To: Counterterrorism From: Office of the General Counsel
Re: (U) 190-HQ-C1321794, 05/10/2007

Privacy Impact Assessment for the

[redacted] b3 b7E

04/15/2007

Contact Points

John J. Hess, Section Chief
[redacted] Unit Chief,
[redacted] SSA
[redacted] Project Manager b6 b7C
Communications Analysis Unit
Counterterrorism Division
[redacted]

Reviewing Officials

Patrick W. Kelley
Privacy and Civil Liberties Officer
Office of the General Counsel
Federal Bureau of Investigation

Jane C. Horvath
Chief Privacy Officer and Civil Liberties Officer
Department of Justice

To: Counterterrorism From: Office of the General Counsel
Re: (U) 190-HQ-C1321794, 05/10/2007

Introduction

(U) Pursuant to Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, issued under the authority of 28 U.S.C. 533 and 534,5 the FBI is authorized to collect information for broad analytic and intelligence purposes in order to protect the national security. Similarly, the FBI has extensive authority pursuant to Attorney General Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise investigations to use all lawful techniques to investigate crimes and to gather criminal intelligence. One technique that is used for both national security and criminal investigations is the [redacted] b7E [redacted] in accordance with constitutional and statutory safeguards.

(S) [redacted] b1 b3 b7E

5 (U) In addition to the FBI's broad authority to collect information for investigatory and national security purposes, several statutes authorize the Bureau to [redacted] b7E for foreign intelligence or law enforcement purposes.

6 (S//NF) [redacted] (S) b1 b3 b7E

(S)

b1
b3
b7E

(S) (S//NF) existed prior to the implementation of the E-Government Act and thus was not subject to the PIA requirements of Section 208.

(S)

(S)

b1
b3
b7E

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

(S) ~~(S)~~ collects data,

(S)

b1
b3
b7E

1.2 From whom is the information collected?

(S)

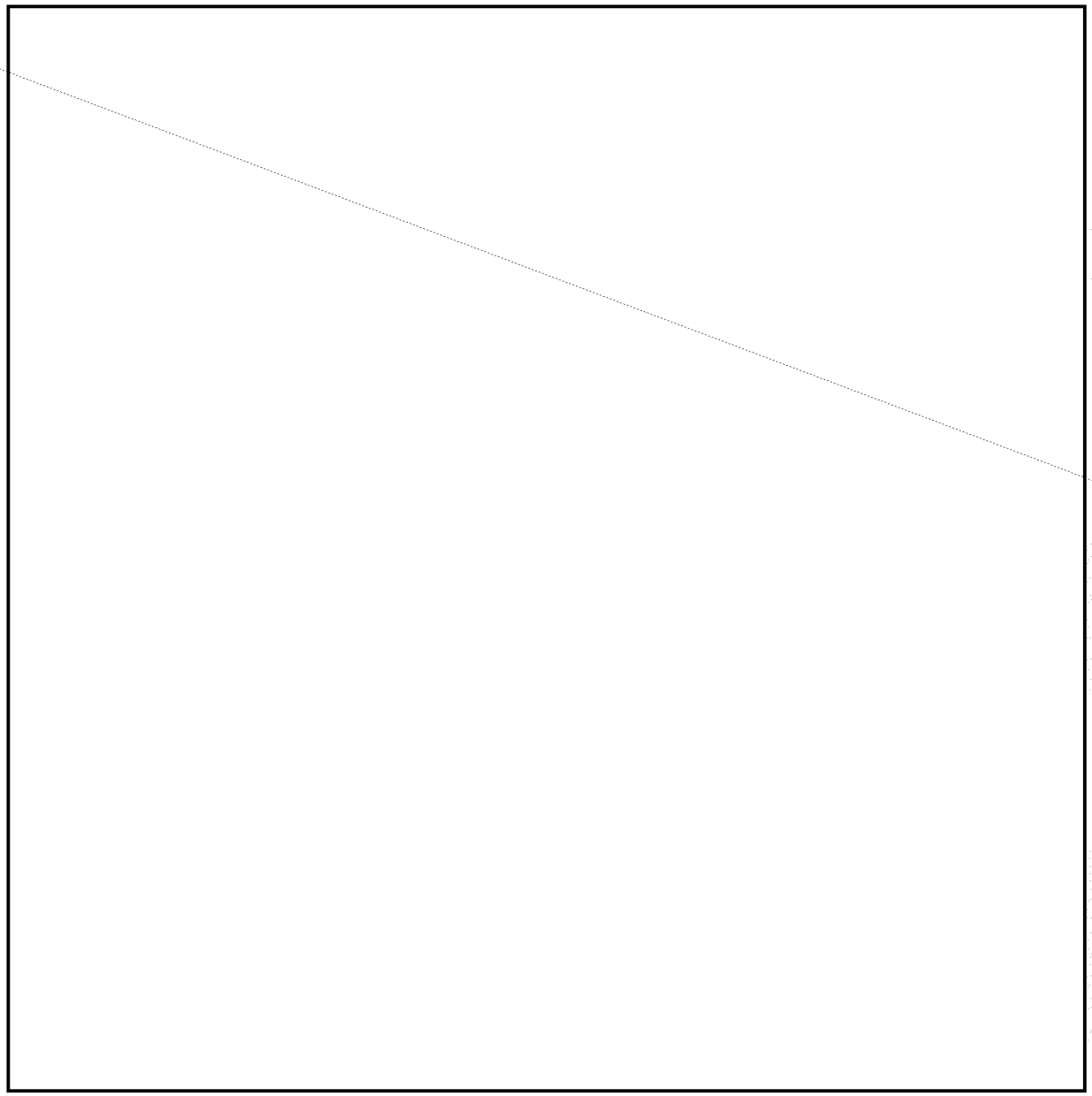
b1
b3
b7E

7 (U)

b7E

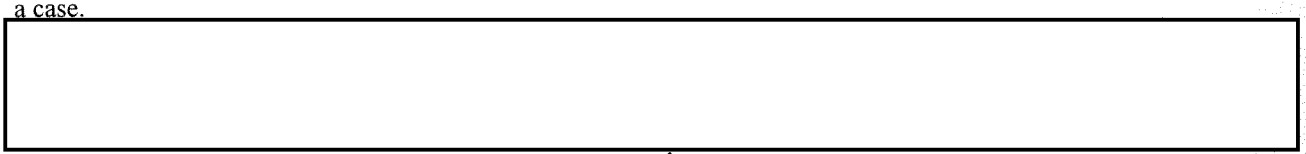
To: Counterterrorism From: Office of the General Counsel
Re: (U) 190-HQ-C1321794, 05/10/2007

(S)



b1
b3
b7E

8 (U) A PIA covering [redacted] was approved on April 3, 2003. b7E
9 (U) A lead is a request from FBI Headquarters Division or an FBI field office for assistance in the investigation of a case.

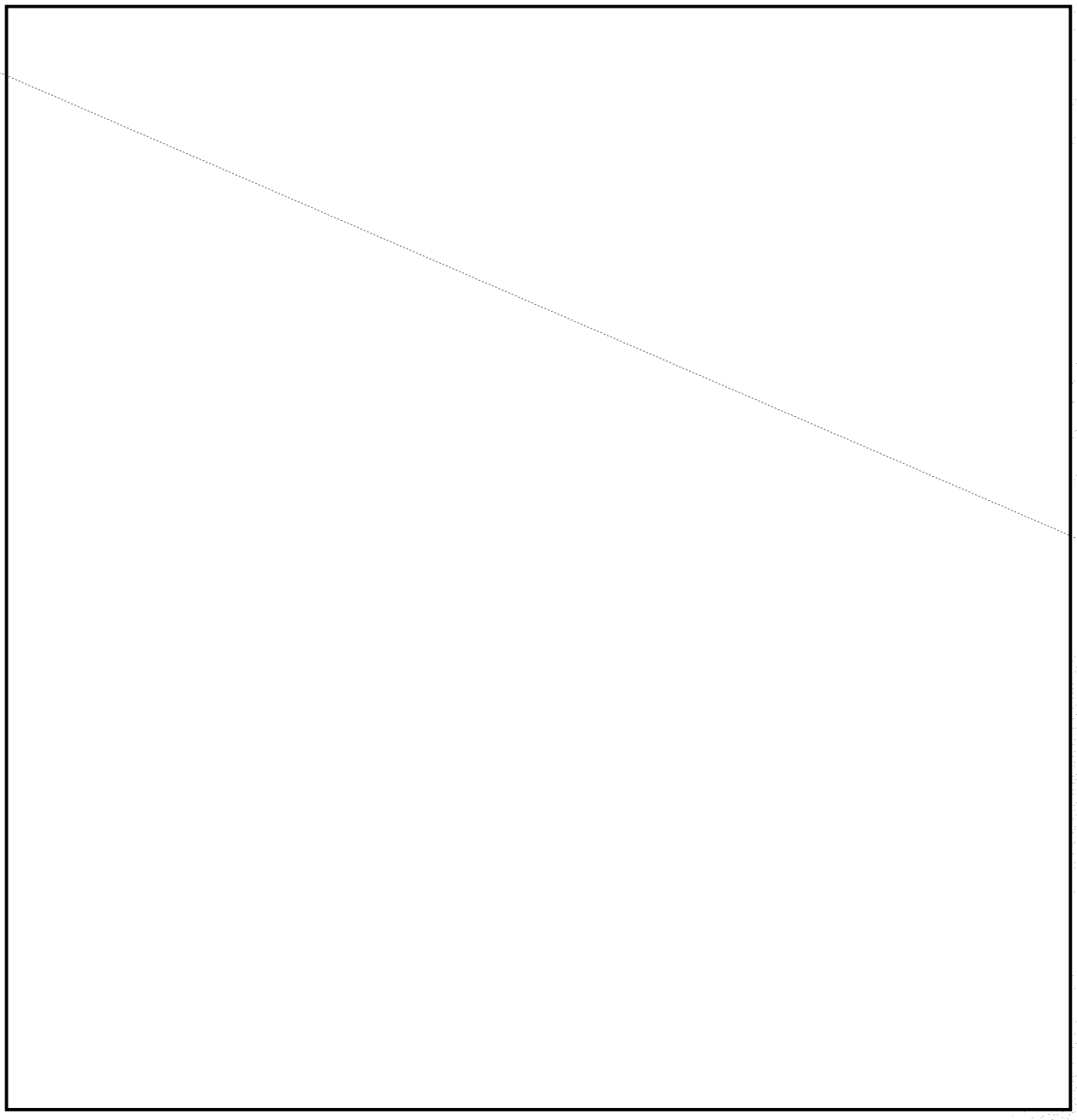


b1
b3
b7E

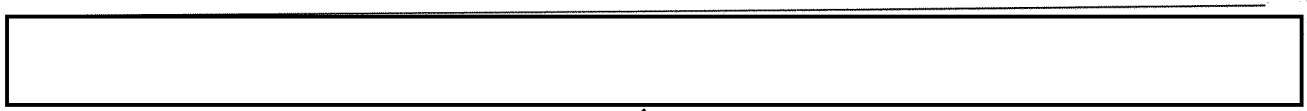
(S)

To: Counterterrorism From: Office of the General Counsel
Re: (U) 190-HQ-C1321794, 05/10/2007

(S)



b1
b3
b7E



(S) b1
b3
b7E

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

(S) (S) The information is collected to support FBI investigations with [redacted] FBI data collected during investigative activities [redacted] b1 b3 b7E

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

(S) [redacted] b1 b3 b7E

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

(S) (S) [redacted] the system is indexed primarily for extremely fast data retrieval of [redacted] b1 b3 b7E

[redacted] 11 [redacted] (S)

(S) [redacted] b1 b3 b7E

[redacted]

(S)

b1
b3
b7E

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

(S)

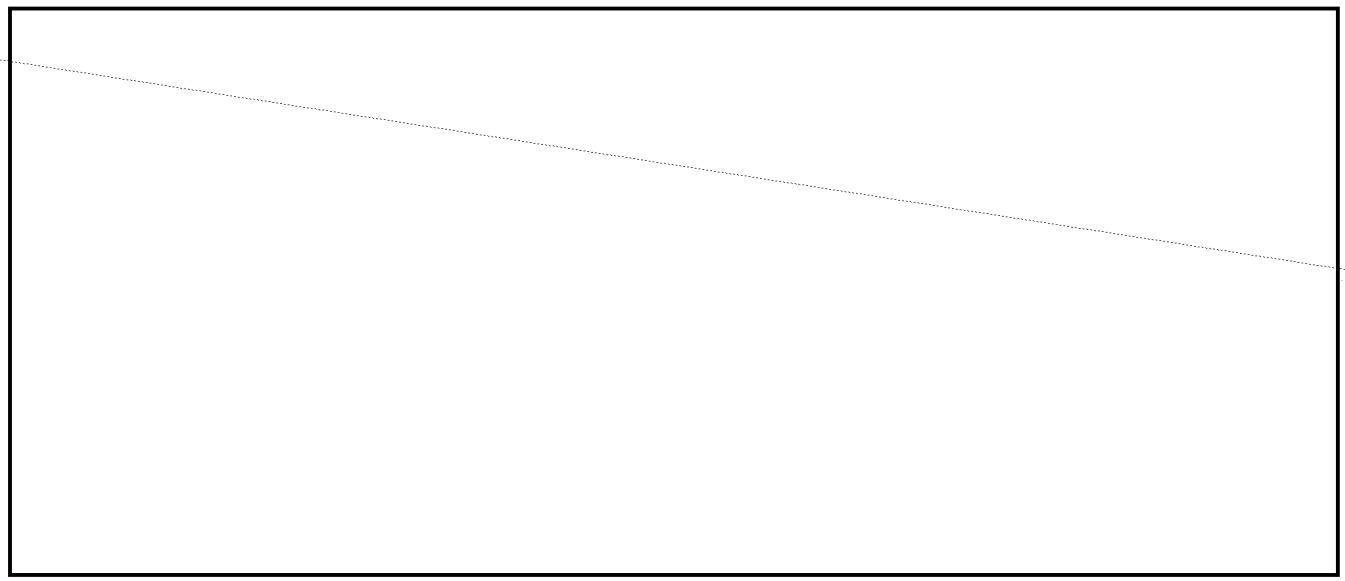
3.1 Describe all uses of the information.

(S) ~~(S)~~ [redacted] is used for lead purposes only in support of potentially any FBI investigation provided there is a predicate reason for consulting the database. [redacted]

[redacted]

b1
b3
b7E

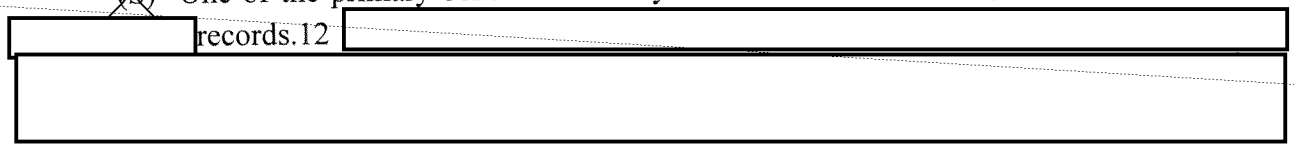
(S)



b1
b3
b7E

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

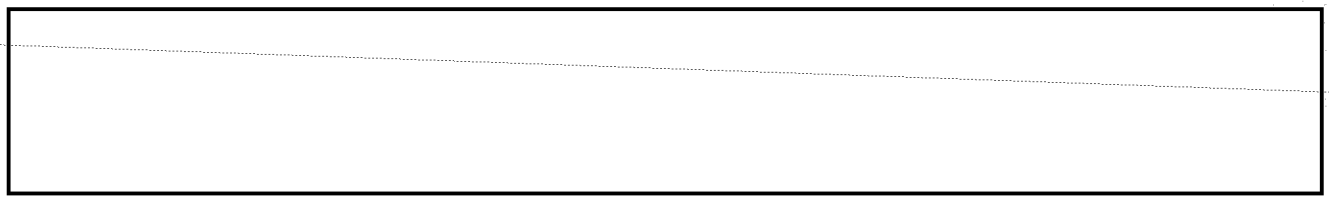
(S) (S) One of the primary benefits of the system is to allow the analytical exploitation of records.12



b1
b3
b7E

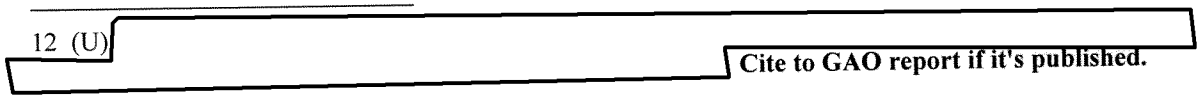
3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

(S)



b1
b3
b7E

12 (U)



b7E

(S)

b1
b3
b7E

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

~~(S)~~ The Counterterrorism Division/Communications Analysis Unit is working with the Records Management Division to develop a records retention policy for FBI-collected data in (S) mindful of the fact that counterterrorism and counterintelligence investigations often include scopes of activity that cover decades.

b1
b3
b7E

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

~~(S)~~ All users receive initial training in the proper use of information from and the same training points are integrated into online Frequently Asked Questions (FAQ) that are available to users. In addition, advanced training classes are held periodically, where the usage information is re-enforced. Users are required to sign stringent Rules of Behavior and real-time audits are conducted to ensure that the rules for using the system are followed. Users must enter a reason for their searches as a "tag." This tag is recorded for other users to see and in the log file for review by system administrators and security officials. After one violation of the tag

b1
b3
b7E

13 (U)

b7E

assignment rules, a user is warned and retrained. After a second, the account is disabled and the user would have to reapply and be completely retrained.

(U) Expansion within the FBI of access to this database by Field Offices and Legal Attaches should not increase any risks to the system or to information in it as these rules will be applied uniformly.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

(S) ~~(S)~~ Only FBI employees or detailees to the FBI (e.g. a Joint Terrorism Task Force member) can obtain an [redacted] account. b1 b3 b7E

4.2 For each recipient component or office, what information is shared and for what purpose?

[redacted] (S) b1 b3 b7E

4.3 How is the information transmitted or disclosed?

(S) ~~(S//NF)~~ Information from [redacted] is put into an electronic communication (EC), which is an official FBI record and is maintained in the Bureau's automated case support b1 b3 b7E

system or is placed in another official FBI document, such as an intelligence assessment written by the Directorate of Intelligence. Dissemination is primarily through electronic means, although (S) [redacted] information may also be disseminated in paper records. b1 b3 b7E

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

(U) The bulk of the data at issue consists of [redacted] b7E [redacted] if at all. Any potential privacy risks are mitigated by the fact that the information extracted from the database is for lead purposes only and cannot be acted upon without further investigation to confirm its accuracy and utility. The database itself requires a demonstrated need to know, as endorsed by a supervisor, as a precondition to obtain access, and employs strong rules of behavior, which are highlighted in a warning banner that users see each time they log on. Users are trained on the proper use of data from the system. Additionally, user activities, including targets queried and a justifiable reason for searches, are logged and reviewed by the Information System Security Officer. This review facilitates prompt disciplinary action for system misuse. Finally, users are trained to disseminate only discreet data elements extracted from the system; wholesale data "dumps" are impermissible.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

~~(S)~~ Under separate approvals from the FBI Office of General Counsel (OGC), the Counterterrorism Division and the Counterintelligence Division, only [redacted] b1 b3 b7E

(S) [redacted] b1 b3 b7E

5.2 What information is shared and for what purpose?

(S) [redacted] b1 b3 b7E

5.3 How is the information transmitted or disclosed?

(S) [redacted] b1 b3 b7E

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

~~(S~~//NF) The data is national security data and is protected at the Secret level. [redacted] b1 b3 b7E (S) [redacted] privacy and security statutory and regulatory requirements, such as Executive Order 12333, that govern use of the data.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

(S) [redacted] b1 b3 b7E

5.6 Are there any provisions in place for auditing the recipients' use of the information?

(S) ~~(S~~//NF) The application stores both user queries and records of the "hits" obtained from each data file. [redacted] b1 b3 b7E

(S) [redacted] b1 b3 b7E

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

(S) [redacted] b1 b3 b7E

Section 6.0
Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

~~(S)~~ In general, no notice is provided. [redacted]

(S) [redacted] b1 b3 b7E

6.2 Do individuals have an opportunity and/or right to decline to provide information?

(U) N/A, because notice is not provided. With respect to [redacted] there is no opportunity to decline to provide the information other than through declining to use the [redacted] b7D b7E

[redacted]

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

(U) N/A.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

(U) N/A. The privacy risks are managed through system access controls and audits rather than through notice.

Section 7.0
Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

(S) [redacted] b1 b3 b7E

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

(S)

(S//NF) N/A.

(S)

b1
b3
b7E

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

(S//NF) Redress is not permitted directly, but the fact that any information in the system is set for lead purposes only

(S)

b1
b3
b7E

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

(S//NF) N/A. See answer above. Since is for use as lead purposes only, no operational or criminal court actions should be based on data in the system.

b1
b3
b7E

(S)

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

(S) (S) (S) [redacted] is available to FBI employees and detailees at FBI Headquarters with appropriate clearances and a need-to-know that is certified in writing by their supervisor. [redacted] will be available for FBI employees and detailees with Top Secret clearances and accounts on the FBI's Secret network, who are at FBI Headquarters, Field Offices or Legal Attaches, as long as they have a need-to-know certification in writing by their supervisor.

b1
b3
b7E

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

(S) [redacted]

b1
b3
b7E

8.3 Does the system use "roles" to assign privileges to users of the system?

(S) Yes. [redacted]

b1
b3
b7E
(S)

8.4 What procedures are in place to determine which users may access the system and are they documented?

(S) ~~(S)~~ Roles are documented in the [redacted] system security plan and are implemented through user access application forms, rules of behavior, security, privacy and system training, and supervisor certification of a need to know. b1 b3 b7E

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

(U) ~~(S)~~ System Administrators and the ISSO have security tools to review access to data items to ensure that access is commensurate with role. In addition, both sets of individuals monitor the database operation log in real time.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

(U) ~~(S)~~ Every user action is logged to an operational log and the user must provide a tag or reason for the search. This log is reviewed in real time and is archived in multiple locations. If an audit reveals a system use violation, prompt action is taken in accordance with a documented Incident Response Plan that among other things, calls for notification of FBI Security Division personnel.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

~~(S)~~ All users are required to undergo initial account training before obtaining access as well as advanced training on data use procedures. These procedures are also on the system's Frequently Asked Questions page. Every user receives a one-page "rules of behavior," which is (S) posted on the [redacted] web page used to log onto the application. Upon logon, these rules of behavior are specifically presented as a pop-up. In addition, every FBI employee with computer access is provided with annual security training that includes an information security component. b1 b3 b7E

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

(S) (U) Yes. [redacted] was granted Authority to Operate on 8/18/2004. [redacted] is currently undergoing the Certification and Accreditation process.

b1
b3
b7E

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Because the system maintains strict access controls that are enforced by real-time auditing, the potential risk to privacy of permitting access to the database is effectively mitigated.

Section 9.0 Technology

(U) The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

(S//NF) Yes, [redacted] (S)

b1
b3
b7E

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

(S) [redacted]

b1
b3
b7E

[redacted] b1 (S) b3 b7E

(S) These risks to the integrity of the data are mitigated through restrictive use policies and user training. [redacted]

[redacted] (S) b1 b3 b7E

(S) Because it is a classified system, security is, and has always been, a primary consideration in system development. Access controls have been tested and certified by [redacted] (S) b1 b3 b7E Certifications and Accreditations. Because of the sensitivity of the data being analyzed, [redacted] includes logging, access control and auditing tools that ensure proper use of this data.

9.3 What design choices were made to enhance privacy?

[redacted] b1 b3 b7E (S)

[redacted] b1 b3 b7E (S)

Conclusion

(S) (S) has as its primary purpose with resulting "hits." Therefore, the privacy impacts of the database are mitigated because the focus is limited only to Further protection for the data is provided by the use-restriction that all results can only be used for lead purposes. (S) the system is not indexed for these searches, making them time consuming and onerous. Consequently, such searches are not conducted, another fact that helps to mitigate the privacy risks associated with the system. (S) Even were these searches conducted, all use of must be accordance with the Attorney General's Guidelines and/or the FBI's Manual of Administrative Operations and Procedures and users must tag their queries with a justification that is in accordance with the AG's guidelines or identifies an FBI investigation. Thus, any query of (S) linked to an FBI investigation. Violations of the rules of behavior for the system are apparent quickly because auditing occurs in real time. This allows for prompt action against violations. Overall, therefore, the database, which is of significant utility to the Bureau, has protections built in or associated with its use that mitigate privacy risks.

b1
b3
b7E

b1 (S)
b3
b7E

To: Counterterrorism From: Office of the General Counsel
Re: (U) 190-HQ-C1321794, 05/10/2007

Responsible Officials

/s/ 5/9/07 (Sign Date)

[redacted] b6 b7C
Project Manager

/s/ 5/10/07 (Sign Date)

[redacted] b6 b7C
Unit Chief
Communications Analysis Unit

/s/ 5/14/07 (Sign Date)
John J. Hess
Section Chief
Communications Exploitation Section

/s/ 5/14/07 (Sign Date)
Patrick W. Kelley
Privacy and Civil Liberties Officer
Federal Bureau of Investigation

/s/ 6/20/07 (Sign Date)
Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice

⊄⊄