redacted]

b7E

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): See above.

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

PCLU is working with Cyber Division and IC3 to ensure that an appropriate (e)(3) notice is added to the electronic complaint portal on the IC3 public website.

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: 2/3/12
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: [redacted] Date Signed: 2/4/12

b6
b7C

FBI PTA: [REDACTED]

b7E

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Internet Crime Complaint Center (IC3), established in 2000, is a partnership between the FBI and the non-profit National White Collar Crime Center (NW3C) to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of Internet crime.¹ Such crimes may include violations of intellectual property rights, computer intrusions, economic espionage, online extortion and international money laundering, in addition to identity theft. The IC3 provides individuals and businesses with a convenient online way to report cyber crime. The IC3 also serves as a central referral entity for complaints involving Internet-related crimes to federal, state and local law enforcement and regulatory agencies.

The [REDACTED] is an Internet-connected, secure but unclassified FBI network enclave supporting IC3. First deployed in January, 2006, the main component of [REDACTED] is a web-based Complaint Referral Form (CRF) [REDACTED] [REDACTED] also hosts several public websites, www.ic3.gov, and www.lookstoogoodtobetrue.com, a joint FBI/industry site focusing on public education about common Internet frauds.

b7E

Individuals wishing to file complaints with IC3 access the CRF through a portal on the www.ic3.gov website. While the complainant ultimately decides how much information to provide, data fields on the CRF include the complainant name, mailing address and telephone number and the name, address, telephone number and web address, if available, of the individual or business allegedly defrauding the complainant. The CRF also contains several text boxes in which specific details of the crime may be reported, including any monetary loss.

Before submitting a CRF, the complainant must first accept the terms and conditions displayed on the website, agreeing, inter alia, that the information provided "is correct to the best of my knowledge" and that "providing false information" could lead to "fine, imprisonment, or both." After submitting a report, the complainant receives, via e-mail, a unique complaint ID for the report and a random password. A complainant may then use the ID/password to access the complaint via the IC3 portal and provide supplemental information.

[REDACTED]

b7E

¹ The NW3C is funded by a grant from the Department of Justice's Bureau of Justice Assistance.

FBI PTA: [REDACTED]

[REDACTED]

b7E

Incoming complaints are acknowledged by e-mail; they are also assigned a password enabling the complainant to access and supplement the complaint, as appropriate. From the Proxy server, complaints are then forwarded [REDACTED]

[REDACTED]

Analysts at IC3 review incoming complaints [REDACTED]

b7E

[REDACTED]

[REDACTED] IC3 then determines whether a complaint, either standing alone or in conjunction with other complaints, warrants possible FBI investigation based on factors such as the total number of complaints against the same subject or entity, the total number of victims and the total monetary loss. If the complaint warrants further investigation, an IC3 Referral report (IC3R) [REDACTED]

[REDACTED] is prepared and sent to the appropriate Field Office for follow-up. If the Field Office opens an assessment or investigation, IC3 is available to provide additional support, such as research of open and commercial data sources. In the event that a complaint does not warrant investigation by the FBI, IC3 refers the complaint to appropriate state or local law enforcement agencies.

As the FBI's partner in IC3, NW3C automatically receives copies of incoming complaints [REDACTED] The NW3C membership consists of state and local law enforcement (LE) agencies and prosecutorial and regulatory agencies investigating economic and cyber crimes. [REDACTED]

b7E

[REDACTED]

[REDACTED]

b7E

FBI PTA

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.

 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?

b7E