FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: [redacted] b7E

BIKR FBI Unique Asset ID: SYS-0000015

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: [redacted] Program Office: Forensic Network Division: Operational Technology Phone: [redacted] Room Number: 2C18-E	**FBI OGC/PCLU POC** Name: [redacted] Phone: [redacted] Room Number: 7350 JEH

b6
b7C

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

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Operational Technology	Signature: [redacted] Date signed: [illegible] Name: [redacted] Title: Program Manager (Acting)	Signature: [redacted] Date signed: 07/16/2014 Name: [redacted] Title: ISSO
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.

_X_ 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): [redacted]

[redacted] The privacy risks and mitigation will be handled in a PIA that addresses [redacted] systems generally. b7E

Applicable SORN(s): _____FBI _____

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:

James J. Landon, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 6/9/11

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. (This kind of information may be available in the System Security Plan, if available, or from a Concept of Operations document, and can be cut and pasted here.):

[redacted] was placed into service in March 2005 to provide [redacted] during the course of a law enforcement or intelligence investigation. Since that time, it has provided local, state, and federal law enforcement with efficient, complete, and legally defensible [redacted] upon request, providing agents, analysts, and law enforcement and intelligence community personnel a [redacted] Privacy documentation was last completed for [redacted] in 2007. This PTA comprises the requisite three-year review. b7E

[redacted] b7E

For example, during the course of a child pornography investigation, [redacted] In addition, during the course of terrorism investigations [redacted] Accordingly, personally identifying information such as one's name, social security number, photograph, telephone number, race, gender, birth date, driver's license number, or other identifying information [redacted] may be loaded onto the [redacted] b7E

[redacted] for review by FBI Special Agents and Intelligence Analysts. [redacted] agents and analysts can submit requests to [redacted] At the conclusion of an investigation, the [redacted] removes all data from the [redacted] leaving no personally identifying information in the system. b7E

[redacted] is designed such that only those [redacted] FBI Special Agents, and Intelligence Analysts assigned to a particular case [redacted] b7E

[redacted]are authorized to have access to the system and only to the [redacted] associated with their specific case. Access is controlled via user access-level privileges and based on case specificity. b7E

[redacted] b7E

Accordingly, the system is designed so that [redacted] b7E

[redacted] connects to no other systems using no other means.

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.]** Personally identifiable information may be maintained in [redacted] but the purpose of the system is to provide [redacted] b7E

[redacted]

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?

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

__X__ YES

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

_____ NO

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

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

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

Information is collected through [redacted] including those which may contain personally identifiable information, will be informed at the appropriate time pursuant to applicable law and policy. b7E

_____ 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:**

As there is no control over what data may be contained within [redacted] it is plausible that the [redacted] may include the subject's or other individuals' social security numbers (SSNs). [redacted] itself does not specifically collect or associate SSNs with other personally identifiable information. If an SSN is part of [redacted] it will only be attributable to a specific person [redacted] No SSNs are otherwise specifically stored or retrievable. b7E

__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] and thus it is not feasible to completely negate the presence of SSNs. SSNs may be included and its location is unknown until [redacted] and the case agent assigned to a particular case have access [redacted] which potentially may contain SSNs.** b7E

_____ 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)?

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

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

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

Confidentiality: __Low __Moderate _X_High __Undefined

Integrity: __Low _X_Moderate __High __Undefined

Availability: __Low _X_Moderate __High __Undefined

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

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

__X__ NO

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

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

__X__ NO

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

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

__X__ NO _____ YES

13. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? [redacted] **was placed into service in March 2005.** b7E

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

__X__ NO [If no, proceed to next question (II.3).] **While the system may feature some technological components that have been updated since the conduct of the last privacy threshold assessment, none of these technological updates alter the core functions of the system as described.**

_____ 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

Note that a PTA was prepared, but, at that time, it was determined that a PIA would not be necessary. The PTA was signed in October 2007.

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: [redacted] b7E
BIKR FBI Unique Asset ID: Pending

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [redacted] Program Office: ITB Division: ITSD/Human Resources Application Support Unit (HRASU) Phone: [redacted] Room Number: 1907	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:	Signature: Date signed: Name: Title:	Signature: [redacted] Date signed: Name: Title:
FBIHQ Division: ITSD	Signature: [redacted] Date signed: 2/27/2014 Name: [redacted] Title: IT Specialist	Signature: Date signed: 3/3/2014 Name: [redacted] Title: Division Privacy Contact OCIO

b6
b7C

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

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

_____ PIA is required by the E-Government Act.

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

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

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

Applicable SORN(s): FBI-002, The FBI Central Records System, 63 Fed. Reg. 8671 (Feb. 20, 1998), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. 17,200 (Mar. 29, 2001), 66 Fed. Reg. 33,558 (June 22, 2001), 70 Fed. Reg. 7513, 17 (Feb. 14, 2005), 72 Fed. Reg. 3410 (Jan. 25, 2007) and DOJ-002, Department of Justice Computer Systems Activity and Access Records, 64 Fed. Reg. 73,585 (Dec. 30, 1999), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001) and 72 Fed. Reg. 3410 (Jan. 25, 2007).

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): System should have a Privacy Act (e)(3) statement at login.

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: /s/ Date Signed: 1/31/2011

1. 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] is in the process of [redacted] b7E
[redacted] There is no change in the information being collected, maintained or disseminated; rather, [redacted] is being deployed on [redacted] which will employ greater network security [redacted]

[redacted]

[redacted] b7E

[redacted] identifies a user by his/her FBINET username within the FBINET domain. No additional PII is collected, maintained or disseminated. The FBINET username of the project creator and project developers are detailed in the project's properties. [redacted] provides a type of audit trail view where project developers can identify individual changes made (by title), who made the change, and when the change was created. b7E

[redacted] identifies the user through the user's FBINET domain username or through an alternative user name created by the user. The user has the option of choosing which username to use. [redacted] user name identifies individuals who modify requirements and other stored documents. [redacted] captures the history of each requirement, thus providing an audit log. b7E

[redacted] tracks user account information, including the username and password (chosen by the individual user), under direction of the System Administrator. In addition to access information, user activity of [redacted] is also maintained for audit purposes. [redacted] users can query project activities by the activity owner's username or first and last name. 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.]**

* [redacted] contain login information and audit logs of the select individuals who access the [redacted] No other PII is contained in [redacted] b7E

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

__X__ The information directly identifies specific individuals.

__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?

_____ 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:**

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)?

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

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

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

[redacted] was most recently certified and accredited on 03/10/2005. There have been no other subsequent C&As since for reasons that could only be speculated (i.e. the system fell off SecD radar). However, because the system is now [redacted] the system is now undergoing recertification. b7E

Confidentiality: __Low __Moderate _X_ High __Undefined

Integrity: __Low _X_ Moderate __High __Undefined

Availability: _X_ 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

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

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

_X__ NO

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

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

_X_ NO _____ YES

13. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

[redacted] was first deployed in 2005. b7E

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

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

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

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

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

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

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

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

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

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

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

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

_____ 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] is in process of [redacted] There is no change in the information being collected, maintained or disseminated; rather, [redacted] is being deployed on [redacted] which will employ greater network security, [redacted] **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.]

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: DAVE (Distributed Application Virtual Environment [redacted] b7E

BIKR FBI Unique Asset ID: N/A. Hosting Environments such as DAVE are not registered in BIKR.

Derived From: **Classified By:** **Reason:** **Declassify On:**	**SYSTEM/PROJECT POC** Name: Lead ITS [redacted] Program Office: Data Center Unit (DCU) Division: ITSD Phone: [redacted] Room Number: 1B054	**FBI OGC/PCLU POC** Name: AGC [redacted] Phone: [redacted] b6 b7C Room Number: 7350 JEH

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Information Technology Services Division (ITSD)	Signature: [redacted] Date signed: 10/31/13 Name: [redacted] Title: Unit Chief, Data Center Unit	Signature: [redacted] Date signed: 10/28/13 Name: [redacted] b6 b7C Title: Unit Chief, Vulnerability & Compliance Support Unit
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

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

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

__X__ PIA is not required for the following reason(s):
___ System does not collect, maintain, or disseminate PII.
___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
__X__ Information in the system relates to internal government operations.
___ System has been previously assessed under an evaluation similar to a PIA.
___ No significant privacy issues (or privacy issues are unchanged).
__X__ Other (describe): DAVE [redacted] is a hosting environment for applications operating on the [redacted] the only PII collected and maintained within DAVE is that of a limited number of IT administrators and security personnel with access rights to the DAVE infrastructure. b7E

Applicable SORN(s): DOJ-002, Department of Justice Computer Systems Activity and Access Records, 64 Fed. Reg. 73,585 (Dec. 30, 1999), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001) and 72 Fed. Reg. 3410 (Jan. 25, 2007).

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

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

Prepare/revise/add Privacy Act (e)(3) statements for related forms? __X__ No ___Yes (indicate forms affected):
PCLU will work with the Program Manager to ensure that a Privacy Act (e)(3) statement appears on the [redacted] initial login screen. b7E

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] b6 b7C Unit Chief, Privacy and Civil Liberties Unit FBI Privacy and Civil Liberties Officer	Signature: [redacted] Date Signed: 10/16/13

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 Distributed Application Virtual Environment (DAVE) [redacted] provides IT infrastructure serving as network and server architecture hosting virtual servers within the [redacted] The DAVE utilizes some common infrastructure services, such as [redacted] The DAVE management servers provide interfaces/databases supporting the allocation of server and network resources and also support the collection of performance statistics for the infrastructure and hosted servers. The DAVE also supports FBI data center consolidation and reduces spending on physical server hardware and maintenance. b7E

All access to information contained in an application hosted on DAVE is controlled by the application, rather than DAVE. For that reason, this Privacy Threshold Analysis (PTA) addresses only the DAVE hosting environment, and not the various software applications that are hosted on DAVE. Those applications will be the subject of separate PTAs.

A select group of IT administrators have access privileges to the DAVE infrastructure and management servers and their login information is stored in DAVE for security purposes. Other than administrator access and activity, the DAVE does not collect, maintain, or disseminate personally identifiable 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

__X__ YES [If yes, please continue.]

- The only PII maintained in DAVE consists of access and activity information for the limited number of IT administrators with access privileges to the DAVE infrastructure.

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.)

_____

[redacted] b7E

__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.]**

- The only PII maintained in DAVE consists of access and activity information for the limited number of IT administrators with access privileges to the DAVE infrastructure.

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?

____ 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.

__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)?

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

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

The DAVE was last certified and accredited on August 31, 2010. Its authority to operate (ATO) has been extended through August 30, 2014 at the following risk levels:

Confidentiality: __Low __Moderate __X__ High __Undefined

Integrity: __Low __Moderate __X__ High __Undefined

Availability: __Low __Moderate __X__ High __Undefined

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

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

__X__ NO

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

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

__X__ NO

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

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

__X__ NO ____ YES

13. Status of System/ Project:

_____ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? August 30, 2010

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

__X__ NO _____ YES

If yes:

a. Provide date/title of the PIA:

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

___ NO ___ YES

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM/PROJECT: DAVE (Distributed Application Virtual Environment) [redacted] b7E

BIKR FBI Unique Asset ID: N/A. Hosting Environments such as DAVE are not registered in BIKR.

Derived From: **Classified By:** **Reason:** **Declassify On:**	**SYSTEM/PROJECT POC** Name: Lead ITS [redacted] Program Office: Data Center Unit Division: ITSD Phone: [redacted] Room Number: 1B054	**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: **Information Technology Services Division (ITSD)**	Signature: [redacted] Date signed: 9/23/15 Name: [redacted] Title: Unit Chief, Data Center Unit	Signature: [redacted] Date signed: 9/23/15 Name: [redacted] Title: Unit Chief, Vulnerability & Compliance Support Unit
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6 b7C

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

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

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

__X__ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- __X__ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- ___ No significant privacy issues (or privacy issues are unchanged).
- __X__ Other (describe): DAVE [redacted] is a hosting environment for applications operating on the [redacted] the only PII collected and maintained within DAVE is that of a limited number of IT administrators and security personnel with access rights to the DAVE infrastructure. b7E

Applicable SORN(s): DOJ-002, Department of Justice Computer Systems Activity and Access Records, 64 Fed. Reg. 73,585 (Dec. 30, 1999), as amended 66 Fed. Reg. 8425 (Jan. 31, 2001) and 72 Fed. Reg. 3410 (Jan. 25, 2007).

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

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

Prepare/revise/add Privacy Act (e)(3) statements for related forms? __X__ No ___Yes (indicate forms affected): PCLU will work with the Program Manager to ensure that a Privacy Act (e)(3) statement appears on the [redacted] initial login screen. b7E

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] b6 b7C Unit Chief, Privacy and Civil Liberties Unit FBI Privacy and Civil Liberties Officer	Signature: [redacted] Date Signed: 10/10/15

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 Distributed Application Virtual Environment (DAVE) [redacted] provides IT infrastructure serving as network and server architecture hosting virtual servers within the [redacted] The DAVE utilizes some common infrastructure services, such as [redacted] The DAVE management servers provide interfaces/databases supporting the allocation of server and network resources and also support the collection of performance statistics for the infrastructure and hosted servers. The DAVE also supports FBI data center consolidation and reduces spending on physical server hardware and maintenance. b7E

All access to information contained in an application hosted on DAVE is controlled by the application, rather than DAVE. For that reason, this Privacy Threshold Analysis (PTA) addresses only the DAVE hosting environment, and not the various software applications that are hosted on DAVE. Those applications will be the subject of separate PTAs.

A select group of IT administrators have access privileges to the DAVE infrastructure and management servers and their login information is stored in DAVE for security purposes. Other than administrator access and activity, the DAVE does not collect, maintain, or disseminate personally identifiable 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

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

- The only PII maintained in DAVE consists of access and activity information for the limited number of IT administrators with access privileges to the DAVE infrastructure.

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.

[redacted] b7E

(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?

_____ 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.]**

- The only PII maintained in DAVE consists of access and activity information for the limited number of IT administrators with access privileges to the DAVE infrastructure.

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?

_____ 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.

__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**:

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

It is anticipated that C&A for DAVE [redacted] will be completed in the Spring of 2014 at the following risk levels: b7E

Confidentiality:	__Low	__Moderate	__X__ High
Integrity:	__Low	__Moderate	__X__ High
Availability:	__Low	__Moderate	__X__ High

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

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

__X__ NO

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

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

__X__ NO

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

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

__X__ NO _____ YES

13. Status of System/ Project:

__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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM / PROJECT: Distributed Application Virtual Environment (DAVE) - [redacted] b7E

BIKR FBI Unique Asset ID: N/A. Hosting platforms such as DAVE are not required to be registered in BIKR.

Derived From: Classified By: Reason: Declassify On:	**SYSTEM/PROJECT POC** Name: ITS [redacted] Program Office: Data Center Support Unit (DCSU) Division: ITSD Phone: [redacted] Room Number: JEH 1B054	**FBI OGC/PCLU POC** Name: AGC [redacted] b6 b7C Phone [redacted] Room Number: JEH 7350

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: **Information Technology Services Division (ITSD)**	Signature: [redacted] Date signed: 5/6/2014 Name: [redacted] Title: Unit Chief, DCSU	Signature: [redacted] b6 b7C Date signed: 5/6/2014 Name: [redacted] Title: Unit Chief, Vulnerability Compliance Support Unit
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

____ PIA is required by the E-Government Act.

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

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

__X__ PIA is not required for the following reason(s):
- ___ System does not collect, maintain, or disseminate PII.
- ___ System is grandfathered (in existence before 4/17/2003; no later changes posing significant privacy risks).
- __X__ Information in the system relates to internal government operations.
- ___ System has been previously assessed under an evaluation similar to a PIA.
- ___ No significant privacy issues (or privacy issues are unchanged).
- __X__ Other: DAVE [redacted] is a hosting environment for applications operating on the [redacted] the only PII collected and maintained within DAVE is that of a limited number of [redacted] with access rights to the DAVE infrastructure.

b7E

Applicable SORN(s): DOJ-002, *Department of Justice Computer Systems Activity and Access Records*, 64 Fed. Reg. 73,585 (Dec. 30, 1999), as amended.

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

Prepare/revise/add Privacy Act (e)(3) statements for related forms? __X__ No ___Yes
PCLU will work with the Program Manager to ensure that a Privacy Act (e)(3) statement appears on the DAVE initial login screen.

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

Other:

Monica E. Ryan, Unit Chief Privacy and Civil Liberties Unit FBI Privacy and Civil Liberties Officer	Signature: [signature] Date Signed: 6/3/14

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Distributed Application Virtual Environment (DAVE) – [redacted] provides a virtual hosting environment for various applications operating within the FBI's [redacted] domain.[1] The DAVE infrastructure provides a network and server architecture on which to host virtual servers. The DAVE utilizes some common infrastructure services, such as [redacted] The DAVE-specific management servers provide interfaces/databases to support the allocation of server and network resources and to support the collection of performance statistics for the infrastructure and hosted servers. The DAVE also supports Data Center consolidation and reduces spending on physical server hardware and maintenance. b7E

All access to information contained in an application hosted on DAVE is controlled by the owner of the particular application, rather than by DAVE. For that reason, this Privacy Threshold Analysis (PTA) is limited to the DAVE hosting environment itself, and does not encompass the various software applications hosted on DAVE. To the extent that particular software applications require privacy documentation, those applications will be the subject of separate documentation.

Access to the DAVE [redacted] infrastructure and management servers is limited to approximately [redacted] assigned to the ITSD's Data Center Support Unit (DCSU) along with [redacted] assigned to the Security Division (SecD). User access and activity information for these individuals is collected and maintained within DAVE, as required, for IT support and security purposes. No personally identifiable information (PII) about other individuals is collected, maintained, used, or disseminated by DAVE [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

__X__ YES [If yes, please continue.]

[1] Separate PTAs have previously been prepared for the DAVE hosting environments on [redacted] domains. b7E

- The only PII maintained in DAVE consists of user access and activity information for the limited number of ITSD and SecD personnel with access rights to the DAVE infrastructure.

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?**

_____ 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.]

- The only PII maintained in DAVE consists of user access and activity information for the limited number of ITSD and SecD personnel with access rights to the DAVE infrastructure.

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?

_____ NO

_____ YES

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

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

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

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

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

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

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

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

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

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

8. Is the system operated by a contractor?

__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 DAVE [redacted] is undergoing certification and accreditation; a completion date is not yet available. It is anticipated that DAVE [redacted] will receive authority to operate (ATO) at the following risk levels: b7E

Confidentiality: __Low __Moderate __X__ **High**

Integrity: __Low __Moderate __X__ **High**

Availability: __Low __Moderate __X__ **High**

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

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

__X__ NO

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

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

__X__ NO

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

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

__X__ NO _____ YES

13. Status of System/ Project:

_____ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? DAVE [redacted] was first deployed in October, 2013. b7E

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

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

There have been no significant changes to DAVE [redacted] affecting the collection, retention, use or dissemination of PII since it was first deployed.

_____ 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

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

Total Deleted Page(s) = 3
Page 4 ~ b7E;
Page 5 ~ b7E;
Page 6 ~ b7E;

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Digital Collection System (DCS) 6000

BIKR FBI Unique Asset ID: SYS-0000023

Derived From: Classified By: Reason: Declassify On: N/A	**SYSTEM/PROJECT POC** Name: Electronics Eng'r [redacted] Program Office: Telecommunications Intercept Collections Technology Unit (TICTU) Division: Operational Technology Division Phone: [redacted] Room Number: ERF-E, 4A68	**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 [redacted]
Program Division: Operational Technology Division (OTD)	Signature: [redacted] Date signed: [redacted] Name: SSA [redacted] Title: Unit Chief, TICTU	Signature: [redacted] Date signed: [redacted] Name: SSA [redacted] Title: Assistant Section Chief
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

(The FBI Privacy and Civil Liberties Officer's determinations, conditions, and/or final approval will be recorded on the following page.)

FBI PTA: Digital Collection System (DCS 6000)

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

__X__ 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)? __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:

Applicable SORN(s): FBI Central Records System, JUSTICE/FBI-002, 63 Fed. Reg. 8659, 8671 (Feb. 20, 1998), as amended at 66 Fed. Reg. 17200 (Mar. 29, 2001) and 66 Fed. Reg. 29994 (June 4, 2001); Electronic Surveillance (ELSUR) Indices, JUSTICE/FBI-006, 70 Fed. Reg. 7514 (Feb. 14, 2005).

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 ___ 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: **PCLU will coordinate with OTD to ensure that a Privacy Impact Assessment (PIA) is prepared for the components of the Digital Collection System operated by TICTU (DCSNet, DCS 3000, DCS 5000 and DCS 6000). This requirement may be satisfied by a consolidated PIA discussing one or more components and separate PIAs for components that are not included in the consolidated PIA.**

[redacted] Acting Unit Chief Privacy and Civil Liberties Unit	Signature: [redacted] Date Signed: 10/1/2014
Jacqueline F. Brown, Acting Deputy General Counsel and FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 10/1/2014

b6
b7C

FBI PTA: Digital Collection System (DCS 6000)

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.

Title III of the Omnibus Crime Control Act of 1968 (TIII), as amended, permits the FBI to intercept wire, oral or electronic communications as authorized by warrant. The DCS 6000 (sometimes referred to as [redacted] an earlier version was known as [redacted] is a [redacted] b7E

[redacted] b7E

[redacted] b7E

- [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?

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

__X__ YES

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

_____ NO

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

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

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

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

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

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

While the DCS 6000 is not designed to collect SSNs, they may be inadvertently collected [redacted] Any SSNs obtained during conversations deemed non-pertinent will be purged, in accordance with 18 U.S.C. § 2518(5). b7E

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

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

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

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

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

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)?

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

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

DCS 6000 was most recently reaccredited on September 12, 2010 and has Authority to Operate (ATO) through September 11, 2013.

Confidentiality: **__Low _X_ Moderate __High __Undefined**

Integrity: **__Low _X_ Moderate __High __Undefined**

Availability: **__Low _X_ Moderate __High __Undefined**

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

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

_____ NO

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

DCS 6000 is encompassed by the OMB 300 for *FBI Digital Collection*, forwarded by the FBI to DOJ on February 13, 2012.

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

__X__ NO

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

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

__X__ NO _____ YES

13. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? DCS 6000 was first deployed in November, 1999.

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.

__X__ Other **[Provide brief explanation]:** Since its initial deployment in 1999, updates to DCS 6000 have involved server enhancements or replacements as well as software (operating system) updates. [redacted] b7E

[redacted]

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

__X__ NO _____ YES

FBI PTA: Digital Collection System (DCS 6000)

If yes:

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

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

___ NO ___ YES

A Privacy Threshold Analysis (PTA) for DCS 6000 was completed in April, 2007.

[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.]