

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Enterprise Directory Service (EDS)

BIKR FBI Unique Asset ID: SYS-0000155

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

b6
b7C

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

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: [insert division name]	Signature: Date signed: Name: [Redacted] Title: [Redacted]	Signature: Date signed: Name: [Redacted] Title: [Redacted]
FBIHQ Division: ITMD	Signature: Date signed: 9/9/10 Name: [Redacted] Title: EDS Project Manager	Signature: Date signed: 9/9/10 Name: [Redacted] Title: IT Specialist

b6
b7C

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

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS: [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): 205-014; 002

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

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

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

N/A (forms have appropriate notices)

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 W. BULL
Deputy General Counsel (Att'ny)
FBI Privacy and Civil Liberties Officer

Signature:
Date Signed:

Elizabeth W. Bull
9/16/2010

L. INFORMATION ABOUT THE SYSTEM / PROJECT

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

[redacted] and the Secret Enclave Infrastructure. EDS consists of [redacted]

[redacted] (c) EDS provides a consistent, secure and up to date authoritative enterprise directory service for systems, services and applications to request and receive user identity attributes required to make access control and basic workflow decisions; (d) EDS is a directory service that contains selected identity and access control attributes of FBI employees, contractors, detailees and integrees; (e) EDS clients include: application systems, FBI Net users, and administrative clients (directory administrator and application specific delegated administrators); (f) Clients (application systems or users) interact with EDS [redacted] EDS will return the attributes to its clients based on directory queries.

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.]

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).

b7E

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

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

The key sensitive data attribute in EDS is the Social Security Account Number (SSAN).

EDS will not display and return the SSAN user attribute unless the client is explicitly authorized to see it. The authorization must first be approved by DAA.

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:** SSNs are used as a key to join data from other systems into a single directory.

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:**

b7E

SSNs are only viewable to system administrators.

_____ 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:

02/24/2010

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 FIA and/or other actions are required.]

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? EDS was deployed in January 2009.

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

NO [If no, proceed to next question (II.3).] See response to question II.1

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

See EDS PTA dated 9/29/07.

If yes:

a. Provide date/title of the PIA:

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

NO YES

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Enterprise Process Automation System (EPAS)

BIKR FBI Unique Asset ID: SYS0000139

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
	Name: [Redacted] Program Office: RPO Division: RPO Phone: [Redacted] Room Number: 6343	Name: [Redacted] Phone: [Redacted] Room Number: 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [Redacted] Date signed: 8/23/12 Name: [Redacted] Title: <i>Vice Chief</i>	Signature: Date signed: Name: Title:
FBIHQ Division: Resource Planning Office	Signature: <i>[Signature]</i> Date signed: 8/23/12 Name: Dave Schlendorf Title: Assistant Director	Signature: Date signed: Name: Add info here 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.]

<input type="checkbox"/> PIA is required by the E-Government Act. <input type="checkbox"/> 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)? <input type="checkbox"/> Yes. <input type="checkbox"/> No (indicate reason): <input checked="" type="checkbox"/> PIA is not required for the following reason(s): <input type="checkbox"/> System does not collect, maintain, or disseminate PII. <input type="checkbox"/> System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks). <input type="checkbox"/> Information in the system relates to internal government operations. <input type="checkbox"/> System has been previously assessed under an evaluation similar to a PIA. <input checked="" type="checkbox"/> No significant privacy issues (or privacy issues are unchanged). <i>PIA already covers the system</i> <input type="checkbox"/> Other (describe):	
Applicable SORN(s): <i>to the extent applicable, CR5 and for PPHS</i>	
Notify FBI RMD/RIDS per MIOG 190.2.3? <input type="checkbox"/> No <input type="checkbox"/> 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? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes (indicate revisions needed):	
Prepare/revise/add Privacy Act (e)(3) statements for related forms? <input type="checkbox"/> No <input type="checkbox"/> Yes (indicate forms affected): <i>As required</i>	
RECORDS. The program should consult with RMD to identify/resolve any Federal records/electronic records issues. The system may contain Federal records whether or not it contains Privacy Act requests and, in any event, a records schedule approved by the National Archives and Records Administration is necessary. RMD can provide advice on this as well as on compliance with requirements for Electronic Recordkeeping Certification and any necessary updates.	
Other:	
Elizabeth Withnell Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: <i>Elizabeth Withnell</i> Date Signed: <i>9/6/12</i>

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 Enterprise Process Automation System (EPAS) implements a workflow system on the FBINET to serve as a standard for automated business processes. As part of a major initiative by the Director's Office, the Resource Planning Office (RPO), Business Process Management Unit (BPMU), which is the EPAS system owner, was tasked with deploying the EPAS project to host automated business processes as they are developed and deployed by both the RPO and other Divisions.

The EPAS Privacy Impact Assessment, dated July 15, 2011, covers forms currently in EPAS and any additional forms that support FBI's administrative operations, including the management of its human resources and payroll functions, hiring, requisition processing, and security. The Privacy and Civil Liberties Officer for the FBI requires a PTA on other workflows that may be added to EPAS.

RPO is requesting approval to launch the following four new processes in EPAS. Access to each will be limited to those with a need to know.

1. Continued Service Agreements (CSA) -- CSA will automate the request and approval of the service agreements required for various incentives and training, such as recruitment, retention, and student loan reimbursement. CSA collects personal information and position and performance data for employees who are applying to receive one of these incentives. This includes the following PII: name, SSN,¹ PAR ratings, position title, EOD, student loan documentation (lender, account number, amount owed), justification for receipt of incentive payment, and amount owed to the FBI.
2. Security Incident Reporting System (SIRS) -- The software that operates the SIRS system is being replaced with a new product. The SIRS process allows Bureau personnel to submit reports of incidents [REDACTED] b7E
[REDACTED] SIRS will contain PII similar to other EPAS processes (name, SSN, phone number, login ID, file number, etc).
3. Invoice Management System (IMS) -- IMS is replacing the stand-alone CPUIMS system for processing of commercial invoices. The Financial Management System (FMS) uses SSN as the [REDACTED] b7E
[REDACTED]

¹ SSNs are required for disbursement of payments from the National Finance Center.

[redacted] however, users [redacted]
[redacted] will have access to these SSNs.

b7E

4. [redacted] will allow Bureau
program managers to [redacted]
[redacted] Most data submitted through this process will be
program based. The only PII contained in [redacted] will be system audit
information, such as names of individuals [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 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.]

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:

- Non-Bureau personnel who have information in EPAS (as part of the Staffing process or Clearance Processing System), are notified about the Privacy Act through the USAjobs posting through which they are applying and the e-QIP (SF-86) form they submit.

- A Privacy Statement is displayed on the main screen of the user interface for Bureau personnel who use the system.

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:** The social security numbers are only displayed when necessary. Since the system is role-based, only users with the appropriate roles can see pages with SSNs displayed.

_____ 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: 2/12/12
EPAS has been moved onto the DAVE platform and thus falls under its C&A. EPAS was given an AFU on this platform on 2/12/12.

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? 2007

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: **7/15/2011 Enterprise Process Automation System**

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

___ NO YES

See Section I.

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [REDACTED]

b7E

BIKR FBI Unique Asset ID: APP-0000273

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: SSA [REDACTED] Program Office: ELSUR Technology Management Unit Division: Operational Technology Division Phone: [REDACTED] Room Number: 1A81, ERF-E	FBI OGC/PCLU POC Name: AGC [REDACTED] Phone: [REDACTED] Room Number: 7350 JEH
--	---	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [REDACTED] Date signed: Name: Title:	Signature: [REDACTED] Date signed: Name: Title:
FBIHQ Division: Operational Technology Division	Signature: [REDACTED] Date signed: 9/27/12 Name: [REDACTED] Title: Unit Chief, ELSUR Technology Management Unit	Signature: [REDACTED] Date signed: 8/29/12 Name: SSA [REDACTED] Title: Assistant Section Chief, Data Acquisition/Intercept Section

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. [redacted] A PIA should be prepared for [redacted] encompassing these applications.

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):

b7E

Applicable SORN(s): [redacted] Electronic Surveillance (ELSUR) Indices system of records, DOJ/FBI-006; the SORN for DOJ/FBI-006 was last published in full at 70 Fed. Reg. 7513, 7514 (Feb. 14, 2005) [redacted] within the Central Records System (CRS), DOJ/FBI-002; the SORN for the CRS was last published in full at 63 Fed. Reg. 8659, 8671 (Feb. 20, 1998).

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):

b7E

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] Acting Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 9/7/12
Elizabeth Withnell, Acting Deputy General Counsel and FBI Privacy and Civil Liberties Officer	Signature: <i>Elizabeth Withnell</i> Date Signed: 9/7/12

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.

[REDACTED]

b7E

[REDACTED]

b7E

[REDACTED] is a web-based application developed by the Operational Technology Division (OTD) [REDACTED]

[REDACTED]

b7E

[REDACTED] operates on both the Secret Enclave and the Unclassified Network (UNet) domains. FBI personnel access [REDACTED] through the Secret Enclave, [REDACTED] in turn, accesses the [REDACTED] via the Internet using UNet. [REDACTED]

b7E

[REDACTED] application does not contain personally identifiable information except [REDACTED] which indirectly identifies an individual. [REDACTED] does contain user account information, which is collected for access and use audits. It also contains [REDACTED] information provided by [REDACTED]

b7E

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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.]

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

[redacted] was certified and accredited on August 31, 2010, as part of the [redacted] and has Authority to Operate (ATO) through August 31, 2013.

b7E

Confidentiality: ___ Low ___ Moderate X High ___ Undefined

Integrity: X Low ___ Moderate ___ High ___ Undefined

Availability: X Low ___ Moderate ___ High ___ Undefined

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? [redacted] was completed and deployed in August 2010.

b7E

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

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

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

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

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

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

_____ 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.

X Other [Provide brief explanation]: [redacted] application was previously named [redacted] when it was developed in 2010. This application [redacted] [redacted] The application replaced the previous [redacted] [redacted] by FBI personnel.

b7E

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: Facial Analysis Comparison and Evaluation Services

BIKR FBI Unique Asset ID: _____

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [Redacted] Program Office: Biometric Services Division: CJIS Phone: [Redacted] Room Number: D1	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number: C3
--	---	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [Handwritten Signature] Date signed: 8/16/12 Name: Kimberly J. Del Greco Title: Section Chief	Signature: [Redacted] Date signed: 8/24/12 Name: [Redacted] Title:
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

xx PIA is required by the E-Government Act.

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

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

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

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

Applicable SORN(s): <u>FIRS</u>	
Notify FBI RMD/RIDS per MIOG 190.2.3? <u>No</u> <u>xx</u> 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? <u>No</u> <u>xx</u> Yes:	
Prepare/revise/add Privacy Act (e)(3) statements for related forms? <u>No</u> <u>Yes</u> : 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:	
<div style="border: 1px solid black; width: 100px; height: 15px; display: inline-block;"></div> Unit Chief Privacy and Civil Liberties Unit	Signature: Date Signed:
Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: <i>Elizabeth W. ...</i> Date Signed: <i>9/6/12</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.

The Facial Analysis Comparison and Evaluation (FACE) Services Unit of the FBI's Criminal Justice Information Services (CJIS) Division, Biometric Services Section (BSS), provides investigative support to FBI Special Agents, analysts, and other authorized personnel. The FACE Services Unit accepts unclassified photographs of subjects of FBI investigations (probe photos) and uses facial recognition technology to compare those photos against FBI databases, other federal photo databases to which the FBI legally has access, and photo repositories from states that have entered into agreements with the FBI to share data. After comparison and evaluation, the FACE Services Unit returns to the FBI case agent or analyst candidate photos that are likely matches to the probe photo, with the caveat that candidate photos may serve only as investigative leads and do not constitute positive identification.

The FACE Services Unit will compare the probe photos against certain federal systems and will enter Memoranda of Understanding (MOU) as needed to ensure data security and privacy. The FACE Services Unit also will provide the probe photos to state Departments of Motor Vehicles (DMVs) to be searched against photo repositories where permitted by state law. In these instances, authorized state personnel will perform the probe photo comparisons and return candidate photos to the FACE Services Unit. The FACE Services Unit will enter MOU with the DMVs to ensure data security and privacy, including the mandatory destruction of the probe photos by the state DMVs after facial comparison is completed.

b7E

If the FACE Services Unit identifies or receives candidate photos based on the searching of the federal and state databases, it will perform additional evaluation in order to determine the most likely candidate(s) for return to the FBI case agent or analyst. The Face Services Unit will store these most likely candidates and limited biographic information in the FACE Services Work Log. The Work Log will also contain the request for assistance originally received from the FBI case agent or analyst. All remaining candidate photos and any associated information will be immediately and permanently destroyed.

Access to the Work Log will be limited to the FACE Services Unit and other authorized FBI personnel who require the information for performance of their official duties. The Work Log records will be retained in adherence to a determined National Archive and Records Administration schedule.

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.

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 not collected by the FACE Services Unit; however, SSNs may be associated with both probe and candidate photos.

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: SSNs assist with the accurate identification of subjects of law enforcement investigations.

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:** The FACE Services Work Log has not undergone C & A; however, the federal databases searched by the FACE Services Unit have undergone C & A.

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

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

Confidentiality: Low Moderate High Undefined

Integrity: Low Moderate High Undefined

Availability: Low Moderate High Undefined

Not applicable – this system is only paper-based.

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

NO

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

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

NO YES

12. Status of System/ Project:

This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NO YES

If yes:

a. Provide date/title of the PIA:

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

NO YES

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: FBI Enterprise Servers (ES) system

BIKR FBI Unique Asset ID: N/A (per ITMD, ES does not have to be registered in BIKR)

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: UC [redacted]	Name: AGC [redacted]
Reason:	Program Office: Operating Systems Support Unit	Phone: [redacted]
Declassify On:	Division: ITSD	Room Number: 7350 JEH
	Phone: [redacted]	
	Room Number: 1714 JEH	

b6
b7C

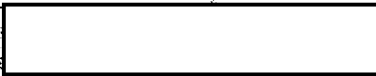

FBI DIVISION INTERMEDIATE APPROVALS [complete as necessary consonant with Division policy]

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division:	Signature: [redacted] Date signed: Name: Title:	Signature: [redacted] Date signed: Name: Title:
FBIHQ Division: Information Technology Services Division	Signature: [redacted] Date signed: 10/17/11 Name: Michael [redacted] Title: Assistant Section Chief, ITSD	Signature: [redacted] Date signed: 10-17-11 Name: [redacted] Title: Information Technology Specialist

b6
b7C

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

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

<p><input type="checkbox"/> PIA is required by the E-Government Act.</p> <p><input type="checkbox"/> PIA is to be completed as a matter of FBI/DOJ discretion.</p> <p>Is PIA to be published on FBI.GOV (after any RMD FOIA redactions)? <input type="checkbox"/> Yes. <input type="checkbox"/> No (indicate reason):</p> <p><input checked="" type="checkbox"/> PIA is not required for the following reason(s):</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> System does not collect, maintain, or disseminate PII.<input type="checkbox"/> System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).<input type="checkbox"/> Information in the system relates to internal government operations.<input type="checkbox"/> System has been previously assessed under an evaluation similar to a PIA.<input type="checkbox"/> No significant privacy issues (or privacy issues are unchanged).<input type="checkbox"/> Other (describe):	
<p>Applicable SORN(s): <u>DOJ Computer Systems Activity and Access Records, DOJ-002, 64 Fed. Reg. 250 (Dec. 30, 1999)</u></p> <p>Notify FBI RMD/RIDS per MIOG 190.2.3? <input checked="" type="checkbox"/> No <input type="checkbox"/> 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</p> <p>SORN/SORN revision(s) required? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes (indicate revisions needed):</p>	
<p>Prepare/revise/add Privacy Act (e)(3) statements for related forms? <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes (indicate forms affected):</p>	
<p>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.</p> <p>Other:</p>	
<p><input type="checkbox"/> Unit Chief Privacy and Civil Liberties Unit</p> <p>James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer</p>	<p>Signature:  Date Signed: 11/16/11</p> <p>Signature:  Date Signed: 11/17/11</p>

b6
b7c

FBI PTA: Enterprise Servers (ES) system

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 Enterprise Servers (ES) system, formerly known as the Mainframe system, provides administrative and investigative mainframe systems support for over [redacted] located throughout FBI Headquarters and Field Offices. The ES system encompasses system hardware and software, application software, and databases operating on the mainframe. [redacted]

b7E

[redacted]

[redacted]

b7E

The ES system itself does not contain, maintain or disseminate personally identifiable information (PII). Appropriate privacy documentation for applications operating on ES that collect, maintain or disseminate PII has been or will be prepared.

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.]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: FBINET Microsoft Exchange 2010 Upgrade

BIKR FBI Unique Asset ID: N/A (Part of SECRET Enclave/FBINET system architecture)

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: SITS [redacted]	Name: AGC [redacted]
Reason:	Program Office: DSSU	Phone: [redacted]
Declassify On:	Division: ITSD	Room Number: 7350 JEH
	Phone: [redacted]	
	Room Number: 1B164	

b6
b7C

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

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Information Technology Services Division (ITSD)	Signature: [redacted] Date signed: 09-04-2013 Name: [redacted] Title: Unit Chief, Directory Services Support Unit	Signature: [redacted] Date signed: 9/4/13 Name: [redacted] Title: Unit Chief, Vulnerability & Compliance Support Unit
FBIHQ Division:	Signature: Date signed: Name: Title: Unit Chief	Signature: Date signed: Name: Title:

b6
b7C

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

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: Exchange 2010 is part of the IT infrastructure supporting the FBINET/Secret Enclave network. The only PII maintained by Exchange is user data, collected for IT security purposes. The user data is authenticated against FBINET's Active Directory.

Applicable SORN(s): DOJ Computer Systems Activity and Access Records, DOJ-002, a complete notice of which was last published at 64 Fed. Reg. 73585 (Dec. 30, 1999).

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

SORN/SORN revision(s) required? No Yes (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 style="width: 100%;" type="text"/> Date Signed: 9/6/13
Jacqueline F. Brown, Acting Deputy General Counsel and FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 9/6/13

b6
b7c

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

Microsoft Exchange is a business-oriented e-mail server, calendaring software and contact manager product utilized by the FBI on the SECRET Enclave (FBINET). The FBI is updating from Exchange Server 2007 (currently in use) to Exchange Server 2010.

(a) FBINET Microsoft Exchange 2010



b7E

(c) To provide currently supported email and groupware functionality within FBINET

(d) email messages, contacts, notes, calendar events

(e) all FBINET users

(f) Transmission to email users will be accomplished via the following email clients:

- Microsoft Outlook 2010 connecting via RPC MAPI protocols (Remote Procedure Call, Messaging Application Programming Interface)
 - During the life cycle of this system it is likely that Outlook 2013 or other Microsoft software products may be deployed.
 - Outlook 2013 and later versions would no longer use the RPC MAPI protocols, but would use RPC over HTTPS protocols. End user functionality will remain the same.
- Outlook Web Access (aka webmail) connecting via HTTPS protocols

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.]

The only PII maintained by Exchange is user data, collected for IT security purposes. The user data is authenticated against FBINET's Active Directory.

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.

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:

b7E

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.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? Exchange 2010 is an updated version of Exchange 2007. Exchange 2007 was deployed August 12, 2009.

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

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

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

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

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

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

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

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

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

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

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

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

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

_____ Other: This project consists of updating the existing FBI's e-mail exchange from Microsoft Exchange 2007 to Exchange 2010. Both systems

utilize FBINET's Active Directory to identify users and validate their credentials.

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

NO YES

If yes:

a. Provide date/title of the PIA

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

NO YES

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: FBINET ScriptLogic Active Administrator Upgrade

BIKR FBI Unique Asset ID: N/A

Derived From:	SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Classified By:	Name: [redacted] contractor	Name: [redacted]
Reason:	Program Office: [redacted] contractor	Phone: [redacted]
Declassify On:	Division: ITB/ITSD	Room Number: 7350 JEH
	Phone: [redacted]	
	Room Number: 9330, JEH	

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: 10 Feb 2012 Name: [redacted] Title: Unit Chief	Signature: [redacted] Date signed: 3-6-12 Name: [redacted] Title: Privacy Contact OCIO
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):

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): if at all 3/5/12 Access Control System

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

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

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

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

Other:

[Redacted] Unit Chief Privacy and Civil Liberties Unit	Signature: [Redacted] Date Signed: 3/16/12
James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: [Redacted] Date Signed: 3/21/12

b6
b7C

I. INFORMATION ABOUT THE SYSTEM / PROJECT

- I. 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.

Ia. The name of this project is "ScriptLogic Active Administrator (AA) software upgrade". This is a COTS product made by Quest, Inc. This PIA applies only to the AA software upgrade on FBINET. ScriptLogic AA (older version) was installed on FBINET more than one year ago.

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

ScriptLogic AA does not collect, maintain, or disseminate any information about individuals (i.e., a human being or natural person, regardless of nationality). Log-on

information and passwords are the only data that are personally identifiable and the privacy impact of this is negligible.

_____ 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. 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

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