

SSNs are used by [] only for electronic matching of access records in the various FBI systems that currently still use the SSN as the primary identifier. Moving forward, it is expected that, wherever possible, other less sensitive attributes, such as the FBI unique ID, will be used to maintain these accounts throughout its lifecycle.

b7E

[] will [] and will assume the physical security constraints inherent to that environment, including limiting access to authorized individuals. All access to and activities conducted within the [] system by users and administrators are logged and auditable. In addition, [] will provide the Bureau with audit and reporting capabilities that reflect who has access to what systems and how that access was granted.

b7E

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

_____ NO

___X___ YES [If yes, please continue.]

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

(Check all that apply.)

___X___ The information directly identifies specific individuals.

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

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

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

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

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

_____ NO ___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.]

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

The information about individuals contained within will pertain only to FBI personnel (including contractors and task force officers); no information about non-FBI personnel will be contained in

b7E

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

NO [If no, proceed to question 7.]

YES

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

NO

YES [If yes, proceed to question 7.]

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

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

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

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

NO YES If yes, check all that apply:

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

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

SSNs are important for other reasons. Describe:

While [redacted] itself will use the Unique Employee Identifier (UEID) for personnel identification purposes. SSN is the common attribute that will be used to link identifies to accounts in other legacy systems that have not yet implemented the UEID in place of the SSN. SSNs will not be accessible to any [redacted] end user. SSNs are used by [redacted] only for electronic matching of access records in the various FBI systems that currently still use the SSN as the primary identifier by authorized administrators.

b7E

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:

SSNs in [redacted] will not be viewable by any system user. In addition, SSNs will be placed in protected status. The SSN field will be hidden from the user profile [redacted] view. The SSN field will also be encrypted.

b7E

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 PI 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:

As [redacted] is developed within the [redacted] [redacted] has had SecD scans as part of the [redacted] C&A process. The last C&A for [redacted] was August 30, 2010. It is rated at the same levels of [redacted] High Confidentiality, High Integrity, and High Availability. [redacted] was last C&A scanned on December 27, 2012.

b7E

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

Confidentiality: ___Low___Moderate XHigh ___Undefined

Integrity: ___Low___Moderate XHigh ___Undefined

Availability: ___Low___Moderate XHigh ___Undefined

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

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

X NO

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

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

X NO _____ YES

will ultimately replace is currently a FISMA system, and thus at that time it is possible will be determined to be a FISMA system.

b7E

12. Status of System/ Project:

_____ This is a new system/ project in development.

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

The functionality of underwent enterprise deployment on January 14, 2013.

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): Changes have been made as part of [redacted] but they do not change the overall assessment that this is part of internal government operations.

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Palantir (U) *Unclassified*

BIKR FBI Unique Asset ID: APP-0000290

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: [REDACTED] Program Office: Intelligence Products Unit (IPU) Division: Information Technology Management Division Phone: [REDACTED] Room Number: CC-4	Name: [REDACTED] Phone: [REDACTED] Room Number: JEH, Rm 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Information Technology Management Division	Signature: [REDACTED] Date signed: 12/4/2013 Name: [REDACTED] Title: Unit Chief	Signature: [REDACTED] Date signed: 12/4/2013 Name: [REDACTED] Title: IT Specialist
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.)

UNCLASSIFIED//FOUO

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

PIA is required by the E-Government Act.

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

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

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

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

Applicable SORN(s): DOJ/FBI-022, FBI Data Warehouse System, 77 Fed. Reg. 40630 (July 10, 2013)

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

SORN/SORN revision(s) required? No Yes

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

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

Other:

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

Signature:
Date Signed:

12/9/13

b6
b7c

UNCLASSIFIED//FOUO

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

(U) Palantir is the knowledge management application for the FBI that combines many capabilities needed for effective intelligence analysis into one integrated platform. Palantir can tie together data from hundreds of formats, including messages, link charts, spreadsheets, documents, as well as structured and unstructured data. This enables agents, analysts, and support staff across the FBI to organize intelligence information, discover non-obvious connections, and collaborate internally. Palantir currently has a Secret instance at the FBI – Palantir (S). This PTA discusses the Unclassified instance of Palantir, which we will refer to as Palantir (U).¹

(U) Palantir allows a user to save his/her analysis and make that analysis available to other users as though it were another data source. Palantir tracks every change to the data (similar to an audit log), displays it for the user, and stores the data for later analysis. Palantir also increases the ability of analysts to collaborate across teams, or programs by allowing users to share their products with others.

(U) [redacted] across the FBI. It will also help users extract relevant information that might not otherwise be apparent to the user. For example, the visual query tools within Palantir allow users to uncover relationships of which the user was not previously aware. Palantir allows even the smallest pieces of data to be “tagged” or characterized for future use. Tagging of the data allows users to create structured information from documents; thus, facilitating the use of electronic analytics which rely on structured data for making connections.

b7E

(U//FOUO) Palantir has several methods for providing access control. Access Controls can be set at any level, [redacted] Access controls can be provided to Palantir [redacted] Palantir users, the access control rules would govern what [redacted] information Palantir users would be able to access. [redacted]

b7E

¹ Unless otherwise noted, “Palantir” refers to characteristics that Palantir (S) and Palantir (U) share.

[redacted]

b7E

(U//FOUO) Second, Palantir users have the ability to set discretionary access controls on Palantir products they create in their Palantir defined workspace,³ to include which users and groups are authorized to access their work. Users also have the ability to set permissions regarding which actions can be taken on the data in their workspace, to include setting the owner, write, read, and discovery permissions. It is important to note

[Redacted]

b7E

from other data sources and therefore, an individual will not be able to share a workspace or information in a Palantir product with anyone who does not have the same access permissions. Additionally, Palantir business managers are currently creating business rules that are in line with FBI access control and data sharing policies for user import, creation and sharing of Palantir products in the Unclassified environment. The rules will dictate what users can share with others. Users will be trained regarding these business rules in the required Palantir training course.

(U//FOUO) Standing up an Unclassified instance of Palantir will allow analysis of [Redacted]

[Redacted]

[Redacted] analysis of the information that users pull into Palantir. At this time,

Palantir will [Redacted]

[Redacted]

Initially, this information is likely to include the following types of information: Personally Identifiable Information (PII), including addresses, email addresses, and phone numbers, and other data pertaining to FBI investigations. At the unclassified level, [Redacted]

b7E

[Redacted]

[Redacted] This will give FBI staff the opportunity to collaborate internally as well as allow for them to communicate and share data.

(U) Users will be instructed that in order to upload a certain amount of information, they will first need to contact their Chief Division Counsel regarding whether new privacy documentation will need to be conducted prior to uploading the new information. In addition, Palantir will conduct additional privacy analysis as necessary as information sets are made available in the future.

(U//FOUO) [Redacted]

[Redacted] Palantir will [Redacted] create link analysis

charts and graphs on the Unclassified platform. Palantir will also allow the opportunity to recreate old link analysis charts. [Redacted]

b7E

[Redacted]

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

³ In Palantir, a user's defined workspace is called an "investigation," but for clarity, that term will not be used in this PTA.

_____ 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 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: Pending with an anticipated completion date of 12/20/2013

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:

Once a certain amount of information is imported into Palantir (U) or is accessible through Palantir (U), it will allow FBI special agents, intelligence analysts, and support staff to perform a variety of analyses to develop and understand entities and their relationships with one system interface. [Redacted]

[Redacted] All data mining activity will be reported in accordance with applicable policies.

b7E

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 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.]

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.]

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM / PROJECT: Palantir

BIKR FBI Unique Asset ID: 2011-027-01

SYSTEM/PROJECT POC	FBI OGC/PCLU POC
Name: [REDACTED] Program Office: NSB Operations Support Phone: [REDACTED] Room Number: JEH, Rm 11100	Name: AGC [REDACTED] Phone: [REDACTED] Room Number: JEH, Rm 7350

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Information Technology Engineering Division (ITED)	Signature: [REDACTED] Date signed: 8/15/2012 Name: [REDACTED] Title: Program Manager	Signature: [REDACTED] Date signed: 8/15/2012 Name: [REDACTED] Title: IT Security Program Manager
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.)

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 FBLGOV (after any RMD FOIA redactions)? Yes. No:
Because this is a national security system, the PIA will not be published.

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

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

Applicable SORN(s): DOJ/FBI-022, FBI Data Warehouse System, 77 FR 40630

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

SORN/SORN revision(s) required? No Yes

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

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

Other:

<input type="checkbox"/> Unit Chief Privacy and Civil Liberties Unit	Signature: <input type="checkbox"/> Date Signed: 8/22/12
Brian Binney, Acting Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: <i>Brian Binney</i> Date Signed: 8/29/12

b6
b7C

UNCLASSIFIED//FOR OFFICIAL USE ONLY

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

(U) [redacted] Palantir is a knowledge management application that combines many capabilities needed for effective intelligence analysis into one integrated platform. Palantir can tie together data from hundreds of formats, including messages, link charts, spreadsheets, documents, as well as structured and unstructured data. This enables analysts to organize intelligence information and discover non-obvious connections.

b3
b7E

(U) Palantir allows a user to save his/her analysis and make that analysis available to other users as though it were another data source. Palantir tracks every change to the data, displays it for the user, and stores the data for later analysis. Palantir also increases the ability of analysts to collaborate, across teams, programs, or agencies.

(U) Palantir is accessible from user workstations on the FBI Secret Enclave. Palantir will have [redacted] and the FBI Secret Enclave. [redacted] Palantir will contain investigative data [redacted] Palantir also contains data from other FBI databases that have completed the appropriate privacy documentation.

b3
b7E

(U) [redacted] [redacted] across the FBI. It will also help users extract relevant information based on intuitive queries that might not otherwise be apparent to the user. Palantir allows even the smallest pieces of data to be "tagged" or characterized for future use.

b3
b7E

(U) Palantir data, [redacted] [redacted] a Palantir product, will be accessible via the FBI Secret Enclave [redacted] [redacted] throughout the FBI.

b3
b7E

[redacted]

b3
b7E

(U//FOUO) Palantir has several methods for providing access control. First, access control [redacted] and associated access permissions, which are passed to and maintained in Palantir. [redacted]

b3
b7E

(U//FOUO) Second, Palantir users have the ability to set discretionary access controls on Palantir products they create in their Palantir defined workspace,² to include which users and groups are authorized to access their work. Users also have the ability to set permissions regarding which actions can be taken on the data in their workspace, to include setting the owner, write, read, and discovery permissions. It is important to note [redacted] and therefore, an individual will not be able to share a workspace or information in a Palantir product with anyone who does not have the same access permissions. Additionally, Palantir business managers are currently creating business rules that are in line with FBI access control and data sharing policies for user import, creation and sharing of Palantir products. The rules will dictate what users can share with others. Users will be trained regarding these business rules in the required Palantir training course.

b3
b7E

(U//FOUO) Finally, information subject to restrictions (e.g. grand jury data) will have the same authorization and permission options as described above except permissions and authorizations will be controlled by Palantir administrators in coordination with case agents.

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.

² In Palantir, a user's defined workspace is called an "investigation," but for clarity, that term will not be used in the PTA.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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:

Palantir is part of the C&A for [redacted] which was last certified in March, 2012.

b3
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. 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:

(U) Palantir allows FBI special agents and intelligence analysts to perform a variety of analyses to develop and understand entities and their relationships with one system interface. [redacted]

[redacted] All data mining activity will be reported in accordance with applicable policies.

b3
b7E

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.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

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

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

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

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

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

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

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

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

_____ Other [Provide brief explanation]:

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

_____ NO _____ YES

If yes:

a. Provide date/title of the PIA:

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

_____ NO _____ YES

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI Privacy Threshold Analysis (PTA) Cover Sheet (OGC/PCLU (Rev. 1/17/07))

NAME OF SYSTEM: Technical Revitalization Program

FBI SYSTEM CONTACT PERSON

Name: [Redacted]
Program Office: Information Technology Operations Division (ITOD)
Division: ITOD
Phone: [Redacted]
Room Number: 1B940
Date PTA submitted for approval: April 11, 2007

b6
b7C

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

	Program Division:ITOD	FBIHQ Division:ITOD
Program Manager (or other appropriate executive as Division determines)	Signature: Date signed: 4/11/07 Name: [Redacted] Title: Program Manager (Customer Support Unit Chief)	Signature: Date signed: 4/21/07 Name: Louis J. Blazy Title:Assistant Director (ITOD)
Division Privacy Officer	Signature: Date signed: Name: [Redacted] Title: Deputy General Counsel	Signature: Date signed: Name: Title:

b6
b7C

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

FINAL FBI APPROVAL:

FBI Privacy and Civil Liberties Officer	Signature: Date Signed: 5/15/07 Name: Patrick W. Kelley Title: Deputy General Counsel
---	--

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

1 - Original signed copy to 190-HQ-C1321794

Copies:

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

(*please reproduce as needed for Program/Division file(s))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: Technical Revitalization Program

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

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

A. General System Description: The Technical Revitalization Program (TRP) is an orderly and planned replacement of the Federal Bureau of Investigation's (FBI) technical assets associated with the FBI's FBINET and UNET enclaves, which are the primary backbones of the FBI's communications and operations.

1. Type of information in the system:

a. The Technical Revitalization Program involves technical assets. It is not a system and therefore has no information.

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

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

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

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

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

7. Has this system been certified and accredited by the FBI Security Divisions? Yes No N/A

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

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

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

NO (If "no," proceed to Section II.) Although the Technical Revitalization Program is not a system, the timing of the replacement of IT equipment postdates April 17, 2003.

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

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

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: Technical Revitalization Program

(Continue to Question 2.)

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

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

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

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

3. Is the system solely related to internal government operations?

YES If "yes," is this a Major Information System (as listed on OGC's FBINET website)?:

Yes. (If "yes," a full PIA is required.. PTA is complete.)

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

NO (If "no," go to section III to determine if a full or short-form PIA is required.)

II. For systems developed after April 17, 2003.

1. What is the purpose of the system? (Answer in detail unless details already provided in A. 2 above):

The Technical Revitalization Program is an orderly and planned replacement of the FBI's technical assets that are associated with its operating platforms.

(Continue to Question 2.)

2. Does the system collect, maintain or disseminate information in identifiable form about individuals?

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

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

3. Is the system solely related to internal government operations?

YES If "yes," is this a Major Information System (as listed on OGC's FBINET website)?:

Yes. (If "yes," a full PIA is required.. PTA is complete.)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

NAME OF SYSTEM: Technical Revitalization Program

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

NO (If "no," go to section III to determine if a full or short-form PIA is required.)

III. Full or Short-Form PIA

1. Is the system a major information system (as listed on OGC's FBINET website)?

YES (If "yes," a full PIA is required. PTA is complete.)

NO (If "no," please continue to question 2.)

2. Does the system involve routine information AND have limited use/access?

The Technical Revitalization Program is not a system.

YES A short-form PIA is required. (I.e., you need only answer Questions 1.1, 1.2, 2.1, 3.1, 4.1, 5.1 (if appropriate), 6.2, 6.3, and 8.9 of the PIA template.) Please note that FBI and DOJ reviewing officials reserve the right to require completion of a full PIA. (PTA is complete--forward with PIA.)

NO (If "no," a full PIA is required. PTA is complete.)

July 24, 2008: Name change annotation:

From: [redacted] (ITOD) (CON)
Sent: Thursday, July 24, 2008 3:16 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (ITOD) (FBI); [redacted] (ITOD) (FBI); [redacted] (ITOD)(FBI)
Subject: Prevention of Information Technology Obsolescence (PITO) - OMB Exhibit 300 FY 10 Submission
Importance: High

b6
b7c

UNCLASSIFIEDNON-RECORD

[redacted]

Per our phone discussion, for your records the Technology Revitalization Program is currently known as Prevention of Information Technology Obsolescence (PITO) program.

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

NAME OF SYSTEM: Evidence Collection and Management System (ECMS)

FBI SYSTEM CONTACT PERSON Name: SSA [redacted] Program Office: Evidence Response Team Unit Division: Laboratory Phone: [redacted] Room Number: 4310 Date PTA submitted for approval: 08/16/2007	FBI OGC/PCLU POC Name: [redacted] [redacted] Phone: [redacted] Room Number: JEH 7338
--	---

b6
b7C

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

	Program Division: [insert division name]	FBIHQ Division: Laboratory
Program Manager (or other appropriate executive as Division determines)	Signature: Date signed: Name: Title:	Signature: /s/ Date signed: 8/16/07 Name: [redacted] Title: Supervisory Special Agent
Division Privacy Officer	Signature: Date signed: Name: Title:	Signature: /s/ Date signed: 8/16/07 Name: John Joseph Behun Title: Section Chief

b6
b7C

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

FINAL FBI APPROVAL:

FBI Privacy and Civil Liberties Officer	Signature: /s/ Date Signed: 8/22/07 Name: David C. Larson Title: Acting Deputy General Counsel
---	---

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

1 - Signed original to 190-HQ-C1321794

Copies:

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

(*please reproduce as needed for Program/Division file(s))

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Evidence Collection and Management System (ECMS)

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

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

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

A. General System Description: Please briefly describe:

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

b7E

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

b7E

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

b7E

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

b7E

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Evidence Collection and Management System (ECMS)

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

[Redacted box]

b7E

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

No persons outside the FBI will have access to the information.

7. Has this system been certified and accredited by the FBI Security Divisions?

NO - The FBI Security Division (SECD) has authorized the ERT Unit to build and beta test. Once the system is proven to be secure, SECD will certify and accredit the system.

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

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

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

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

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

___ YES If "yes," please explain the nature of those changes: (Continue to Question 2.)

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

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

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

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

3. Is the system solely related to internal government operations?

___ YES If "yes," is this a Major Information System (as listed on OGC's FBINET website)?:

___ Yes. (If "yes," a full PIA is required.. PTA is complete.)

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Evidence Collection and Management System (ECMS)

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

___NO (If "no," go to section III to determine if a full or short-form PIA is required.)

II. For systems developed after April 17, 2003.

1. What is the purpose of the system? (Answer in detail unless details already provided in A. 2 above):
SEE A.2 above.

(Continue to Question 2.)

2. Does the system collect, maintain or disseminate information in identifiable form about individuals?

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

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

3. Is the system solely related to internal government operations?

YES. See A.1 and A.2 above.

[Redacted]

[Redacted]

b7E

If "yes," is this a Major Information System (as listed on OGC's FBINET website)?:

___Yes. (If "yes," a full PIA is required.. PTA is complete.)

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

___NO (If "no," go to section III to determine if a full or short-form PIA is required.)

III. Full or Short-Form PIA

FBI PRIVACY THRESHOLD ANALYSIS (PTA)

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

NAME OF SYSTEM: Evidence Collection and Management System (ECMS)

1. Is the system a major information system (as listed on OGC's FBINET website)?

YES (If "yes," a full PIA is required. PTA is complete.)

NO (If "no," please continue to question 2.)

2. Does the system involve routine information AND have limited use/access?

YES A short-form PIA is required. (I.e., you need only answer Questions 1.1, 1.2, 2.1, 3.1, 4.1, 5.1 (if appropriate), 6.2, 6.3, and 8.9 of the PIA template.) Please note that FBI and DOJ reviewing officials reserve the right to require completion of a full PIA. (PTA is complete—forward with PIA.)

NO (If "no," a full PIA is required. PTA is complete.)

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

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

NAME OF SYSTEM / PROJECT: Correspondence and Electronic Request Management (CERM)

	SYSTEM/PROJECT POC Name: [Redacted] Program Office: Executive Secretariat Division: Director's Office Phone: [Redacted] Room Number: 6147	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number: 7338
--	---	---

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: 7/13/09 Name: [Redacted] Title: <i>UNIT CHIEF, EXEC SEC</i>	Signature: [Redacted] Date signed: [Redacted] Name: [Redacted] Title: [Redacted]
FBIHQ Division: Director's Office	Signature: [Redacted] Date signed: [Redacted] Name: [Redacted] Title: Executive Secretariat Unit Chief	Signature: [Redacted] Date signed: 7/14/09 Name: [Redacted] Title: RPO Special Assistant

b6
b7C

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

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

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

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

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

b6
b7C

FBI PTA: Correspondence and Electronic Request Management (CERM)

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): FBI-002 (backed up by DOJ-003)

Notify FBI RMD/RIDS per MIOG 190.2.3? N/A-previously addressed.


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

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

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

Signature: 
Date Signed: 7/27/03

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

The Correspondence and Electronic Request Management (CERM, formerly called the Correspondence Management System (CMS)) provides the FBI Executive Secretariat (ExecSec) with management and tracking features to include: control of incoming documents or electronic forms; assignment of requests for response or action to specific action offices; creation or review of official responses; management of response versions; routing responses to approving officials; and reporting current status and overdue items. CERM also provides functionality to ensure that the records have adequacy, authenticity, and legal sufficiency; and preserves trustworthy and secure records.

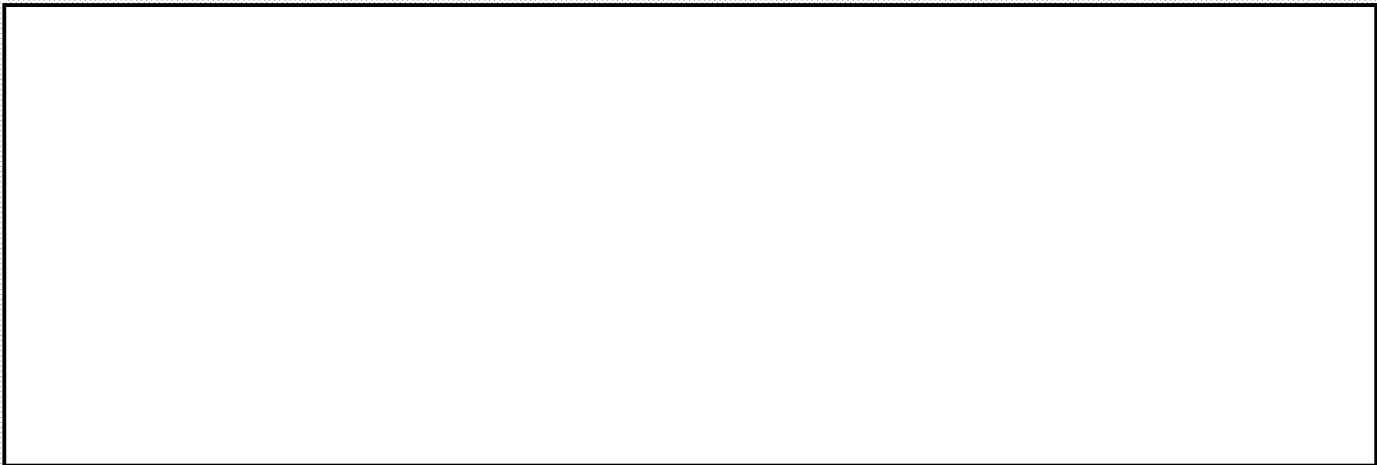
CERM provides tracking features to include: control of incoming documents or electronic forms; assignment of requests for response or action to specific action offices; creation or review of official responses; management of response versions; routing responses to approving officials; and reporting current status and overdue items. The ExecSec uses CERM to catalog the assigned "Action Office" and "Record Action" items necessary for each correspondence. After a document is entered into CERM the ExecSec can assign the "Action Office" and show each particular "Record Action" specifically for that record. All records stored in CERM are retrieved by searching based on the metadata gathered or a document content search possible if the images are scanned using OCR capable software.

All CERM documents are kept as part of the FBI Director's official collection of records. Therefore they fall under the permanent retention schedule established by the National Archives and Records Administration (NARA).



b7E

¹ The system's name was formally changed from CMS to CERM on 08/19/2008.



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

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

YES. [If yes, please continue.]

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

NO. YES.

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

NO. YES.

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

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

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

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

SSNs are important for other reasons. Describe:

FBI PTA: Correspondence and Electronic Request Management (CERM)

_____ 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: CERM makes scanned copies of incoming correspondence as received by the FBI. If SSNs are provided in incoming correspondence, then the SSNs will be contained within the system as they appear on the scanned documents.

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. The system may retain information voluntarily submitted at a correspondent's own initiative.

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

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

NO.

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

N/A. Although CERM may scan and retain information directly provided by individuals, the FBI has not asked the individuals to supply any information and any information provided has been at the individual's own initiative.

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

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

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

YES. If yes, provide date of last C&A certification/re-certification: 02/06/2009

_____ Don't Know.

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

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

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

NO. _____ YES. _____ Don't know.

FBI PTA: Correspondence and Electronic Request Management (CERM)

10. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? The CERM (then called CMS) system was procured prior to the end of FY-2002, and the system obtained approval to operate for certification testing on 10/1/2002.

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

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

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

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

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

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

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

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

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

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

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

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

_____ 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.

[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 .]

[Redacted]

b7E

(OGC/PCLU (Rev. 01/05/09))

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

NAME OF SYSTEM / PROJECT: [Redacted]

b7E

Derived From: Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [Redacted] Program Office: QITSU Division: ITOD Phone: [Redacted] Room Number: Bldg 9, LL11, Quantico	FBI OGC/PCLU POC Name: [Redacted] Phone: [Redacted] Room Number: JEH 7338
--	--	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: ITOD	Signature: [Redacted] Date signed: 5/19/09 Name: [Redacted] Title: Unit Chief/System Owner	Signature: [Redacted] Date signed: 5/26/09 Name: [Redacted] Title: ITOD Division Privacy Officer
FBIHQ Division:	Signature: Date signed: Name: Title:	Signature: Date signed: Name: Title:

b6
b7C

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

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

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

- 1 - Signed original to file 190-HQ-C1321794 (fwd to JEH 1B204 via PA-520)
- Copies (recipients please print/reproduce as needed for Program/Division file(s)):

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

- 1 - OGC/PCLU intranet
- 1 - PCLU UC
- 1 - PCLU Library
- 1 - PCLU Tickler

b6
b7C

RELEASED JAN 1, 2009



FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

FIA required: No Yes: SORN/SORN revision required: No Yes:


Applicable SORN(s): JUSTICE/FBI-002, Central records System

Notify FBI RMD/RIDS per MIOG 190.2.3: No Yes

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

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

Other: System is grandfathered.

David C. Larson, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature:  Date Signed: 6/15/07
--	---



I. INFORMATION ABOUT THE SYSTEM

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

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



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

____X____ YES. [If yes, please continue.]

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

____X____ NO.

_____ YES.



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

_____ NO.

____X____ YES. Email global address list provides name, email address, unit, and phone number (if available)

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

____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:

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

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

_____ YES.

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

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

_____ NO.

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

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

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

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

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

YES. If yes, provide date of last C&A certification/re-certification: 2/9/09

Don't Know.

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

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

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

NO. YES. Don't know.

10. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed? 1997

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

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

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

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

- _____ A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.
- _____ A new use of an IT system/project, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)
- _____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.
- _____ A new method of authenticating the use of and access to information in identifiable form by members of the public.
- _____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.
- _____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.
- _____ A change that results in a new use or disclosure of information in identifiable form.
- _____ A change that results in new items of information in identifiable form being added into the system/project.
- _____ Changes do not involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system/project.
- _____ Other. [Provide brief explanation]:

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

a. Provide date/title of the PIA:

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

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

UNCLASSIFIED/FOUO

(OGC/PCLU (Rev. 01/05/09))

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

b3
b7E
b7D

NAME OF SYSTEM / PROJECT: [redacted]

Derived From: Not Applicable Classified By: Reason: Declassify On:	SYSTEM/PROJECT POC Name: [redacted] Program Office: HUMINT Technical Unit (HTU) Division: Directorate of Intelligence (DI) Phone: [redacted] Room Number: 11100	FBI OGC/PCLU POC Name: [redacted] Phone: [redacted] Room Number: 7338
---	---	---

b6
b7C

FBI DIVISION INTERMEDIATE APPROVALS

	Program Manager (or other appropriate executive as Division determines)	Division Privacy Officer
Program Division: Office of IT Program Management (OIPM)	Signature: [redacted] Date signed: 05/08/09 Name: [redacted] Title: Program Management Executive	Signature: [redacted] Date signed: 5/8/09 Name: [redacted] Title: Information Technology Specialist
FBIHQ Division: Directorate of Intelligence (DI)	Signature: <i>Kevin Favreau</i> Date signed: 5/7/09 Name: Kevin Favreau Title: Assistant Director DI	Signature: [redacted] Date signed: 5/6/09 Name: [redacted] Title: Privacy Officer for the Directorate of Intelligence

b6
b7C

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

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

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

- 1 - Signed original to file 190-HQ-C1321794 (fwd to JEH 1B204 via PA-520)
- Copies (recipients please print/reproduce as needed for Program/Division file(s)):

UNCLASSIFIED/FOUO

UNCLASSIFIED/FOUO

FBI PTA:

b3
b7D
b7E

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

- 1 - OGC/PCLU intranet
- 1 - PCLU UC
- 1 - PCLU Library
- 1 - PCLU Tickler

b6
b7C

UNCLASSIFIED/FOUO

FBI PTA:

b3
b7D
b7E

FINAL FBI APPROVAL / DETERMINATIONS / CONDITIONS:

PIA required: No Yes: SORN/SORN revision required: No Yes:

No changes to system to warrant a Privacy analysis,

Applicable SORN(s): *last PIA done in 2006*

Notify FBI RMD/RIDS per MIOG 190.2.3: No Yes

Memorandum made in 2006 to sup. memo

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

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

Other:

David C. Larson, Deputy General Counsel FBI Privacy and Civil Liberties Officer	Signature: <i>[Handwritten Signature]</i> Date Signed: <i>5/6/2009</i>
--	---

FBI PTA:

b3
b7D
b7E

I. INFORMATION ABOUT THE SYSTEM / PROJECT

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

b3
b7D
b7E

UNCLASSIFIED/FOUO

FBI PTA:

b3
b7D
b7E

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

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

YES.

b3
b7D
b7E

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

NO. YES.

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

NO. YES.

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

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

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

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

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

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:**

b3
b7D
b7E

UNCLASSIFIED/FOUO

FBI PTA:

b3
b7D
b7E

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

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

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

YES.

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

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

NO.

b3
b7D
b7E

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:

UNCLASSIFIED/FOUO

FBI PTA:

b3
b7D
b7E

7. Has the system undergone Certification & Accreditation (C&A) by the FBI Security Division (SecD)?
___ NO. If no, indicate reason; if C&A is pending, provide anticipated completion date:
___X___ YES. If yes, provide date of last C&A certification/re-certification: May 13, 2008
___ Don't Know.

8. Is this system/project the subject of an OMB-300 budget submission?
___X___ NO. ___ Don't know. ___ YES. If yes, please provide the date and name or title of the OMB submission:

9. Is this a national security system (as determined by the SecD)?
___ NO. ___X___ YES. ___ Don't know.

10. Status of System/ Project:

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

II. EXISTING SYSTEMS / PROJECTS

1. When was the system/project developed?

It was first deployed in a limited pilot to six Field Offices on May 14, 2008.

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

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

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

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

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

UNCLASSIFIED/FOUO