

FBI FTA:

b7E

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

PLA required: No Yes: SORN/SORN revision required: No Yes:

Applicable SORN(s):

Notify FBI RMD/RIDS per MIOG 190.2.3: No Yes

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

The program should consult with RMD to identify/resolve any Federal records/electronic records issues.

Other:

David C. Larson, Deputy General Counsel
FBI Privacy and Civil Liberties Officer

Signature:

Date Signed:


8/10/05

FBI PTA: [redacted] b7E

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

[redacted]

[redacted] The system is open access for anyone with access to the FBI Net intranet. Users must provide their name, phone number and FBI Net email address. Only the email address is ever seen again. It is only seen by administrators that can look at reports of usage in the system. The names and phone numbers could be accessed by administrators. [redacted]

b7E

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

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

While there may be information about individuals in identifiable form [redacted] [redacted] If any PII appears in a document that is useful [redacted] an analyst or agent will [redacted] and will upload the relevant information into a case file.

b7E

YES. [If yes, please continue.]

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

NO. YES.

As noted above, the only personally identifiable information that is collected consists of user information. Within the FBI, all user information pertains to FBI personnel, contractors or consultants.

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

NO. YES.

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

NO. YES. If yes, check all that apply:

FBI PTA:

b7E

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

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

_____ SSNs are important for other reasons. Describe:

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

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

Explain:

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

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

_____ YES.

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

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

_____ NO.

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

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

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

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

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

YES. If yes, provide date of last C&A certification/re-certification: 9/12/2007

_____ Don't Know.

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

FBI PTA: [redacted]

b7E

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

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

X NO. _____ YES. _____ Don't know.

10. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

[redacted] It completed C&A [redacted] June 2004.

b7E

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

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

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

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

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

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

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

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

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

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

FBI PTA:

b7E

- _____ A change that results in a new use or disclosure of information in identifiable form.
- _____ A change that results in new items of information in identifiable form being added into the system/project.
- _____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.
- _____ Other. [Provide brief explanation]:

3. Does a PIA for this system/project already exist? NO. YES. If yes:

a. Provide date/title of the PIA:

b. Has the system/project undergone any significant changes since the PIA? NO. YES.

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Enterprise Management System (EMS) [redacted]
[redacted]

b7E

BIKR FBI Unique Asset ID: 2010-017-01-P-404-139-9999

Derived From:	SYSTEM/PROJECT POC Name: [redacted] Program Office: ITPMS/APU Division: ITMD Phone: [redacted] Room Number: CC-4, WS-99	FBI OGC/PCLU POC
Classified By:		Name: [redacted]
Reason:		Phone: [redacted]
Declassify On:		Room Number: 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [redacted] Date signed: [redacted] 12-18-13 Name: [redacted] Title: APU Unit Chief [redacted]	Signature: [redacted] Date signed: [redacted] 12-15-13 Name: [redacted] Title: IT Specialist
FBIHQ Division:	Signature: [redacted] Date signed: [redacted] 12-22-13 Name: [redacted] Title: ISMEU Unit Chief	Signature: [redacted] Date signed: [redacted] 12/31/2013 Name: [redacted] Title: IT Security Program Lead

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):

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:

Unit Chief
Privacy and Civil Liberties Unit
FBI Privacy and Civil Liberties Officer

Signature:
Date Signed: 01/06/2013

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

1. Provide a general description of the system or project that includes:

(a) name of the system/project, including associated acronyms;

The Enterprise Management System (EMS) Project implements tools that enable the Information and Technology Branch (ITB) to improve IT services management. The suite of tools enable ITB to better manage, monitor, measure, and automate certain IT functions. This PTA covers the development of four EMS tools to include:

[Redacted]

- Operations Orchestration (OO)

b7E

[Redacted]

- Universal Configuration Management Database (uCMDB)

[Redacted]

b7E

(b) purpose of the system/project;

[Redacted]

b7E

(c) structure of the system/project, including interconnections with other projects or systems;

[Redacted]

b7E

(d) nature of the information in the system/project and how it will be used;

[Redacted]

b7E

(e) who will have access to the information in the system/project;

FBINet system administrators will access the [Redacted] b7E

(f) and the manner of transmission to all users.

[Redacted] users will access the application through a secured web browser. b7E

Operations Orchestration (OO):

(b) purpose of the system/project;

OO enables the automation of common IT operational tasks, such as manually configuring a network router setting. The automated procedures (called Opsflows or flows) are made available to IT personnel through the OO application.

(c) structure of the system/project, including interconnections with other projects or systems;

Operations Orchestration (OO) contains the following [Redacted] that will run on the FBINet enclave: b7E

[Redacted]

b7E

OO will connect with Network Automation.

(d) nature of the information in the system/project and how it will be used;

OO stores details about operation flows or scripts that are used to automate specified tasks. It stores details regarding running configured scripts and the results of those script activities on network devices (i.e. switch, router, load balancer).

(e) who will have access to the information in the system/project;

FBINet system administrators will access the OO application.

(f) and the manner of transmission to all users.

OO users will access the application through a secured web browser.

[Redacted]

b7E

(b) purpose of the system/project;

[Redacted]

b7E

(c) structure of the system/project, including interconnections with other projects or systems;

[Redacted]

b7E

(d) nature of the information in the system/project and how it will be used;

[Redacted]

b7E

(e) who will have access to the information in the system/project;

ITMD project managers, project team members, and system administrators will access the [Redacted]

b7E

(f) and the manner of transmission to all users.

[Redacted] users will access the application through a secured web browser. b7E

Universal Configuration Management Database (uCMDB)

(b) purpose of the system/project;

The Universal Configuration Management Database (uCMDB) is a configuration management database that discovers information about the configuration assets. Configuration assets or items include IT inventory items such as servers, network devices (routers, switches, etc.) that exist in the network that uCMDB is configured to collect. It allows configuration managers a reference source to track the assets they are responsible

for and monitor any changes to those assets. uCMDB will be installed for test in the FBINet environment.

(c) structure of the system/project, including interconnections with other projects or systems;

The uCMDB system consists of a

[Redacted]

[Redacted]

b7E

[Redacted]

b7E

[Redacted]

b7E

(d) nature of the information in the system/project and how it will be used;

The database will store information about data center hardware so that the administrators of data centers can better manage inventory and changes in the environment. uCMDB



b7E

(e) who will have access to the information in the system/project;

Enclave system administrators will access the uCMDB application.

(f) and the manner of transmission to all users.

uCMDB users will access the application through a secured web browser.

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

____ NO

YES [If yes, please continue.]

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

(Check all that apply.)

____ The information directly identifies specific individuals.

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

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

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

None of the above. If none of the above, describe why the information does not identify specific individuals either directly or indirectly. **The only PII being stored in the system are the user logins.**

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

____ NO ____ YES

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

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

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

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

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

_____ YES

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

_____ NO

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

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

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

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

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

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

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

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

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

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

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

8. Is the system operated by a contractor?

_____ No.

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

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

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

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

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

Confidentiality: __Low__Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

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

10. 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?

_____ NO _____ YES

If yes:

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

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

___ NO ___ YES

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED] (ITSD) b7E

BIKR FBI Unique Asset ID: Pending

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [REDACTED] Program Office: Platform Support Unit Division: IT Services Division (ITSD) Phone: [REDACTED] Room Number: GP-703	FBI OGC/PCLU POC Name: AGC [REDACTED] Phone: [REDACTED] Room Number: 7350 JEH
--	---	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title: [REDACTED]	Signature: Date signed: Name: Title: [REDACTED]
FBIHQ Division: Information Technology Services Division	Signature: [REDACTED] Date signed: 12/19/11 Name: [REDACTED] Title: Unit Chief, Platform Support Unit	Signature: [REDACTED] Date signed: 12-14-11 Name: [REDACTED] Title: IT Specialist, IT Branch

b6
b7C

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 (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): N/A

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

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

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

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

Other:

<input type="checkbox"/> Unit Chief Privacy and Civil Liberties Unit	Signature: <input type="checkbox"/> Date Signed: 12/21/11
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 12/22/11

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.

ITSD's Platform Support Unit (PSU) manages the enterprise database, email, and virtualization infrastructure for the systems and applications operated and maintained by ITSD. Personnel use the [redacted] sometimes referred to as [redacted] to [redacted]

b7E

[redacted] through the Secret Enclave infrastructure. [redacted] of the database *itself* rather than the raw information contained *in* the database. [redacted]

b7E

[redacted] does not include information about any individual using the database.

When PSU [redacted] its personnel access [redacted] [redacted] Personnel use that information to [redacted] rather than the database, PSU provides the relevant information to the administrators of [redacted] [redacted]

b7E

Access to [redacted] is limited to personnel assigned to PSU designated as administrators [redacted]

b7E

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

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

YES [If yes, please continue.]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT:

b7E

BIKR FBI Unique Asset ID: _____

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: <input type="text"/>	Name: <input type="text"/>
Reason:	Program Office: ITMS	Phone: <input type="text"/>
Declassify On:	Division: CJIS	Room Number: C3, 655
	Phone: <input type="text"/>	<input type="text"/>
	Room Number: Mod. B2 (13-N-B2)	

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] CJIS	Signature: <input type="text"/> Date signed: 9/11/2010 Name: <input type="text"/> Title: Supervisory IT Specialist	Signature: <input type="text"/> Date signed: 9/17/2010 Name: <input type="text"/> Title: Supervisory Security Specialist
FBIHQ Division: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

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

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

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

1- DOJ Office of Privacy and Civil Liberties (via e-mail to privacy@usdoj.gov; if classified, via hand delivery to 1331 Penn. Ave. NW, Suite 940, 20530) 1 - OGC/PCLU intranet

2- FBI OCIO / OIPP ()

1- FBI SecD/AU (UC)

1- RMD/RMAU ()

1- Program Division POC

1- Division Privacy Officer

b6
b7C

[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.]

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):

*System is infrastructure
(+ huge)*

Applicable SORN(s): _____

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

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

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

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

Other:

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

Signature:
Date Signed:

Elizabeth R. Withnell
9/24/10

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

[REDACTED] system provides a centralized storage resource that supports all FBI [REDACTED]

[REDACTED] is managed as a single entity providing a common infrastructure of storage. This storage can be partitioned to support the short and/or long-term needs of each of the supported systems. [REDACTED] is comprised of the

b7E

[REDACTED]

[REDACTED]

b7E

[REDACTED]

b7E

[REDACTED]

b7E

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

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

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

YES [If yes, please continue.]

Although "maintains" information about individuals, only provides storage and backup/recovery services for other Systems that have their own privacy documentation. does not have direct access to the data and does not modify the data in any way. The data is owned by other Systems or Programs that are ultimately responsible to collect, maintain or disseminate any information about individuals.

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.)

- The information directly identifies specific individuals. *but see above request.*
- The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals, but not in this system. *System is infrastructure.*
- The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals), but not in this system.

But please see explanation in 2. above.

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.]

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

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

Information may identify U.S. citizens, but the purpose of the system is not to do so.

But please see explanation in 2. above; the information is retrieved only as back-up storage for other Systems.

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:

However, Social Security numbers are merely maintained as storage/back-up for other Systems; please see explanation in 2. above.

b7E

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:

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

_____ 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:

Last C&A: June 2009

Confidentiality: ___Low___Moderate High ___Undefined

Integrity: ___Low___Moderate High ___Undefined

Availability: ___Low___Moderate High ___Undefined

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

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

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

NO

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

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

NO

YES If yes, please describe the data mining function:

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

NO

YES

13. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? **March 2006**

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

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

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.

Explanation: The recent changes to [redacted] have been in the form of hardware upgrades. Newer model [redacted] have been installed, and older [redacted] are being removed. There were no changes in services, processes, or data.

b7E

_____ Other [Provide brief explanation]:

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

NO _____ YES

If yes:

a. Provide date/title of the PIA:

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

_____ NO _____ YES

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

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

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

Total Deleted Page(s) = 1
Page 4 ~ b7E;

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

Unclassified/For Official Use Only

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

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

NAME OF SYSTEM / PROJECT: Financial Management System (FMS)

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [redacted]	Name: [redacted]
	Program Office: Information Technology Operations Division Division: Financial Systems Unit Phone: [redacted]	Phone: [redacted] Room Number: 7458
	Room Number: FBIHQ RM 1302	

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: Financial Systems Unit (FSU)	Signature: [redacted] Date signed: 7/22/09 Name: [redacted] Title: IT Specialist	Signature: [redacted] Date signed: 9/29/09 Name: [redacted] Title: SC, Div Privacy Officer
FBIHQ Division: [insert division name]	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7458).
(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

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

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

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

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

b6
b7C

FBI PTA: Financial Management System (FMS)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

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

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

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

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

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

Information in the system relates to internal government operations.

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

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

____ Other (describe):

Applicable SORN(s): CRS, JUSTICE/FBI-002; DOJ Payroll System, JUSTICE/JMD-003

Notify FBI RMD/RIDS per MIOG 190.2.3? ____ No ____ Yes (see sample EC on PCLU intranet website).

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:

David C. Larson, Deputy General Counsel
FBI Privacy and Civil Liberties Officer

Signature:
Date Signed:

FBI PTA: Financial Management System (FMS)

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Financial Management System (FMS) is a major application system, developed in 1983, which supports the management of the FBI business and personnel financial records and performs a variety of clearly defined functions for which there are readily identifiable security considerations and needs. For example, [REDACTED]

b7E

Primary users of the FMS are the Finance Division, FBIHQ Travel Coordinators and Budget Offices, Field Office Draft Personnel, Commercial Payments and Confidential Services Unit, and Supply Technicians. Members of the Financial Systems Unit that perform Operations, Maintenance, and Customer Service to users have access to FMS.

Access to FMS is granted on a "need to know" basis utilizing the [REDACTED]

b7E

Internally, the FMS interfaces with the payroll system, the Property Management Application, the Commercial Payments Unit Invoice Management System (CPUIMS), and the Budget Formulation Application.

b7E

FBI PTA: Financial Management System (FMS)

[Redacted box]

b7E

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

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

______ YES. (If yes, please continue.)

The data contained within Financial Management System (FMS) includes sensitive personnel and financial information. FMS is considered a mission critical system and is one of many major applications that operate on the FBI general support system, FBI Enterprise Server (commonly known as the Administrative Mainframe).

[Redacted box] Data is classified according to Executive Order 12356

b7E

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

_____ NO. ______ YES.

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

_____ NO. ______ YES.

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

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

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

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

_____ SSNs are important for other reasons. Describe:

[Redacted box]

b7E

FBI PTA: Financial Management System (FMS)

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

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

Explain:

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

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

__________ YES.

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

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

__________ NO.

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

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

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

Employee and contract personnel must sign an FD-857 (Sensitive Information Non-Disclosure Agreement). Bureau employees complete a GSA Smart Pay - MasterCard IBA Cardholder form and the SF-1012 Travel Voucher

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

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

__________ YES. **If yes, provide date of last C&A certification/re-certification:** 11/13/2007

_____ Don't Know.

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

_____ NO.

_____ Don't know.

__________ YES. **If yes, please provide the date and name or title of the OMB submission:** FBI Administrative Systems Support, April 30, 2009

FBI PTA: Financial Management System (FMS)

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

NO. YES. Don't know.

10. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 1983

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

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

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

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

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

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

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

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

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

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

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

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

Unclassified/For Official Use Only

FBI PTA: Financial Management System (FMS)

_____ 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:** Grandfathered system as of April 17, 2003; PTA exists, dated 6/15/2006, FMS (Financial Management System).

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

NO. ___ YES ___ N/A

[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 .]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: FBI Access to Federal Trade Commission Consumer Sentinel Database (CSDB)

BIKR FBI Unique Asset ID: N/A

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: CS [REDACTED] Program Office: Financial Intelligence Center (FIC) Division: Criminal Investigative Division (CID) Phone: [REDACTED] Room Number: 3475 JEH	FBI OGC/PCLU POC Name: AGC [REDACTED] Phone: [REDACTED] Room Number: 7350 JEH
--	--	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title: [REDACTED]	Signature: Date signed: Name: Title: [REDACTED]
FBIHQ Division: Criminal Investigative Division (CID)	Signature: [REDACTED] Date signed: 5-16-11 Name: [REDACTED] Title: Unit Chief, CID/Financial Intelligence Center (FIC)	Signature: [REDACTED] Date signed: 5-17-11 Name: [REDACTED] Title: Supervisory Special Agent, CID

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 (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:

The FBI is obtaining direct electronic access to complaints of consumer fraud and identity theft contained in the Federal Trade Commission's (FTC) Consumer Sentinel database (CSDB) for authorized law enforcement and intelligence purposes. The CSDB will be queried for relevant information, including personally identifiable information (PII), by FBI personnel who have been granted access privileges by the FTC. FBI access to the CSDB will be governed by a Memorandum of Agreement (MOA) between the FBI and the FTC.

No PIA is necessary because any information downloaded or printed by the FBI from the CSDB is being transferred directly from an FTC System of Records to the FBI Central Records System (CRS), and the sharing of information is encompassed by published System of Records Notices (SORNs) for both systems.

Applicable SORN(s): FBI Central Records System, Justice/FBI-002; Federal Trade Commission Consumer Information System, FTC-IV-1

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

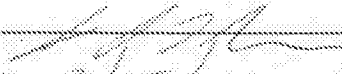
SORN/SORN revision(s) required? No ___ Yes (indicate revisions needed):

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:

James J. Landon, Deputy General Counsel and
FBI Privacy and Civil Liberties Officer

Signature: 
Date Signed: 3/25/11

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 has entered into a Memorandum of Agreement (MOA) with the Federal Trade Commission (FTC) to obtain access to information contained in the FTC's Consumer Sentinel database (CSDB). The CSDB is a secure online database that serves as a repository for complaints of identity theft or deceptive business practices filed by individuals with various entities, including the FTC, the FBI's Internet Crime Complaint Center (IC3), the U.S. Postal Inspection Service and the Better Business Bureau.

The CSDB contains personally identifiable information (PII) of individuals filing complaints, as well as about individuals who are the subject of complaints. The PII includes information such as name, address, telephone number, date of birth, Social Security Number, credit card numbers and e-mail address, extracted or summarized from an individual's complaint. The CSDB also contains POC information for the agency receiving the complaint.

The CSDB is encompassed by a published System of Records Notice (SORN), FTC-IV-1, *Consumer Information System*, available on the FTC website. Pursuant to a published routine use also available on the FTC website, the FTC may share information from any of its Systems of Records with "another agency ... under the control of the United States for a civil or criminal law enforcement activity."¹

The information in the CSDB pertaining to financial fraud, money laundering and identity theft is relevant to the investigative and/or intelligence responsibilities of the FBI's Criminal Investigative Division (CID) and squads within FBI Field Offices investigating white collar crime. Under this project, FBI personnel with a demonstrated need-to-know will be authorized to electronically access the CSDB from secure FBI workstations. The FTC will provide those individuals with "hard tokens" permitting electronic access. The CSDB will be queried for complaints suggesting egregious conduct (for example, multiple complaints against a single entity or individual; complaints alleging the loss of a significant amount of money; complaints against individuals who are already the subject of existing FBI investigations). All FBI queries of the CSDB will be made as part of one or more open assessments, as authorized by the Attorney General Guidelines for Domestic FBI Operations (AGG-DOM) and the FBI's Domestic Investigations Operations Guide (the DIOG).

¹ The FTC and the FBI both agree that the term "law enforcement activity" encompasses authorized FBI intelligence activities.

[Redacted]

b7E

Information from the CSDB may also be printed or downloaded from FBI workstations. Any information printed or downloaded from the CSDB will be included in FBI investigative or intelligence files. The information will also be further analyzed to corroborate the underlying complaint(s) as well as to obtain additional information supporting additional investigative or intelligence activity.

[Redacted]

b7E

Pursuant to the MOA between the FBI and the FTC, any information that has been printed, downloaded or otherwise removed from the CSDB must be deleted or destroyed within ninety (90) days unless it is still required for law enforcement purposes (including authorized intelligence activities, see footnote 1).

This project involves electronic access to an FTC System of Records, the Consumer Information System and the subsequent transfer of relevant information to an FBI System of Records, the Central Records System. The information is not stored or maintained outside of these systems. Both systems have published System of Records Notices (SORNs) and the use of the information is authorized by one or more published routine uses for each system.

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.

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

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

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

NO YES

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

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

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

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

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

YES

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

_____ NO

YES [If yes, proceed to question 7.]

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

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

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

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

_____ 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)?

Information acquired from the CSDB will be maintained by the FBI in one or more applications residing on the FBI's Secret Enclave. Secret Enclave has Authority to Operate (ATO) through March 14, 2011 and is presently undergoing re-certification.

Secret Enclave's risk levels will remain unchanged and are as follows:

Confidentiality: ___Low___Moderate High ___Undefined

Integrity: ___Low___Moderate High ___Undefined

Availability: ___Low___Moderate High ___Undefined

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

NO

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

11. Does the system/project 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

Queries of the CSDB are not intended or designed to identify a predictive pattern of criminal or terrorist activity. Individuals identified in the CSDB are already either the complainant, victim, or subject of one or more existing consumer complaints or a POC at an agency receiving such a complaint.

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

NO

YES

13. Status of System/Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

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

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

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

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

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

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

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

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

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

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

_____ Other [Provide brief explanation]:

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

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

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

_____ NO _____ YES

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

[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.]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: One Way Transfer Systems **b7E**
BIKR FBI Unique Asset ID:

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: Program Office: Division: CTD Phone: Room Number: 415A	FBI OGC/PCLU POC Name: Phone: Room Number: FTTTF-629
--	--	---

b6
b7C
b7E

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: Counterterrorism	Signature: <i>John A. Boyle</i> Date signed: <i>8/21/2011</i> Name: John A. Boyle Title: Section Chief	Signature: Date signed: Name: Title: Division Privacy Officer

b6
b7C

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

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [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): *Infrastructure*

Applicable SORN(s): *N/A*

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

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

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

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

Other:

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

b6
b7c

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

Provide a general description of the system or project that includes:

(a) Name of the system/project, including associated acronyms;

[redacted] uses multiple One Way Transfer (OWT) Controlled Interfaces (CI) to transfer large amounts of data from lower classification networks to higher classification networks. An OWT is a mechanism that facilitates adjudicating the security policies of different connected Information Systems to control the flow of information from a low security enclave to a higher security enclave. Three OWT systems are encompassed by this PTA:

b7E

1. The first is between the [redacted] and the [redacted]. It is used to test any required systems changes to the OWT CI before they are implemented within the production networks.

b7E

2. The second is between the [redacted] and the [redacted].

2. The third is between the [redacted] and the [redacted].

(b) Structure of the system/project, including interconnections with other projects or systems;

System Name	Classification & Compartments	Accredited By
[redacted]	[redacted]	FBI
[redacted]	[redacted]	FBI
[redacted]	[redacted]	FBI
[redacted]	[redacted]	FBI

b7E

[Redacted]

FBI

b7E

(c) Purpose of the system/project;

The system provides a secure mechanism to control the transfer of large amounts of data between the lower security enclave and the higher security enclave, while maintaining the security policies and protections of each separate enclave.

(d) Nature of the information in the system/project and how it will be used;

The first OWT described above is used ^{to} test required configuration changes to the OWT system before implementing those changes on the production OWT systems. The second OWT system is used to transfer large amounts of data [Redacted]

[Redacted]

b7E

The third OWT described above is used to transfer large amounts [Redacted]

[Redacted]

(e) Who will have access to the information in the system/project;

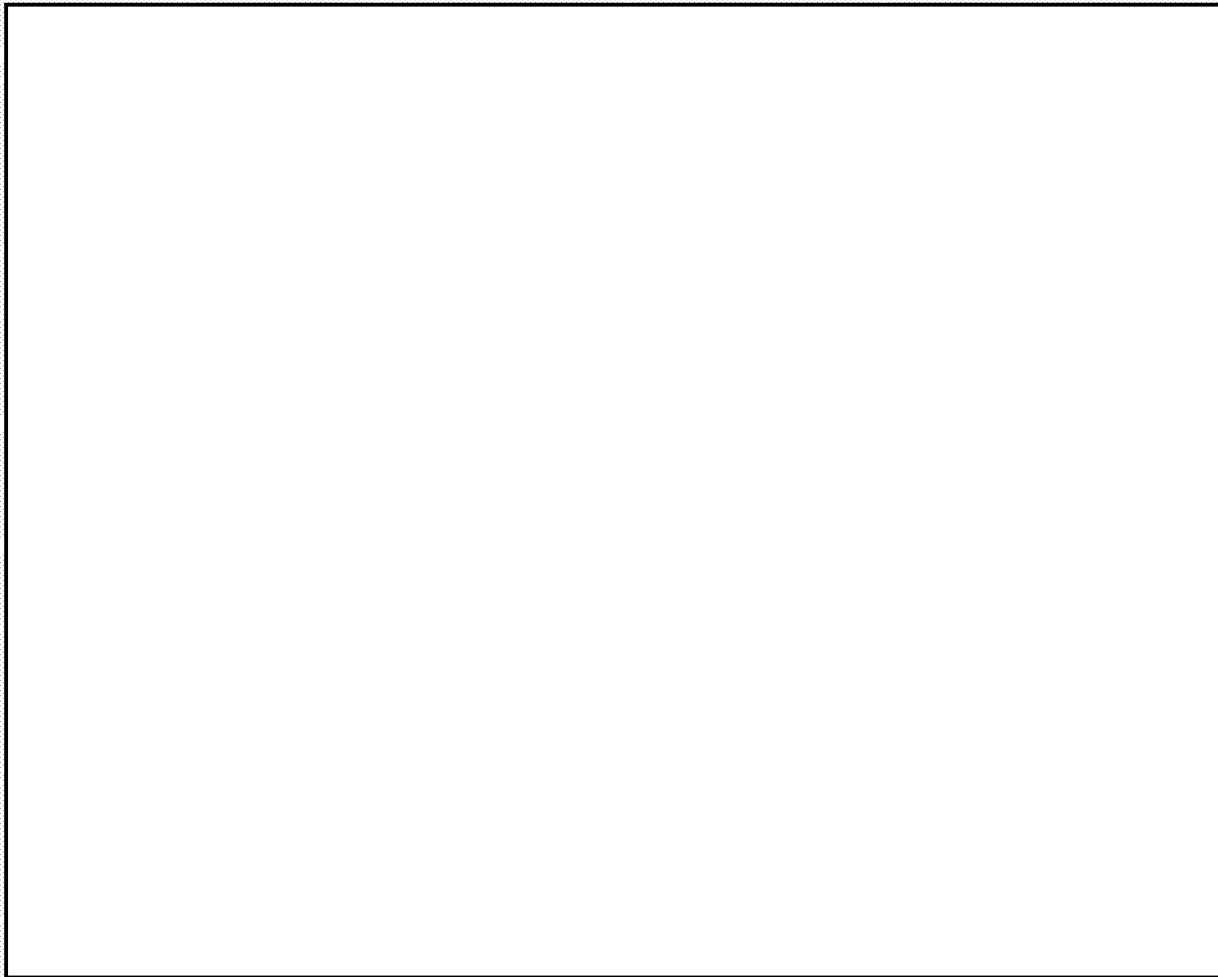
The [Redacted] Administration Team and the Infrastructure Support Team System Administrators are the only groups with access to the [Redacted] OWT Systems.

b7E

(f) Manner of transmission to all users.

[Redacted]

b7E



b7E

[redacted] QWT Systems uses [redacted]
[redacted] to transfer data from the lower security classification network up to the higher security classification network, while maintaining the security parameters of both the higher and lower classified networks. The data flow is uni-directional from the SEND server to the RECEIVE server. [redacted]

b7E

[redacted] is designed to allow only outbound traffic, enforcing the uni-directional flow of information and security parameters of the two networks.

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.]

While the underlying data that is transferred may contain PII, the one-way transfer itself is part of the infrastructure of [redacted]. The privacy implications of the data that is transferred are addressed in documentation for [redacted].

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