FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: Financial Disclosure Forms Analyzer (FDF-A)

____ PIA is required by the E-Government Act.

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

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

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

Applicable SORN(s): FBI-002

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

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

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

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: 3/11/2010

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.** A critical aspect of determining an individual's ability to receive or maintain a security clearance is that of financial status. For years, government agencies have required individuals with certain security classification levels to provide detailed information regarding their financial situations. Financial disclosure and analysis has historically been a lengthy, tedious, paper-based process. Current clearance holders must disclose their financial status annually to maintain their clearances. The Financial Disclosure Forms- Analyzer's (FDF-A) [redacted] to electronically collect, store and analyze over 20,000 FBI employees' financial information on an annual basis. Currently, there is no process for deleting information of former employees from the system. b7E

FDF-A's primary mission is to collect and analyze financial data, alert appropriate investigatory personnel when adverse conditions are met, identify those who fail to comply in a timely manner and store, archive and retrieve historical records. FDF-A is an online system that will allow specific Bureau personnel, with access to FBINet, to file their required financial disclosures, and allow Analysts to track and analyze these disclosures. FDF-A is also known as the Financial Disclosure Program (FDP). The primary users are Analysts in the Analysis and Investigations Unit (AIU) in the Internal Security Section (ISS) of the Security Division (SecD).

The FDF-A software application [redacted] The FDF-A is a web-based system wherein the filers complete the financial disclosure form through an interactive interview process with the FDF-A [redacted] b7E The FDF-A prompts the users through form completion and validates their input according to accepted data types by field. The information is then stored in [redacted] database as the filer's submission. The FDF-A's [redacted]

[redacted] b7E

The FDF-A application [redacted] b7E

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.]**

__X__ YES [If yes, please continue.]

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

_____ NO __X__ 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 __X__ YES

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

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

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

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

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

__X__ The system/project provides special protection to SSNs (e.g., SSNs are encrypted, hidden from all users via a look-up table, or only available to certain users). **Describe:** Only a few System Administrators have access to the data and each is required to file annually. An Information System Security Officer (ISSO) reviews audit logs on a monthly basis and reports any suspicious activity.

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

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

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

__X__ YES

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

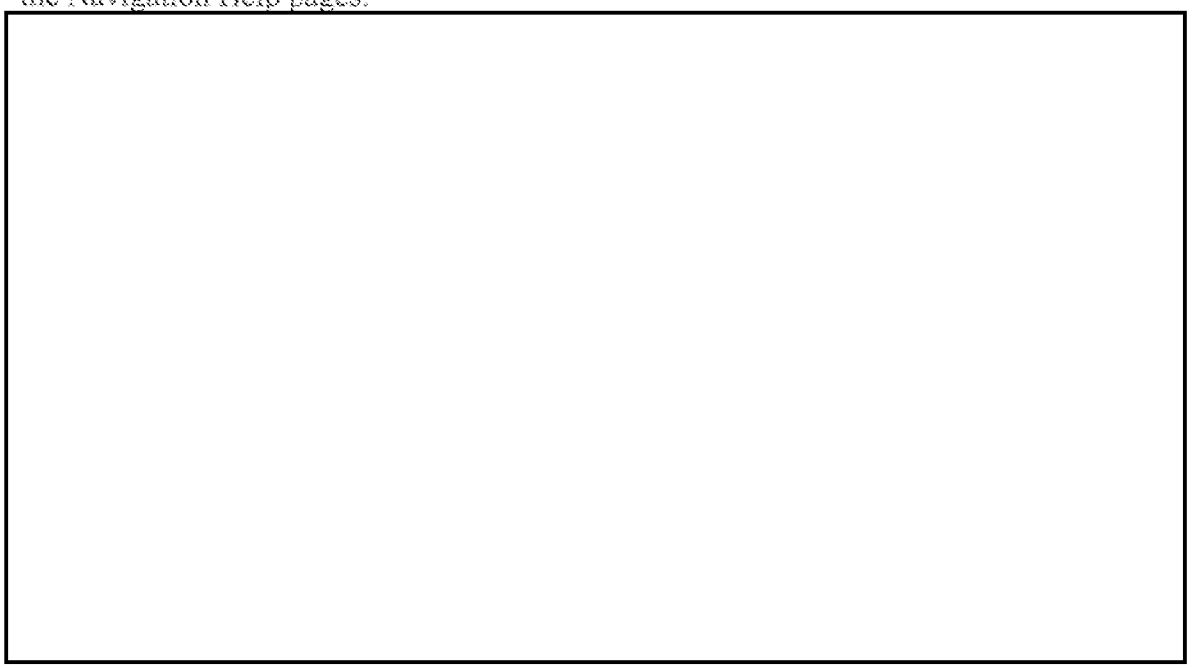
_____ YES [If yes, proceed to question 7.]

__X__ NO

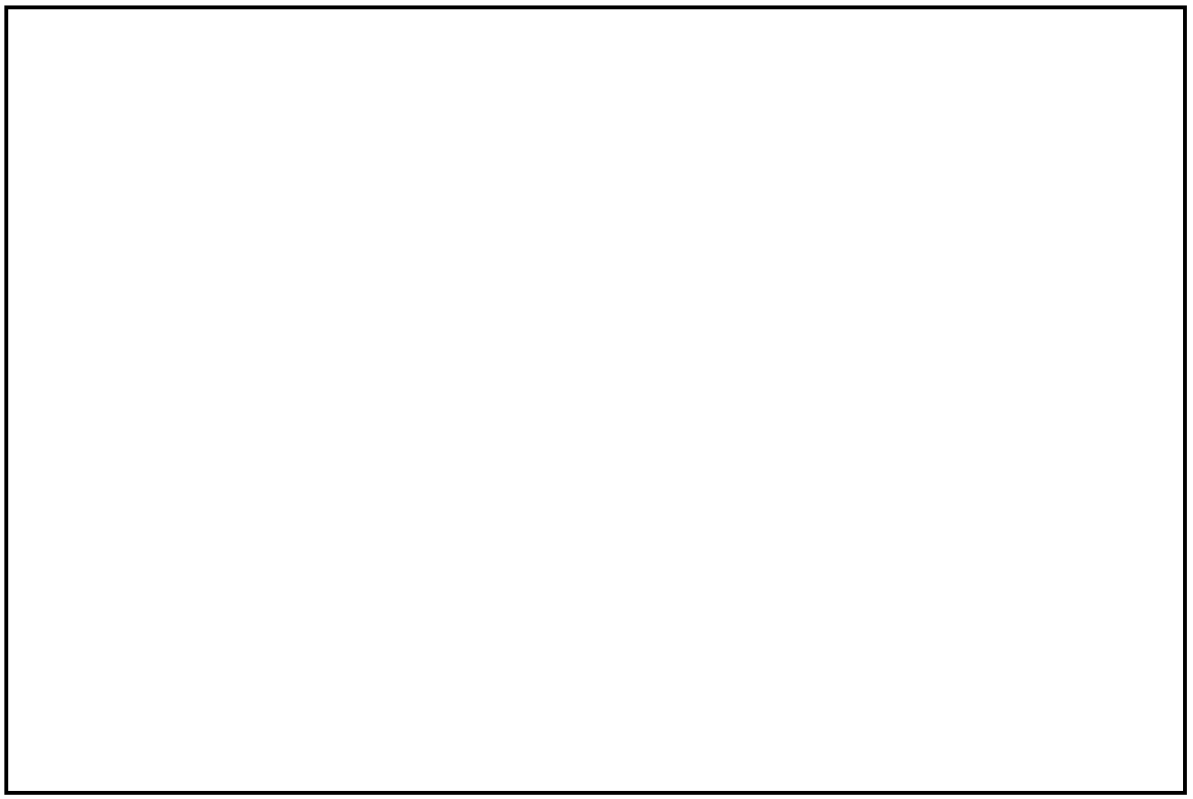
b. Are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)?

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

__X__ YES **Identify any forms, paper or electronic, used to request such information from the information subject:** The following is posted on the Navigation Help pages:



b7E



b7E

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

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

__X__ YES **If yes, provide date of last C&A certification/re-certification:** March 1, 2009 which expires on February 28, 2010. A new certification is underway and expected to be complete and signed off by March 12, 2010.

_____ Don't Know.

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

_____ NO _____ Don't know __X__ YES **If yes, please provide the date and name or title of the OMB submission:** Security Management Information System (SMIS)

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 PIA and/or other actions are required.]**

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 2003- 2005 manual submissions, 2006 – 2009 electronic submissions

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 boxes that apply)**:

__X__ A conversion from paper-based records to an electronic system. The conversion occurred prior to the 2006 PIA.

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

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

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

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

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

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

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

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

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

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

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

_____ NO __X__ YES

If yes:

a. **Provide date/title of the PIA:** 02/24/2006, PRIVACY IMPACT ASSESSMENT (PIA), SECURITY DIVISION IMPLEMENTATION OF THE FINANCIAL DISCLOSURE FORMS ANALYZER (FDF-A FINANCIAL FILER SYSTEM)

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

__X__ NO ___ YES

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

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

Total Deleted Page(s) = 2
Page 4 ~ b7E;
Page 6 ~ b7E;

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

(OGC/PCLU (Rev. 07/06/2010)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: [redacted] Name Check Program [redacted] b7E

BIKR FBI Unique Asset ID: 2010-020-01-P-113-215-9999

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Investigative Projects Unit Division: IT Management Division Phone: [redacted] Room Number: CC-4	**FBI OGC/PCLU POC** Name: [redacted] Phone: [redacted] Room Number: JEH 7350

b6 b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Records Management Division (RMD)	Signature: [redacted] Date signed: 6/11/11 Name: Michael A. Cannon Title: NNCP Section Chief	Signature: Date signed: Name: Title:
FBIHQ Division: Records Management Division (RMD)	Signature: [redacted] Date signed: 6/11/11 Name: Michelle A. Jupina Title: Assistant Director	Signature: [redacted] Date signed: 6/11/2011 Name: David M. Hardy Title: RIDS Section Chief

Additional division(s) approvals may be added as warranted:

FBIHQ Division: Records Management Division (RMD)	Signature: [redacted] Date signed: 5/17/11 Name: [redacted] Title: Division Operations Manager	
RMD Unit: BOSU	Signature: [redacted] Date signed: 5/16/11 Name: [redacted] Title: Unit Chief	
RMD Unit: NNCP	Signature: [redacted] Date signed: 5/16/11 Name: [redacted] Title: Assistant Section Chief	
RMD Unit: NNCP	Signature: [redacted] Date signed: 5/16/11 Name: [redacted] Title: Assistant Section Chief	

b6 b7C

After all division approvals, forward signed hard copy plus electronic copy to FBI OGC/PCLU (JEH 7350).

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

__X__ PIA is required by the E-Government Act. **In order to ensure that privacy requirements are built into the system, [redacted] is required to prepare a PIA upon completion of Final Design Review. b7E

_____ 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)? _X__ 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): A new sorn will be required.

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

SORN/SORN revision(s) required? ___No _X__Yes (indicate revisions needed): Once RMD determines what the system design will include, RMD should work with OGC/PCLU in drafting a new sorn.

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

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

Other:

[redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 6/8/11
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 6/8/11

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.

The National Name Check Program (NNCP), which operates in the Records Management Division (RMD) of the Federal Bureau of Investigation, processes name check requests for federal agencies, including the Department of Homeland Security's U.S. Citizenship and Immigrations Services (USCIS), the Office of Personnel Management (OPM), and the Department of State (DOS). Information obtained from the NNCP is used in adjudicating matters related to Government employment, federal appointment, security clearances, attendance at [redacted] functions, issuance of immigration benefits or a visa, and naturalization petitions. b7E

In order to provide information to meet customer needs, the NNCP conducts searches of the FBI's Central Records System (CRS), which includes records from FBI Headquarters, FBI Field Offices, and Legal Attaches. Records accessed from these locations contain FBI investigative, administrative, personnel, and general files. NNCP analysts review and analyze potentially identifiable documents to determine whether a specific individual has been the subject of, or is mentioned in, any FBI investigation. If any relevant information is discovered, it is disseminated to the requesting agency, subject to appropriate legal and operational restrictions. The requesting agency uses the information in its adjudication process.

[redacted] o include Name Check Program (NCP) and Name Check Dissemination Database (NCDD); [redacted] NNCP's business processes. b7E

[redacted] b7E

[redacted] b7E

[redacted] b7E

Transactional data, to include audit logs of activities performed, will be stored in the system. Transactional data includes copies of information used by the NNCP Research Analyst to process the request along with final copies of information sent to the requesting agency. Transactional data will be maintained according to established procedures and timeframes. Information used to process the request that is not ultimately sent to the requesting agency is purged at the close of the request. Information sent to the requesting agency is stored in the [redacted] in accordance with the applicable retention period for summary files of 7 years after the end of the calendar year in which a name check was completed. b7E

[redacted]

[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.]

_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?

___X_ NO _____ YES

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

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

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

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

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

* Aside from audit logs, the system does not directly collect information from individuals. However, individuals may provide PII to the requesting agency, and the requesting agency will provide that information to the FBI in order to initiate the name check. When applicable, the requesting agency is responsible for obtaining consent from the individual to share the information with the FBI to perform the check.

_____ YES

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

_____ NO

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

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

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

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

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

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

_____ 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.

___X__ SSNs are important for other reasons. **Describe:**
Currently, SSNs are initially submitted as part of a name check request, used as a search element by the FBI federated search tool, reviewed in the NNCP automated business processes, and included in the response submitted for the name check request. The Name Check Program has been advised by the Office of the General

Counsel of the privacy risks associated with returning the SSN as part of the result back to the customer. The Name Check Program will work with the Office of the General Counsel to determine alternatives to this process.

_____ 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: Yes,**

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

8. Is the system operated by a contractor?

_X_ No.

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

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

__X___ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date**: This system is in the Planning and Requirements phase of the FBI Life Cycle Management (LCM) process and will go through the C&A process. The estimated completion date is FY 2013/ FY2014.

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

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

Confidentiality:__Low__Moderate__High__Undefined

Integrity: __Low__Moderate__High__Undefined

Availability: __Low__Moderate__High__Undefined

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

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

__X__ NO (The National Name Check Program is a fee-for-service program; so an OMB-300 budget submission is not required.)

_____ 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:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

_____ NO _____ YES

If yes:

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

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

___ NO ___ YES

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: OCS 2007 R2 to Lync Server 2010 migration

BIKR FBI Unique Asset ID: _____

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Division: ITED Phone: [redacted] Room Number: LS401-3	**FBI OGC/PCLU POC** Name: Phone: Room Number:

b6
b7C

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

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:
FBIHQ Division: [redacted] (ITED) ITB\ITED\EES\PFU	Signature: [redacted] Date signed: 4/26/2011 Name: [redacted] Title: Unit Chief	Signature: [redacted] Date signed: 4-27-11 Name: [redacted] Title: ELS

b6
b7C

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

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

_____ PIA is required by the E-Government Act.

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

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

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

Applicable SORN(s): _____

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

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

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

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

Other:

James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 5/9/11

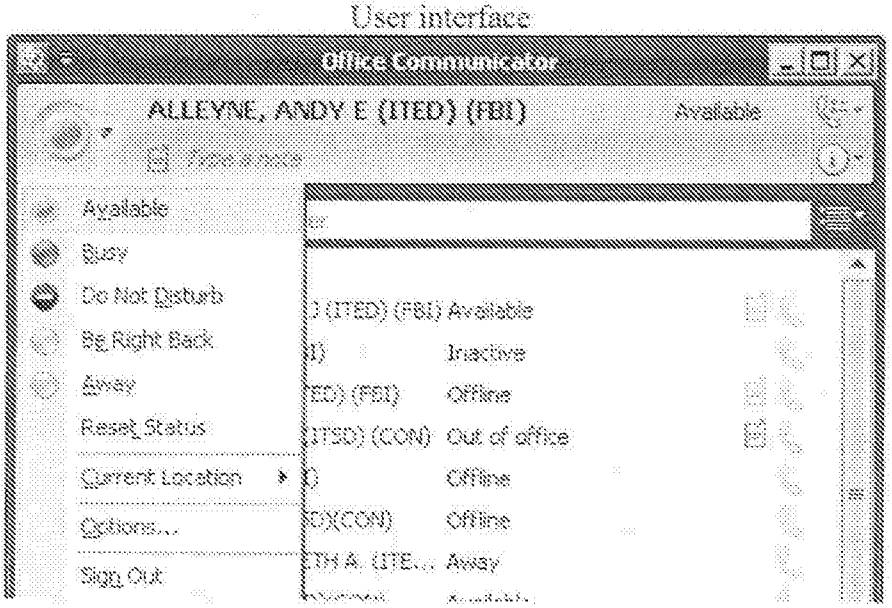
I. INFORMATION ABOUT THE SYSTEM / PROJECT

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.

Currently on the Secret Enclave Office Communicator Server 2007 R2 (OCS) provides presence, Instant messaging and limited Video conferencing to all FBI employees with Next Generation Workstations (NGW). These features are incorporated into all Microsoft Suite products to include Microsoft Office Suite (Word, Excel, etc.) and SharePoint's MySites. Below is a picture of the OCS icon and the basic user interface which can be found on all NGW machines.

Icon

User interface



To expand on the benefits provided by OCS, The Office Communicator Server 2007 R2 (OCS) to Lync Server 2010 (Lync) migration effort (hereinafter OCS to Lync Migration) is being undertaken. OCS to Lync Migration will provide video conferencing, instant messaging, voice over IP abilities, presence in the office, which will allow users the opportunity to make their presence known with a simple color-based system within various Microsoft office suites. Some of the benefits of the OCS to Lync migration are as follows: cost effective video conferences between Field and HQ components; instant communication between any FBI employee with access to the Secret Enclave; the ability to tell at a glance if a contact is Available, Busy, or Away. While the presence feature

cannot be disabled, it can be limited by manually changing to a static value of Away, Be Right Back, Do Not Disturb or Busy. Training and product details for OCS and in turn Lync can be found on the intranet by doing a search for "Office Communicator" or clicking on the following link [redacted] Training.

The OCS to Lync Migration uses a Commercial Off the Shelf (COTs) product that is publicly available, but the system is being deployed on the Secret Enclave and will be treated accordingly. The client software will be deployed using the Enclave's current deployment method [redacted] Platform Engineering Unit (PEU). Before the system is deployed in production, it will be deployed into the Operations Test and Evaluation Facility (OTEF) for production testing, security scans and performance validation. Once all the appropriate approvals have been obtained, the system will be deployed to production. When the system is fully deployed and operational, all employees with access to the Secret Enclave will have access to presence information, instant messages, Voice Over IP (VoIP), and video conferencing directly from any desktop with access to the enclave. b7E

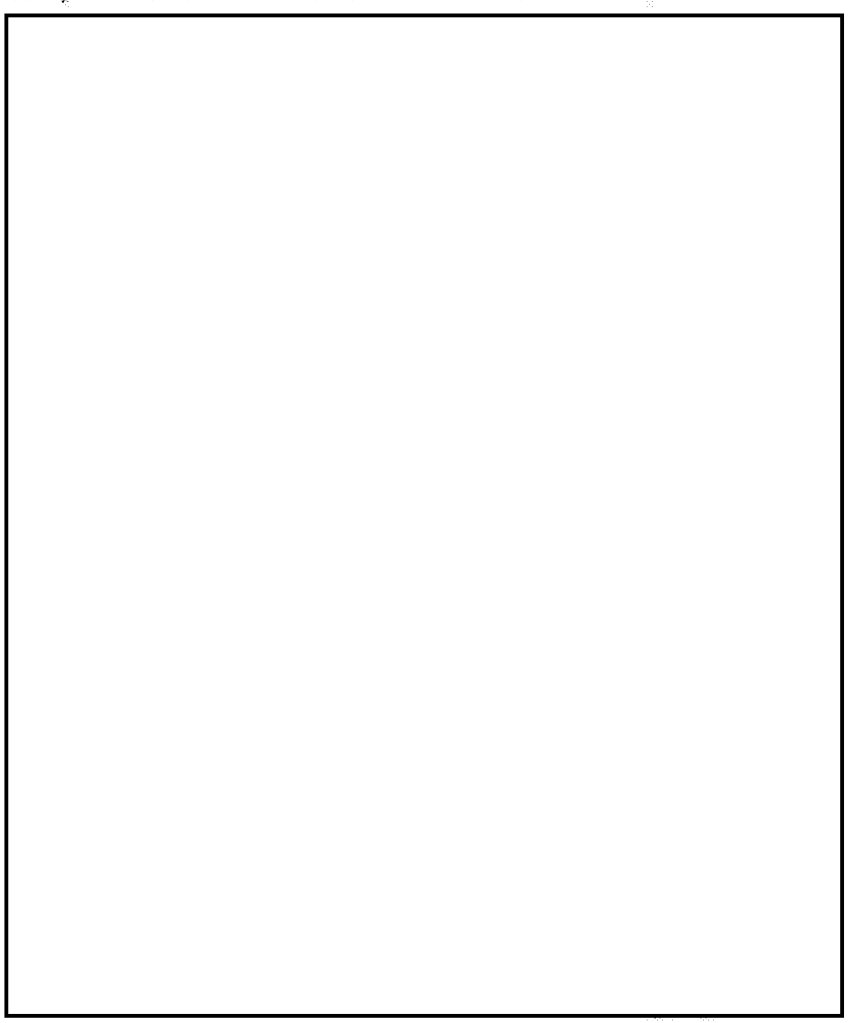
The following Table is a comprehensive list of protocol's and ports used for intranet communications by Lync Server 2010 to facilitate communications between clients, servers and command and control system components.

SYSTEM FUNCTION	[redacted]
Instant Messaging (IM) and Presence	
Voice communication	
Application and desktop sharing	
Web/AV conferencing	
Central management	

b7E

Below is a simplistic view of the data flow within Lync. Data is pushed or pulled between various clients and not saved in any central location within the system. Data that is "pushed" between clients are broadcast to all clients listening, while data that is "pulled" require a client to ask another client to give information about itself. For example, presence information is broadcast (pushed) from client to client in real time. However, to start an instant message conversation between clients, the initiator must contact Active Directory for the Service (SRV) record and an "A host" record of the target machine and frontend server. Once this information is gathered the connection is made to the target client and the conversation can begin. All instant messages between clients from that point forward are pushed back and forth.

This system does not collect, maintain, or disseminate Personally Identifiable Information (PII), but rather provides a control mechanism for VOIP, IM and AV to travel between Lync system components and infrastructure components within the Secret Enclave. For example, information about presence is gathered in real time and is not stored but rather pushed out to clients in a controlled interval in real time.



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)?

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

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

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

_____ The information directly identifies specific individuals.

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

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

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

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

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

_____ NO _____ YES

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

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

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

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

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

_____ YES

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

_____ NO

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

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

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

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

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

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

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

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

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

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

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

8. Is the system operated by a contractor?

_____No.

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

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

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

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

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

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

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

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

_____ NO

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

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

_____ NO

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

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

_____ NO _____ YES

13. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

_____ NO _____ YES

If yes:

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

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

___ NO ___YES

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: [redacted] b7E

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [redacted] Program Office: ITMS/TISU Division: CJIS Phone: [redacted] Room Number: Module B1	FBI OGC/PCLU POC Name: [redacted] Phone: [redacted] Room Number: C3-Rm655

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: CJIS	Signature: Date signed: Name: [redacted] Title: TISU Unit Chief	Signature: Date signed: Name: [redacted] Title: CJIS Division Privacy Officer
FBIHQ Division: CJIS	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

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

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

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

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

[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):

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:

David C. Larson, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 2/23/2010

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Criminal Justice Information Services Division (CJIS) has developed a Certified and Accredited (C&A) [redacted] The [redacted] provides [redacted] for Federal Bureau of Investigation (FBI) and contractor personnel. [redacted] b7E [redacted] has been developed to replace numerous other [redacted] in order to facilitate providing FBI and contractor personnel access to the tools and resources necessary to perform their job functions [redacted] This [redacted] allows for [redacted] what took [redacted] prior to its implementation. Utilizing this [redacted] and the audit mechanisms in place to ensure the proper protection.

[redacted] is used for development and support of the CJIS [redacted] b7E [redacted]

[redacted] is an ongoing project which will provide [redacted] for the entire CJIS Division. [redacted] is being engineered with the rules and guidelines as regulated by the CJIS and Security Divisions policies and procedures. b7E [redacted] located within the CJIS Division [redacted] The [redacted] has a current C&A under the [redacted] accreditation.

[1] A PTA for this system was completed in 2008; this PTA is an update.

The nature of the information/data on the [redacted] is not intended as a permanent store of Personally Identifiable Information (PII) nor to house searchable data containing PII. The systems [redacted] do store PII. However, these systems are covered by existing Privacy Impact Assessments (PIA). [redacted] the data [redacted] and PII is [redacted] account holder from the [redacted] FBI employees and contractors. This system and information housed thereon is utilized only by FBI and contractor personnel [redacted] Information generated and/or housed on [redacted] may be used by FBI and contractor personnel for [redacted] It is disseminated only to the extent permitted by existing FBI/CJIS security and PIA policies for [redacted] and to disseminate this data through the approved channels as established by existing system PIA policies and CJIS/FBI procedures. b7E

In addition, [redacted] so the possibility exists that [redacted] data containing PII for employees, contractors and candidates for employment within the FBI. [redacted] system will not be utilized to collect any new PII data; [redacted] system will be used to [redacted] existing data/information [redacted] that are authorized to house this data. b7E

[redacted] is achieved through [redacted] with rules and guidelines as regulated by the FBI - CJIS and Security Divisions policies and procedures. b7E

[redacted] b7E

[redacted] b7E

[redacted] only sensitive but unclassified (SBU) data.

[redacted] has a limited number of required system personnel [redacted] who have access [redacted] b7E

[redacted] users will continue to receive annual general and privileged user training concerning appropriate rules of behavior and regulations including the handling of PII within FBI controlled environments. [redacted] b7E utilizes role-based access to allow and/or restrict access [redacted]

[redacted] PII data from systems with existing PIAs in place. The system will not generate new PII data to be stored, housed or searched. The system will [redacted] b7E and disseminate this data through the approved channels as established by PIA policies and CJIS/FBI security procedures.

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

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

__X__ YES [However, [redacted] PII data from systems with PIAs or other privacy documentation in place. The system will [redacted] and disseminate this data through the approved channels as established by PIA policies and CJIS/FBI security procedures.] b7E

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

_____ NO __X__ 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 __X__ YES

Only to the extent that [redacted] administrators can retrieve FBI employee and contractor domain user account information from within the [redacted] In addition, [redacted] b7E

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

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

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

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

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

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

[redacted] with rules and guidelines as regulated by the CJIS and Security Divisions policies and procedures [redacted] b7E Only authorized FBI personnel and/or contractors may have access to the system. The information/data is further protected by [redacted] Logging and auditing procedures are performed as required and appropriate with the FBI Security Division policies. [redacted] has a limited number of required system personnel to ensure that data security, integrity and confidentiality are maintained.

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

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

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

_____ YES

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

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

_____ NO

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

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

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

information from the information subject:

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

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

__X__ YES **If yes, provide date of last C&A certification/re-certification:** 08-22-2008

_____ Don't Know.

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

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

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

__X__ NO _____ YES _____ Don't know

10. Status of System/ Project:

_____ 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? 8-22-2008

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 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.

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

As described earlier, [redacted] is being developed to [redacted] within the CJIS Division. Data that was housed [redacted] may contain PII. The possibility exist that this data would get migrated to [redacted] for internal reference by FBI employees and contractors. b7E

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

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

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

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

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

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

As describe earlier, [redacted] is being developed to [redacted] within the CJIS Division. Data that was housed [redacted] may contain PII. The possibility exists that this data would get migrated to [redacted] for internal reference by FBI employees and contractors. The potential exists that as FBI systems with PII are accessed [redacted] that PII is [redacted] b7E

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

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

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

__X__ NO _____ YES

If yes:

a. **Provide date/title of the PIA:** Previous PTA approved 09-2008.

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 PTA and/or other actions are required.]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Password Reset

BIKR FBI Unique Asset ID: _____

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Division: Information Technology Services Division Phone: [redacted] Room Number: 1396	**FBI OGC/PCLU POC** Name: Phone: Room Number:

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: {insert division name}	Signature: [redacted] Date signed: 6/12/12 Name: [redacted] Title: IT Specialist/System Owner	Signature: [redacted] Date signed: Name: [redacted] Title: Privacy Officer
FBIHQ Division: {insert division name}	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

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

____ PIA is required by the E-Government Act.

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

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

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

X Please put a link to this document somewhere on the password reset site.

Applicable SORN(s): DOJ-Justice/FBI-002 & DHS-Justice/FBI-018

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

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

Prepare/revise/add Privacy Act (e)(3) statements for related forms? __No __X__ Yes (indicate forms affected):

You need a PA statement; a privacy policy is not sufficient.

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

Other:

Elizabeth Withnell, Unit Chief Privacy and Civil Liberties Unit	Signature: Date Signed:
~~James J. Landon~~, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: Elizabeth Withnell 9/23/12

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Password Reset project consists of an application called Avatier Identity Management Suite (AIMS). The application is used as a self password management tool for the entire FBI enterprise. The users can reset their password for their user accounts, unlock their account, or change their password. The system interacts with the users through the intranet using a web application framework called ASP.NET. AIMS stores account information within an Oracle database. To register the changes, it interacts with active directory through Lightweight Directory Access Protocol (LDAP) and connection with the domain controllers.

The information in the system concerns each user's account information, which is the same information as is located in Active Directory. The database also contains answers to security questions for each user. The system owner has access to this information and the Oracle database team has access to this information.

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

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

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

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

__X__ The information directly identifies specific individuals.

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

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

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

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

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

_____ NO __X__ YES

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

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

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

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

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

__X__ YES

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

__X__ NO

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

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

_X__ 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:**
Electronic "Privacy Policy & Terms of Use" statement

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

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

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

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

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

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

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

8. Is the system operated by a contractor?

__X__ No.

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

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

__X__ NO **If no, indicate reason; if C&A is pending, provide anticipated completion date**: PASSWORD RESET [redacted] is a candidate for the normal security process of an approval to test and approval for use. b7E

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

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

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

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

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

__X__ NO

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

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

__X__ NO _____ YES

12. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 2008

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

__X___ NO _____ YES

If yes:

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

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

____ NO ___YES

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: National Academy Physical Fitness Assessment Database

BIKR FBI Unique Asset ID: NA

	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [redacted] Program Office: Physical Training Unit Division: TD Phone: [redacted] Room Number: 104A	Name: AGC [redacted] Phone: [redacted] Room Number: JEH, 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program [illegible] appropriate executive	Division Privacy Officer
Program Division:	Signature: [redacted] Date signed: 11/8/2013 Name: [redacted] Title: Unit Chief	Signature: Date signed: Name: Title:
FBIHQ Division: Training Division	Signature: [redacted] Date signed: 11/8/2013 Name: [redacted] Title: Unit Chief	Signature: [redacted] Date signed: 11/9/2013 Name: [redacted] Title: Special Assistant

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:

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

Applicable SORN(s): ___FBI-002 – Central Records System_____

Notify FBI RMD/RIDS per MIOG 190.2.3? ___No _X_ Yes--See sample EC on PCLU intranet website here: http://home/DO/OGC/LTD/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: Although the system is changing from paper to electronic records, the system will still only be accessible to one individual. Further, the names of participants will be deleted from the system 180 days after their completion of the program. Thus, there are no significant privacy risks raised by this system, thereby eliminating the need for further privacy documentation.

[redacted] Acting Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 11/13/2012
Jacqueline F. Brown, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 11/14/12

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The National Academy Physical Fitness Assessment (PFA) database is a record keeping system, containing health and fitness information of individual National Academy students. National Academy is a 10-week program for upper and mid-level state and local law enforcement officers. The PFA database is comprised of an Excel spreadsheet stored on a local unclassified computer, not on a shared drive. The information collected includes an individual's name, age, sex, weight, height, waist measurements, pulse rates, mile run time, and results of other various physical tests.

The information collected helps the Physical Training Unit (PTU) provide students with pre and post training assessments. In addition, the PTU uses the information to create a gender/age based percentile ranking for each individual session and for all cumulative sessions. The system is accessible only to one individual, and is not transmitted to any other individuals. In the event where the performance data may be shared (for research purposes), the names are removed so that data cannot be linked to any participants. In addition, the names of participants will be deleted from the system 180 days after they have completed the program.

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.

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

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

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

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

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

__X__ NO _____ YES

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

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

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

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

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

__X__ YES

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

__X__ NO

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

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

____ NO

__X__ YES **Identify any forms, paper or electronic, used to request such information from the information subject: An appropriate (e)(3) notice has been developed and is now being used.**

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

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

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

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

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

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

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

8. Is the system operated by a contractor?

__X__No.

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

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

__X__ NO **If no, indicate reason: if C&A is pending, provide anticipated completion date**: The information is kept on a local excel spreadsheet, and is used only for PTU health and fitness purposes.

_____ 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