

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 3/30/2005

To: IT Operations
Director's Office

Attn: Ms. Gail Scavongelli
Attn: Mr. Zalmay Azmi, CIO
Mr. [redacted] (OCA)
Mr. [redacted] (OPA)
Mr. [redacted] (OCTO)

CJIS
Training
Administrative Services
Counterintelligence
Criminal Investigative
Laboratory
Inspection
Security
Finance
Counterterrorism

Attn: Mr. [redacted]
Attn: Mr. [redacted]
Attn: Mr. [redacted]
Attn: Ms. [redacted]
Attn: Ms. [redacted]
Attn: Mr. [redacted]
Attn: Mr. [redacted]
Attn: Mr. Richard Haley
Attn: Mr. [redacted]
Mr. [redacted]
Mr. [redacted]
Attn: Mr. [redacted]
Attn: Mr. David Hardy
Ms. Marie Allen
Attn: Mr. [redacted]
Attn: Mr. [redacted]

b6
b7C

Cyber
Records Management

Investigative Technology
Office of Intelligence

From: General Counsel
Administrative Law Unit/ Room 7338
Contact: [redacted] (202) 324-[redacted]

b6
b7C
b2

Approved By: Kelley Patrick W
[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-11-2007 BY 65179 DMH/BJA/CAL

Drafted By: [redacted] lbh

Case ID #: 66F-HQ-C1321794

1058805

Title: ADMINISTRATIVE LAW UNIT CORRESPONDENCE
PRIVACY IMPACT ASSESSMENT (PIA) UPDATE
INVESTIGATIVE DATA WAREHOUSE (IDW)

Synopsis: [redacted]
[redacted]

b2
b7E

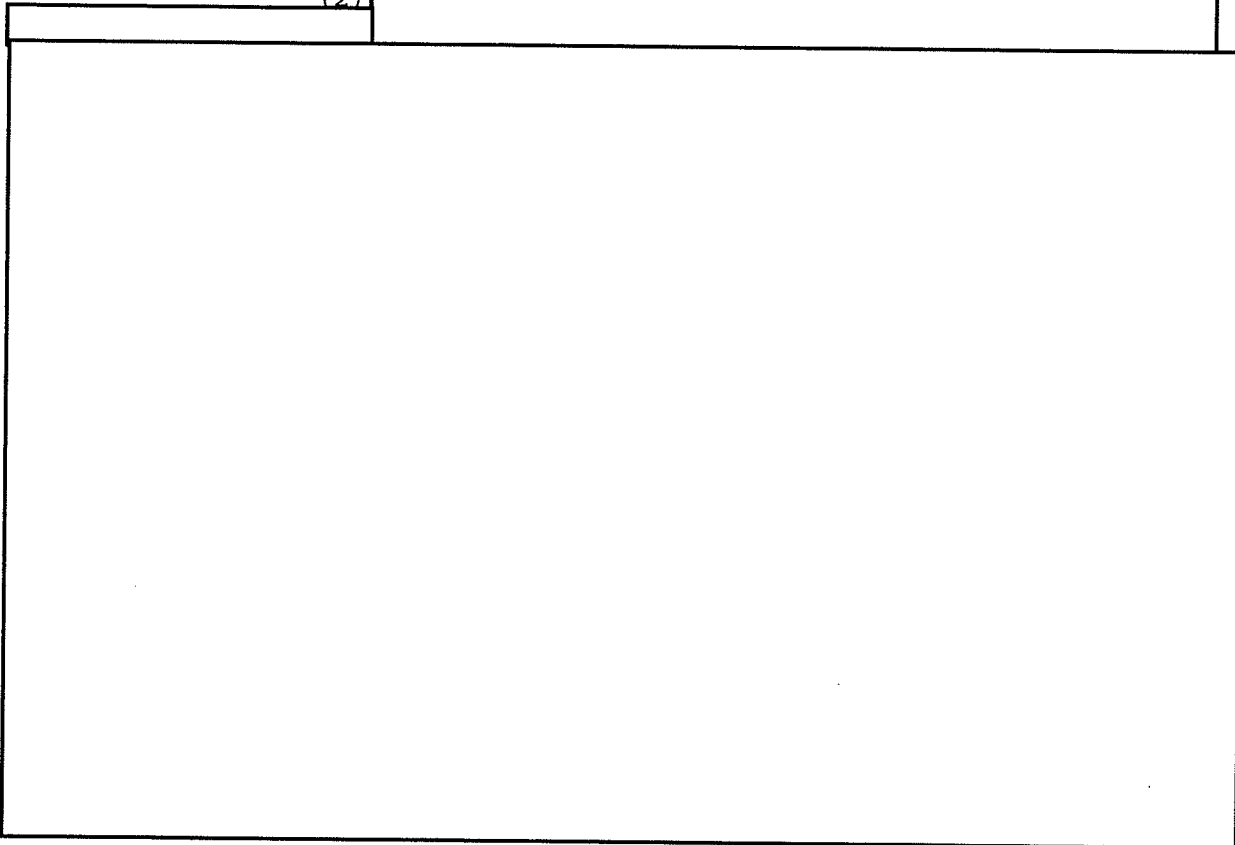
Reference: 66F-HQ-1321794 Serial 166
66F-HQ-1321794 Serial 197

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005

Administrative: This documents contains footnotes. To read the footnotes, download and print the document in WordPerfect. This is a privileged FBI communication; do not circulate outside the FBI without the permission of the Office of the General Counsel.

Enclosure(s): (1) Privacy Impact Assessment, [redacted]

(2) [redacted]



b2
b7E

¹Please see the referenced EC, 66F-HQ-1321794 Serial 166, for more information.

²Please see the referenced EC, 66F-HQ-1321794 Serial 197, for more information.

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005

LEAD(s):

Set Lead 1: (Action)

OCIO, OCTO









AT WASHINGTON, DC

Please take action consistent with this EC.

Set Lead 2: (Info)

ALL RECEIVING OFFICES

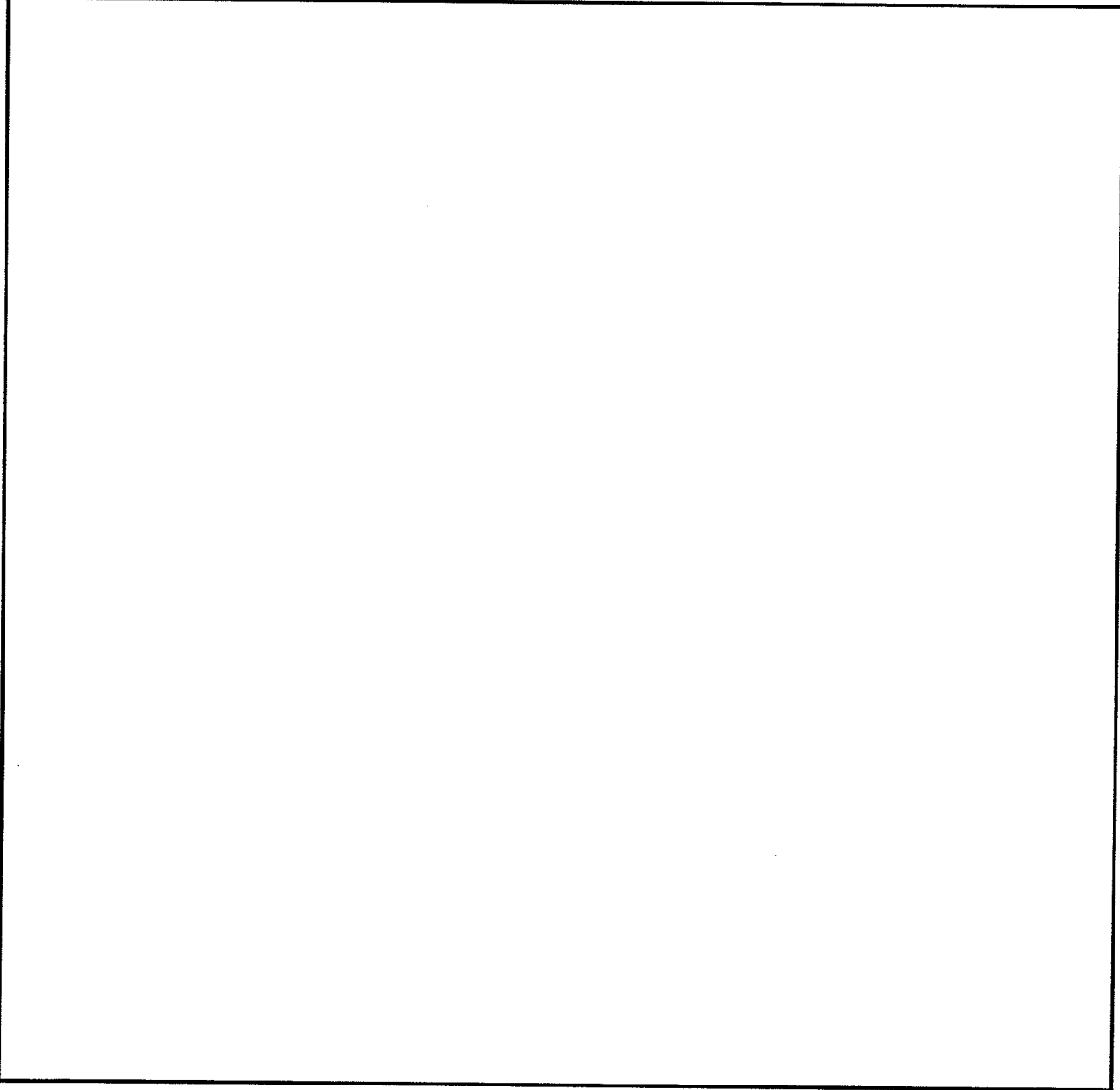
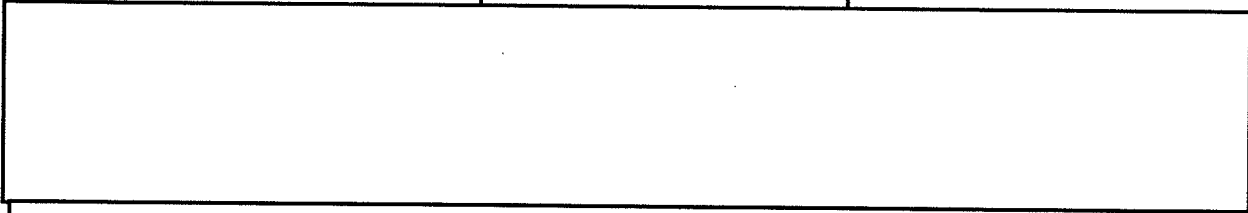
For information only.

cc: 1 - Ms. Caproni
1 - Mr. Kelley
1 - Ms. 
1 - Ms. 
1 - Mr. 
1 - Mr. 
1 - Mr. 
1 - Ms. 
1 - Ms. 
1 - Ms. 
1 - ALU Tickler
1 - ALU Library (InfP/PIA/2005)

b6
b7c

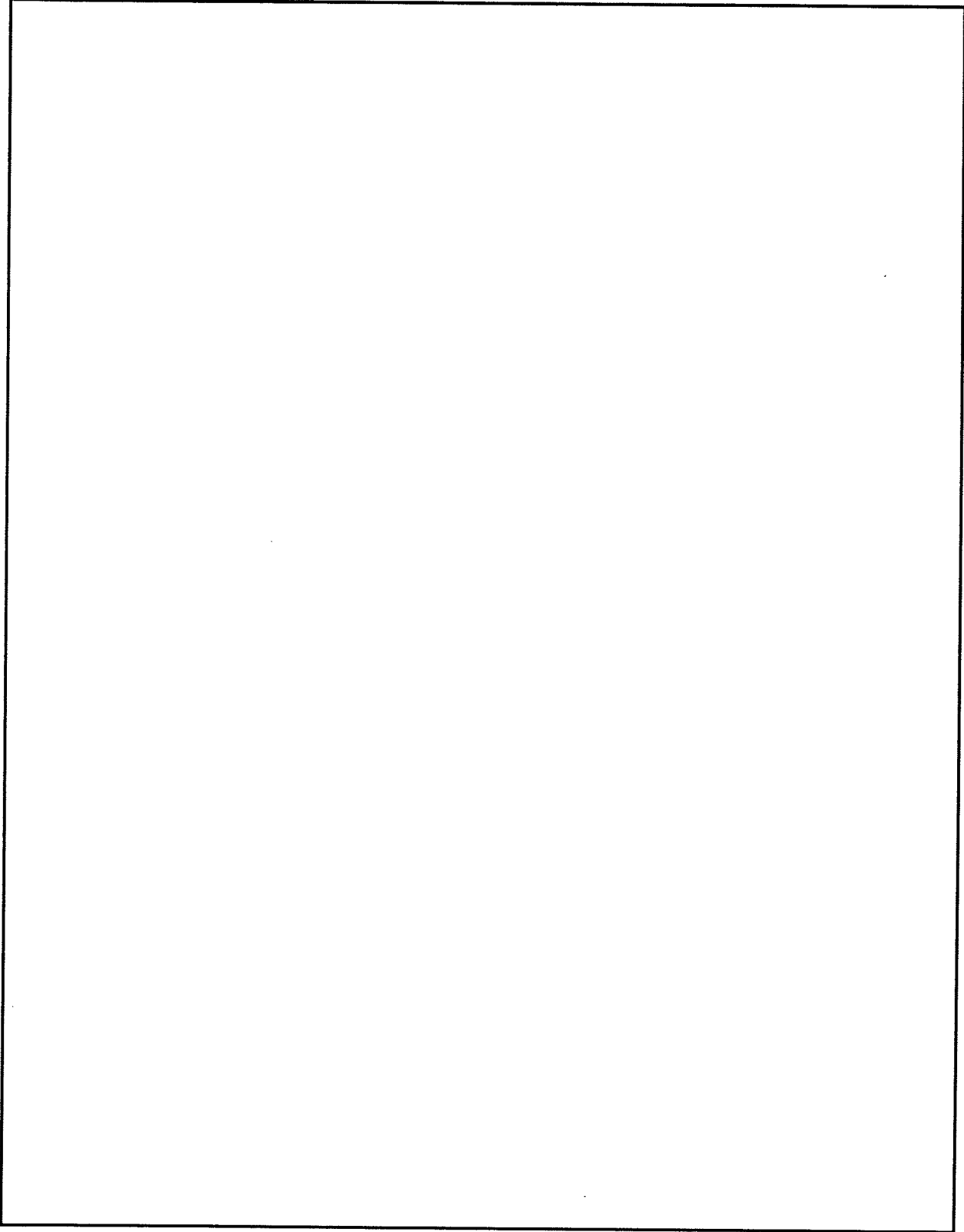
To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005

Enclosure 1
Privacy Impact Assessment



b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



b2
b6
b7C
b7E

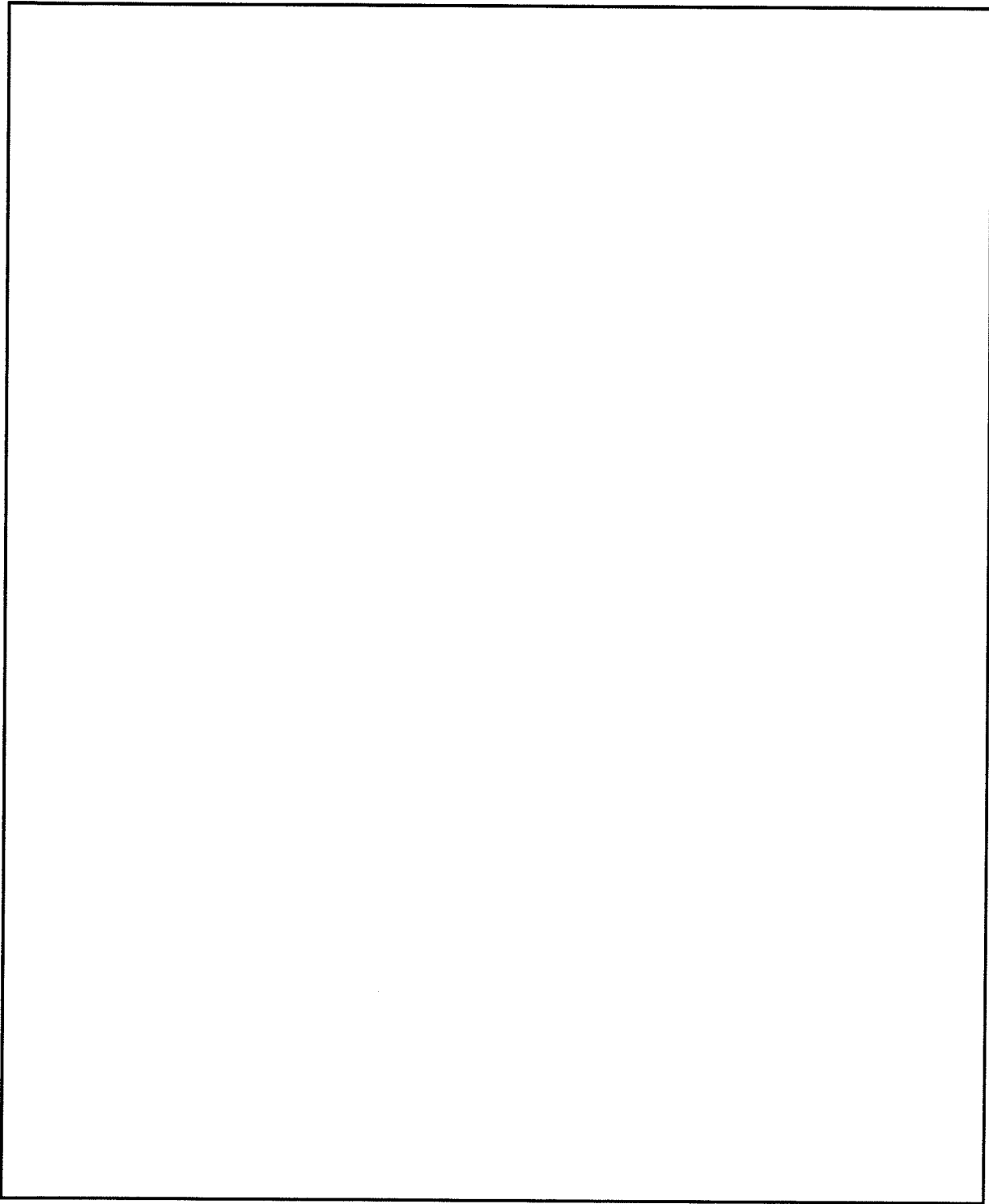
To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005

b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005

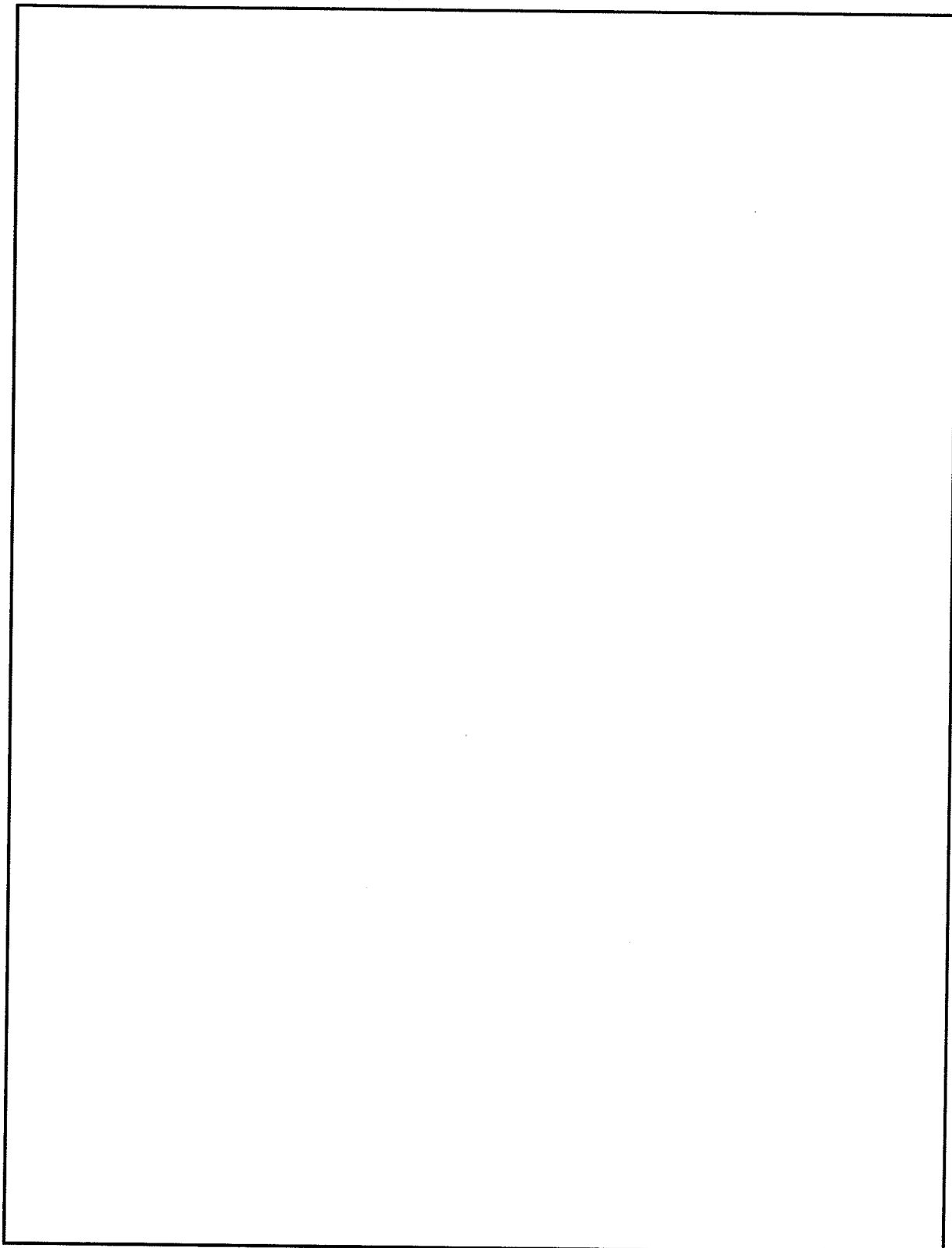
b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



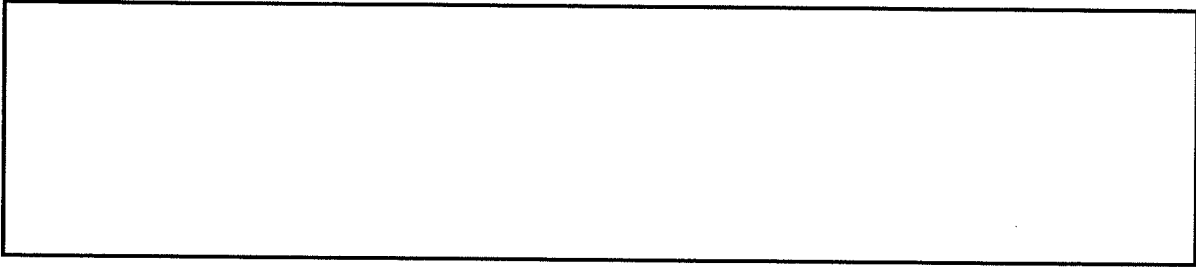
b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005

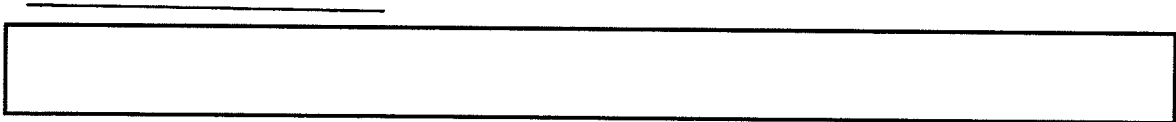


b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



b2
b7E



b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005

Enclosure 2
Request for additional data sets

Original Message-----

From: [redacted] (CTD) (FBI)
Sent: Thursday, February 17, 2005 10:54 AM
To: [redacted] (OGC) (FBI) [redacted] (OI) (OGA)
Subject: RE: [redacted]

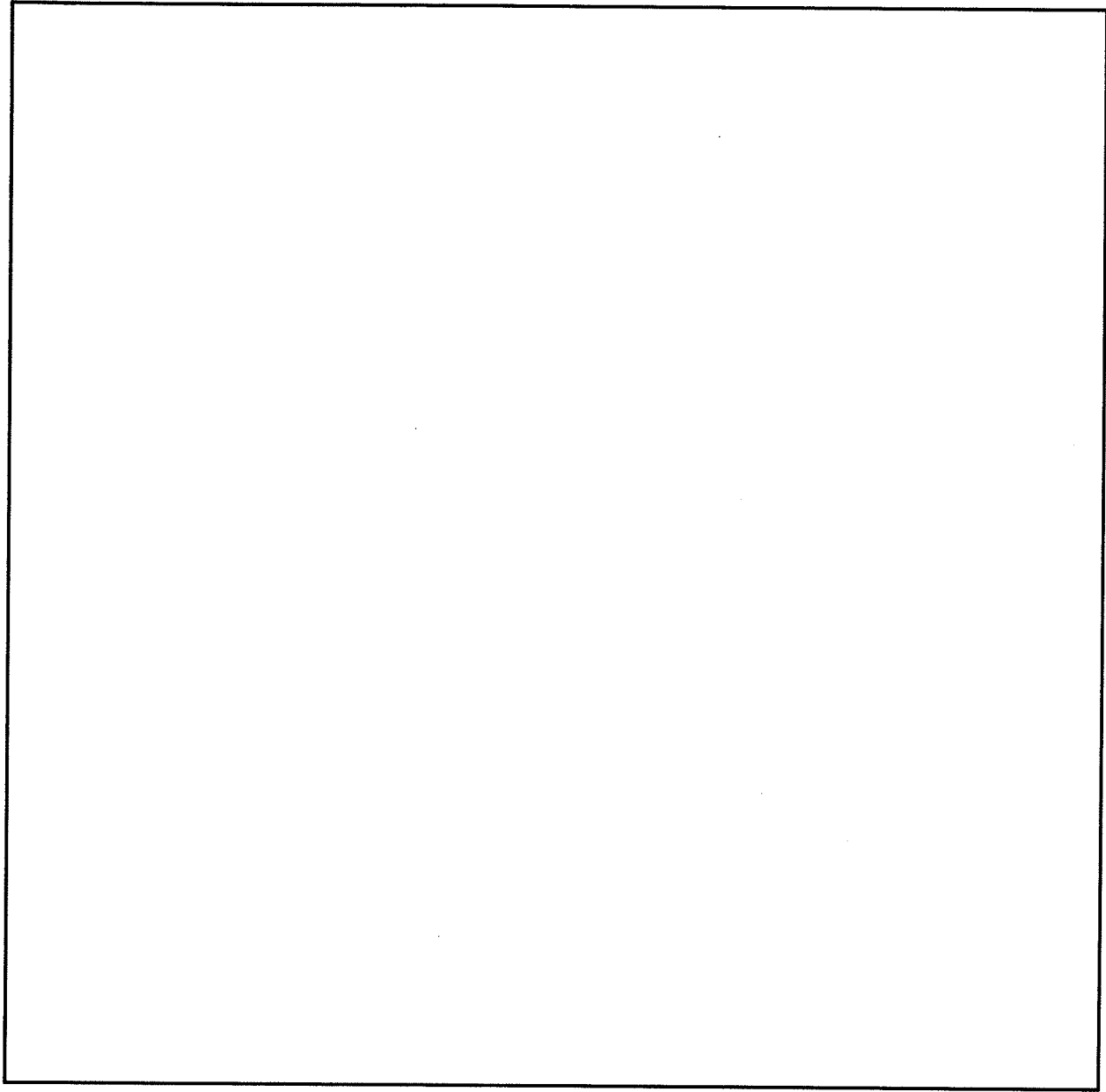
b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



b2
b6
b7C
b7E

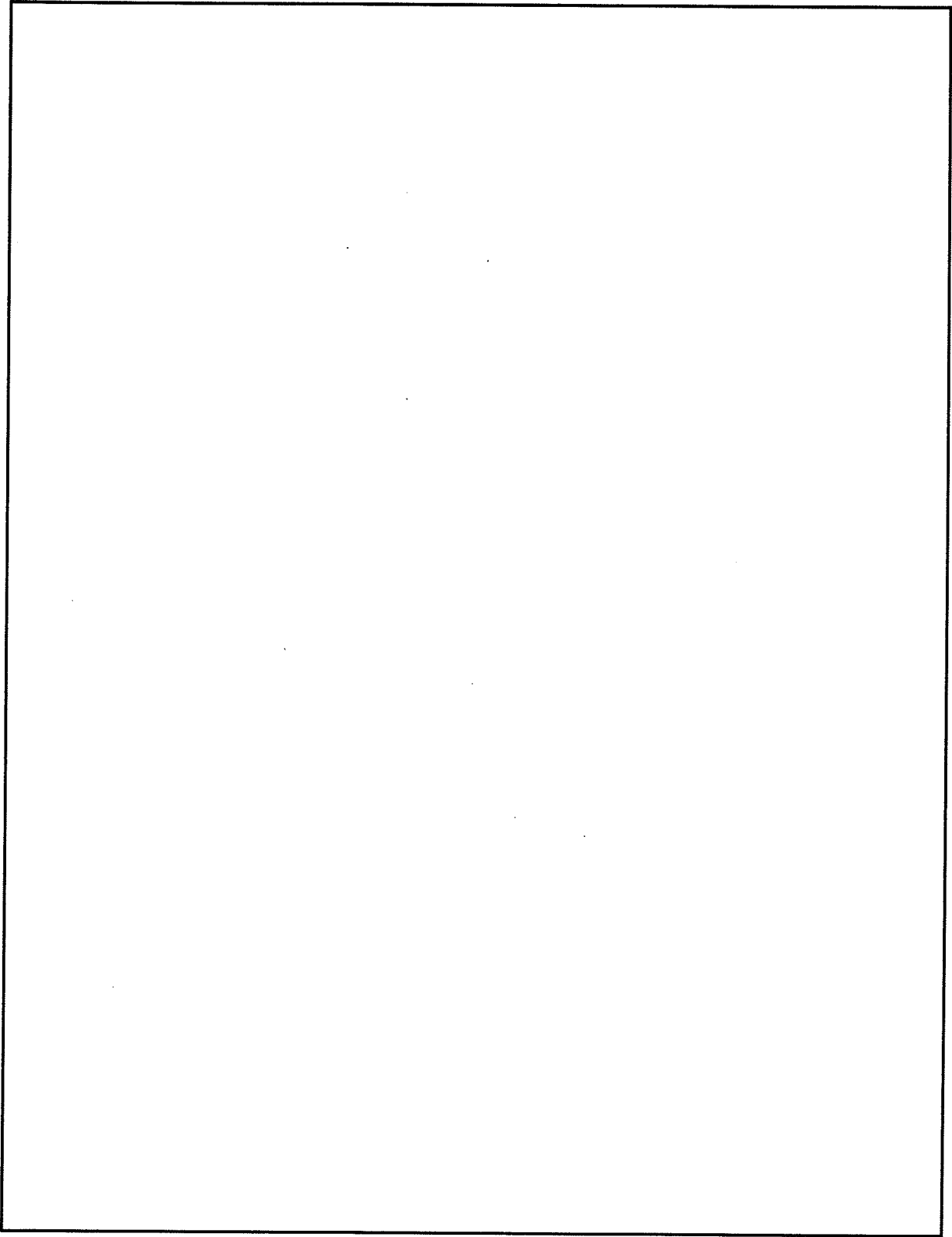
-----Original Message-----

b2
b6
b7C
b7E

From: [redacted] (OGC) (FBI)
Sent: Wednesday, February 16, 2005 1:04 PM
To: [redacted] (CTD) (FBI); [redacted] (OI) (OGA)
Subject: [redacted]

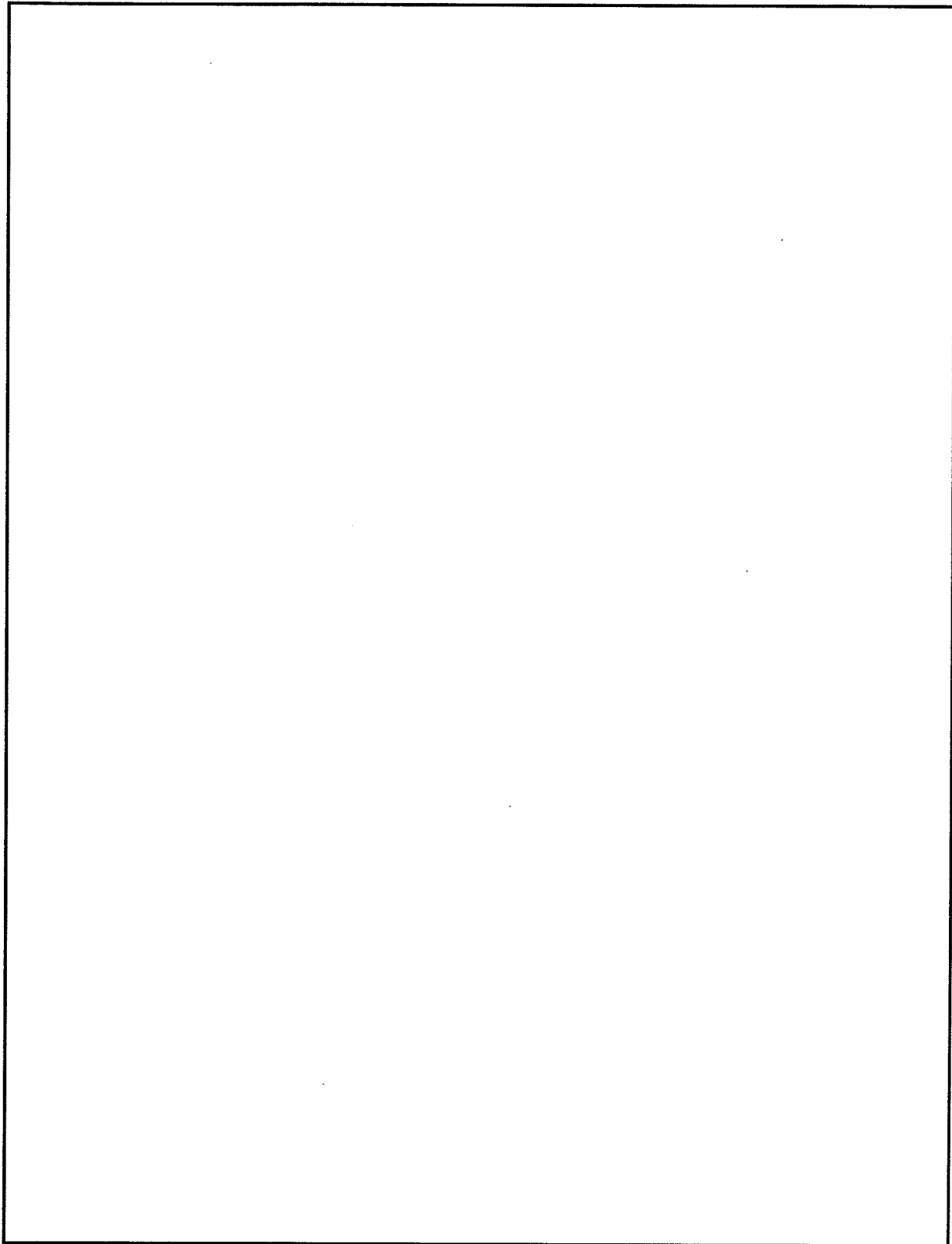
UNCLASSIFIED
NON-RECORD

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



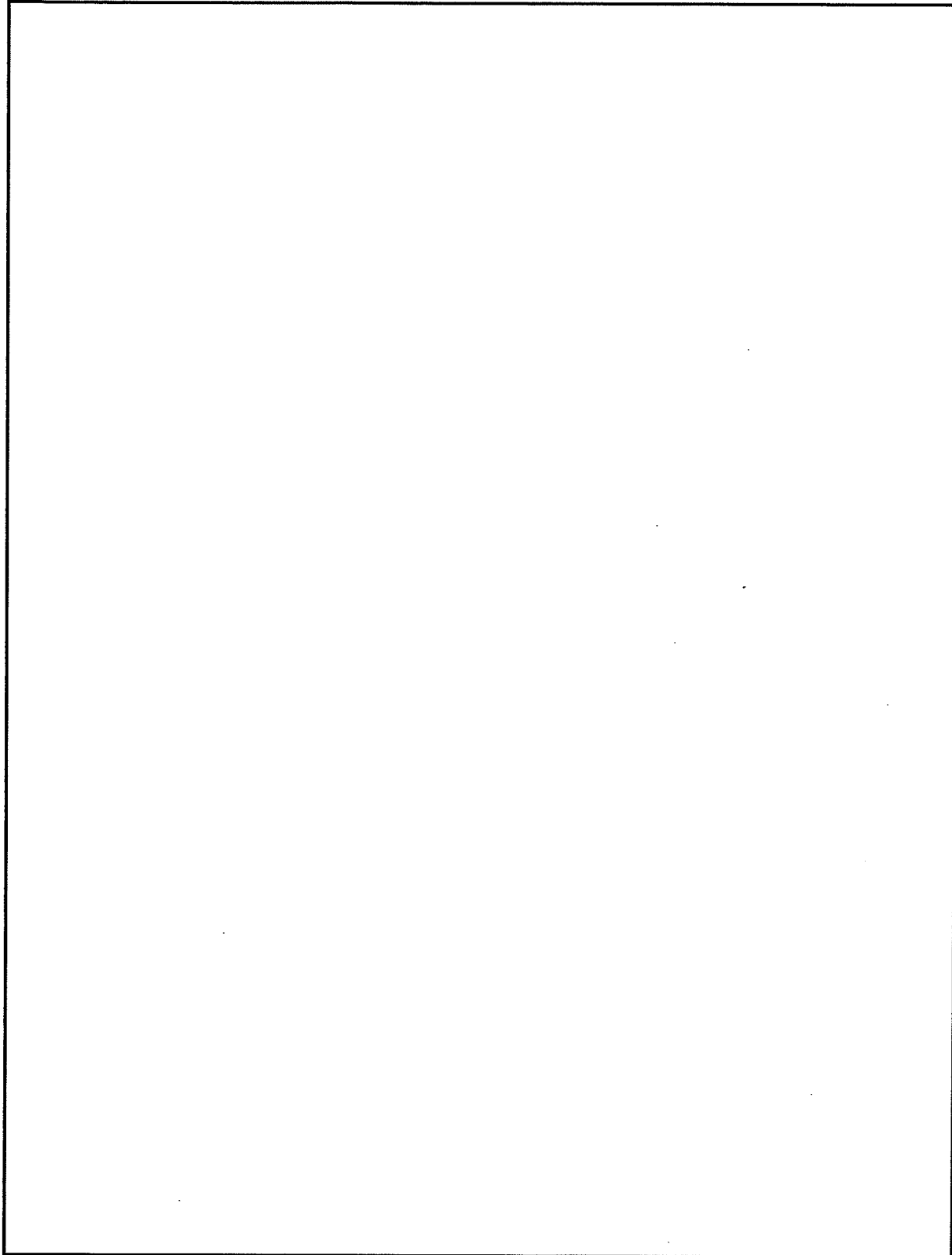
b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



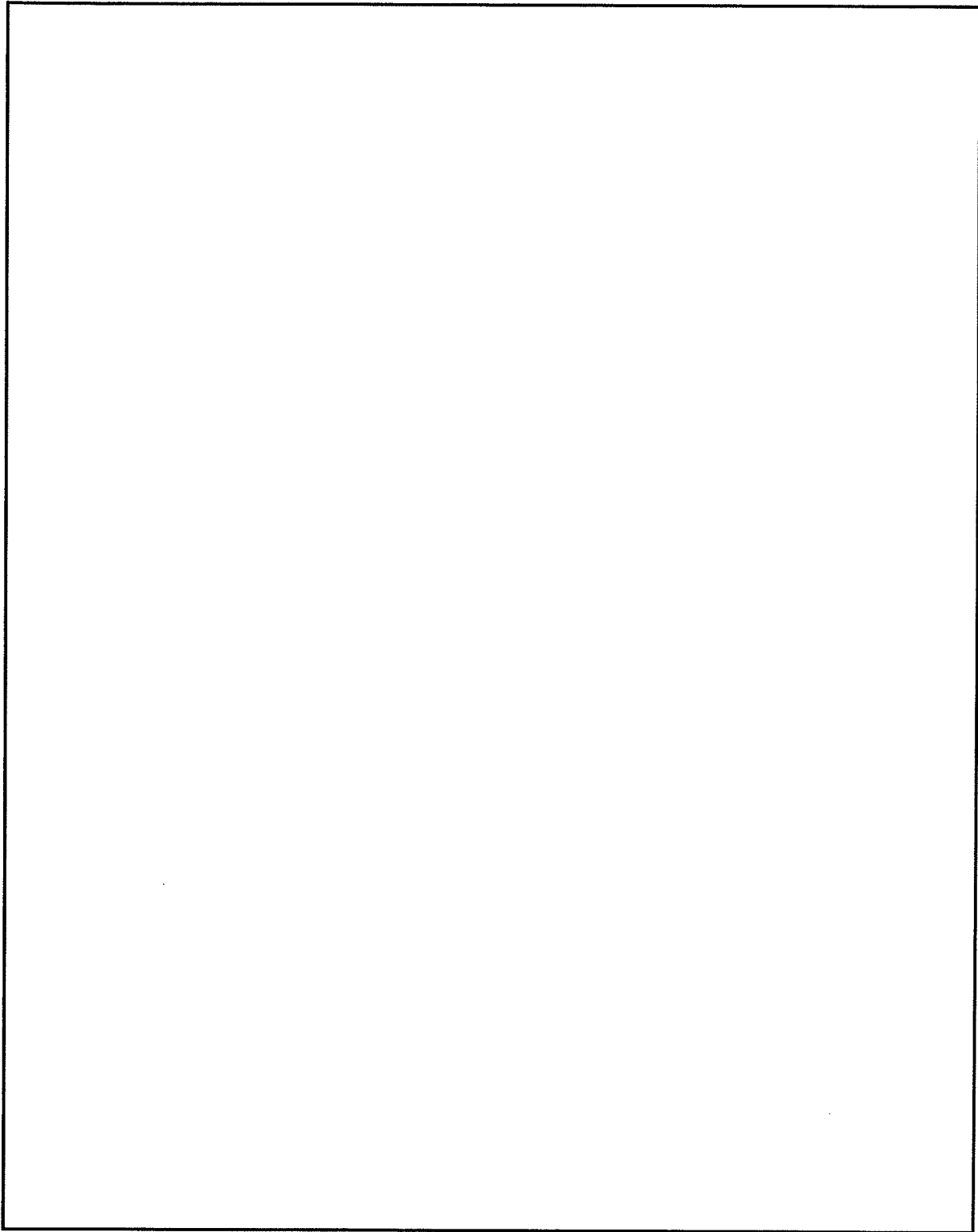
b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



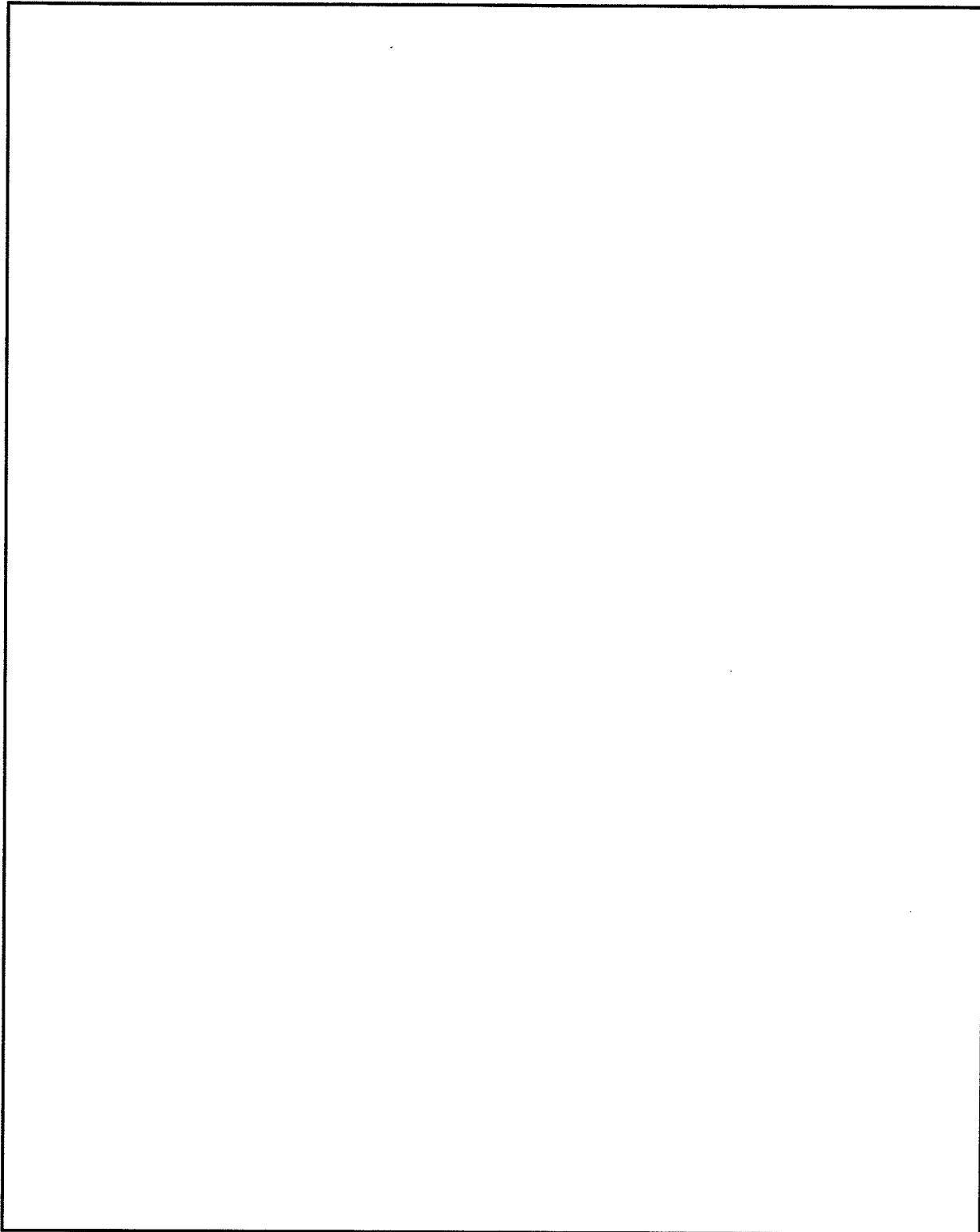
b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



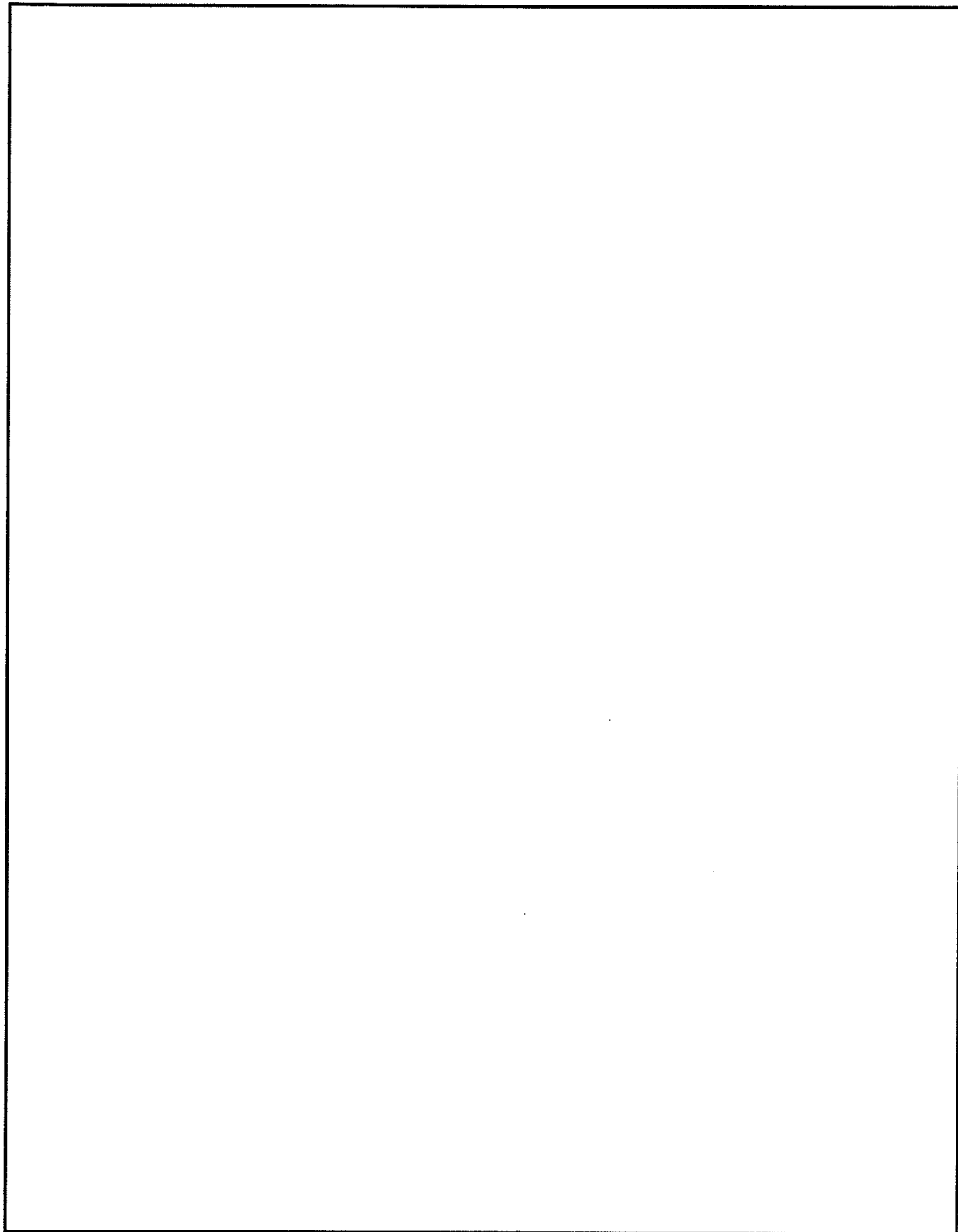
b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



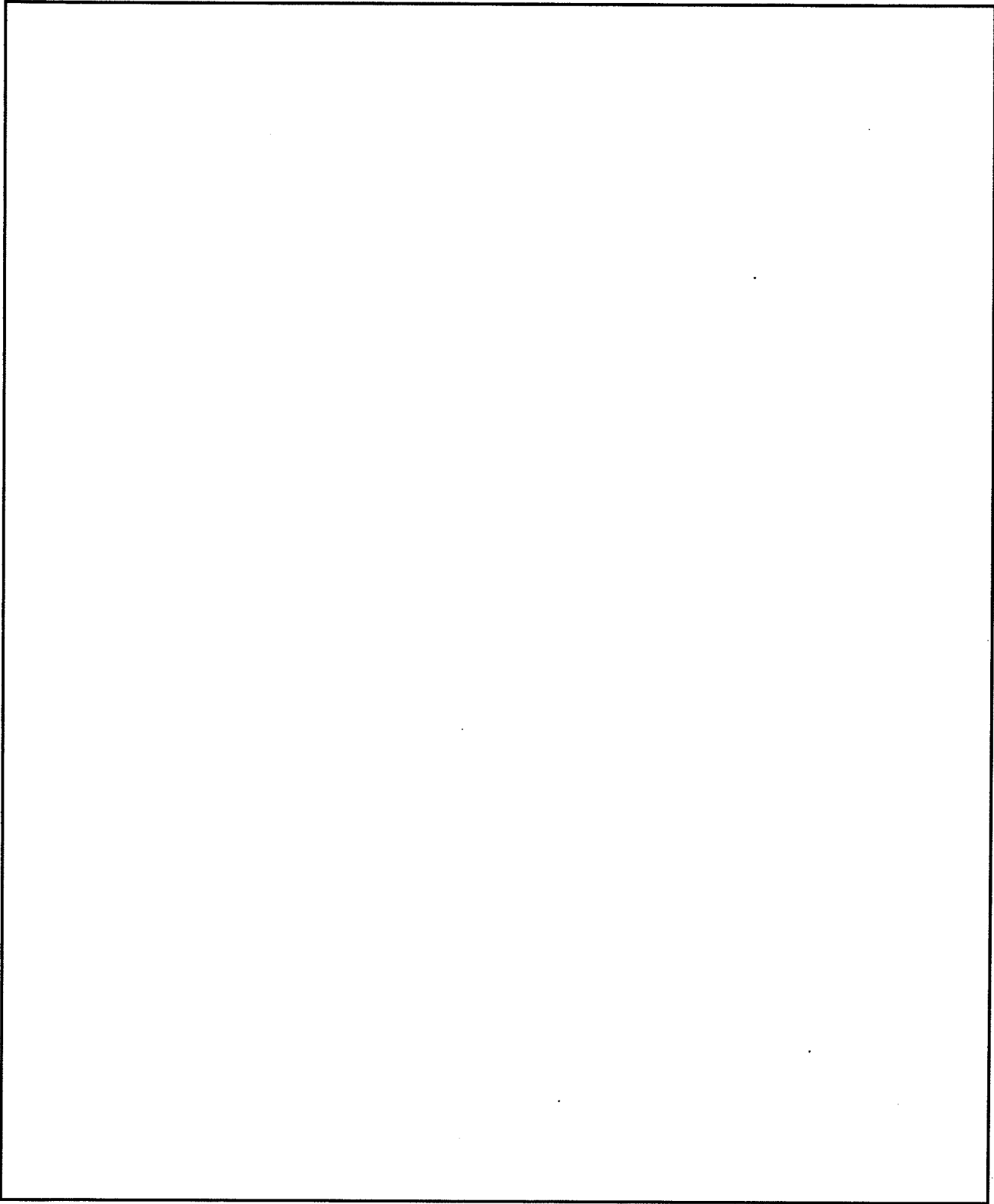
b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005

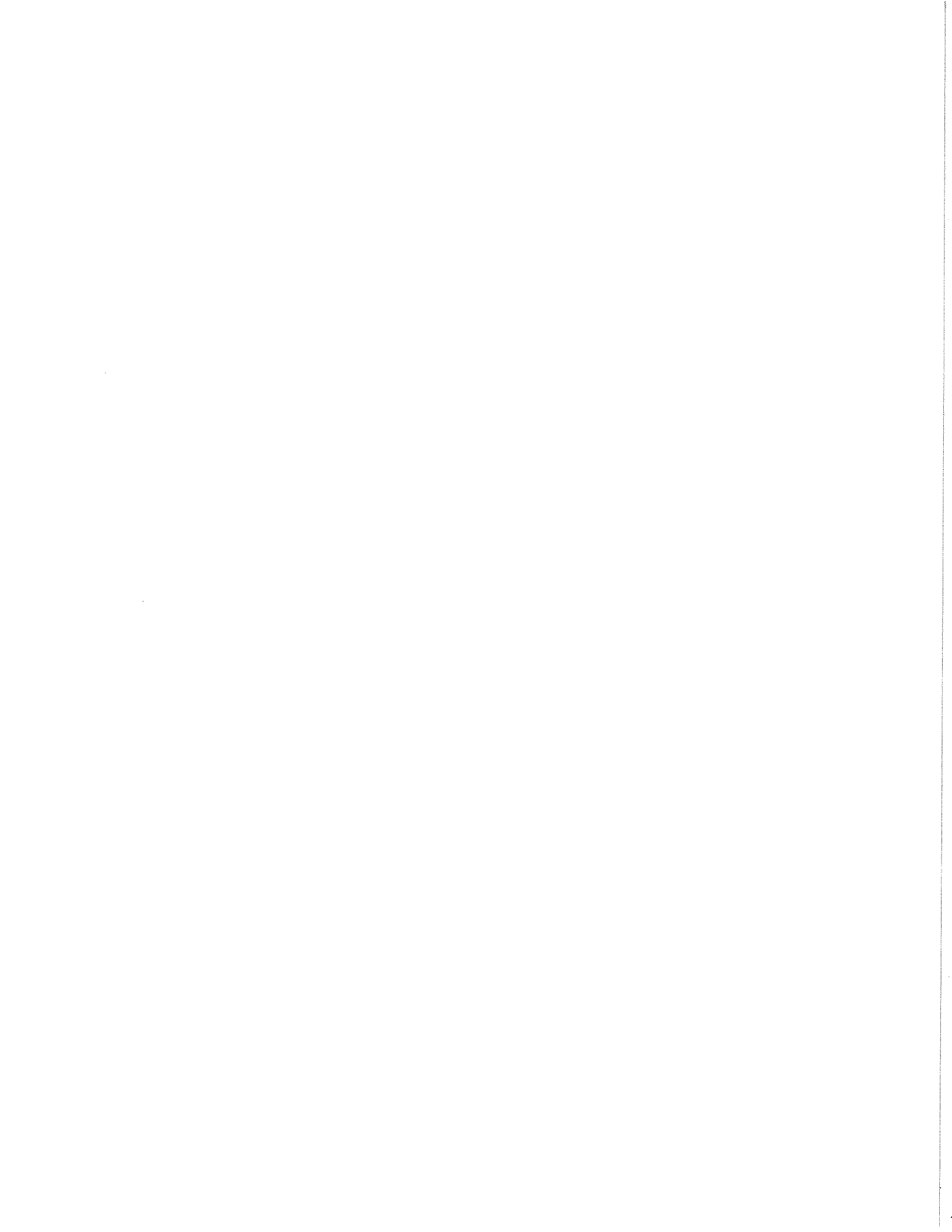


b2
b7E

To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005



b2
b7E



To: Counterterrorism From: General Counsel
Re: 66F-HQ-C1321794, 3/30/2005

b2
b7E

◆◆

~~SECRET~~

~~FOR OFFICIAL USE ONLY~~

DATE: 07-11-2007
CLASSIFIED BY 65179 DMH/BJA/CAL
REASON: 1.4 (C D)
DECLASSIFY ON: 07-11-2032

1/30/2007

IDW Data Contention and Audit Inventory for 2006 1058805

SUBJECT CASE ID	Serial	Collection	Requestor (via EC or email)	Date	ID Number	Action/Notes
281M [redacted]		ACS	[redacted]	21-Dec-06 2006-21DEC-01		4 files deleted under this case on 12/21/06
194A [redacted] 272B- [redacted]		ACS	[redacted]	20-Nov-06 2006-20NOV-01		No cases found under the 194 ID. Reclassed from 272B to a 194.
315M [redacted]	79	ACS	[redacted]	14-Nov-06 2006-14NOV-01		Removed serial 14NOV06. Removed meta data 16NOV06
332C [redacted]		ACS	[redacted]	1-Nov-06 2006-01NOV-01	332C [redacted]	removed 9 files.
65T [redacted]	2	ACS	[redacted]	31-Oct-06 2006-31OCT-01		Removed 65T's (33)
n/a		SAR	[redacted]	31-Oct-06 2006-31OCT-01A		Audited Revised SAR Losses per request.
66F [redacted]		ACS	[redacted]	23-Oct-06 2006-23OCT-01A		Provided Audits for the 2 issues.
315C [redacted]		ALL	[redacted]	29-Sep-06 2006-29SEP-01		Removed 19 doc id's per requested search terms.
101 [redacted]		SAMNET	[redacted]	27-Sep-06 2006-27SEP-01A		Blocked case id in [redacted] Index

b2
b6
b7C
b7A
b7E

~~SECRET~~

~~FOR OFFICIAL USE ONLY~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

IDW Data Contention and Audit Inventory for 2006

3150 [redacted]	1 and 4	ACS	[redacted]	11-Sep-06 2006-11SEP-01A	Provided Audit for these case id's on 28Sept06
3150 [redacted] [redacted] [redacted] [redacted]	38 and 39	ACS	[redacted]	11-Sep-06 2006-11SEP-01A	Provided Audit for these case id's on 28Sept06
		ACS	[redacted]	21-Aug-06 2006-21AUG-01	Removed from Quarantine
66F [redacted]		ALL	[redacted]	10-Aug-06 2006-10AUG-01A	No Results for requested audit.
3150 [redacted]	ALL	ACS	[redacted]	21-Jul-06:2006-21JUL-01	Removed all docs from collection on 21JUL06.
n/a		ALL	[redacted]	15-Jul-06 2006-15JUL-01A	Provided Audit for this issue.
315H [redacted] 100 [redacted] [redacted] 311A [redacted] [redacted]	ALL	ALL	[redacted]	21-Jun-06:2006-21JUN-01A	Provided audit for specific documents.
	24	ACS	[redacted]	9-Jun-06 2006-09JUN-01	Removed this document on 12JUN06
n/a		ALL	[redacted]	5-May-06:2006-05MAY-01A	Provided audit for all users and all data deletions for IDW from 31DEC06- 05MAY06 on 09MAY06.

b2
b6
b7C
b7A

IDW Data Contention and Audit Inventory for 2006

n/a	ACS	[Redacted]	17-Apr-06 2006-17APR-01A	Provided audit for issue.
(\$)		[Redacted]	2006-27APR-01 & 27-Apr-06 01A	Removed 7 documents on 28APR06 and provided requested audit on 01MAY06.
		[Redacted]	2006-27APR-01 & 27-Apr-06 01A	Removed 7 documents on 28APR06 and provided requested audit on 01MAY06.
66F		[Redacted]	6-Mar-06 2006-06MAR-01A	Provided audit for issue.

b2
b6
b7C
b1
b7A

1058805

The data expungement and corrective actions processes that are utilized by IDW are identified in the Investigative Data Warehouse–Secret Version 1 (IDW-S V1) *Data Administration Manual (DAM)*, Version 0.6, 23 DEC 2005, Section 4, as excerpted below.

For files that are unauthorized due to classification issues, the following process applies.

4. IDW-S Data Security Administration

As noted earlier, the IDW-S system is authorized to hold and process national security data classified up to and including Secret. The IDW-S system is not authorized to process any Top Secret data nor any Sensitive Compartmented Information (SCI). To ensure that IDW-S contains only data for which it is authorized, all data received by IDW-S is subjected to an automated process of [redacted]

[redacted]

b2
b7E

[redacted]

b2
b7E

[redacted] The procedure for deleting individual files from IDW-S is provided below.

[redacted]

b2
b7E

[redacted] The procedure for secure deletion of individual files [redacted] is also provided below.

These process are also outlined in the Federal Bureau of Investigation (FBI) Investigative Data Warehouse (IDW) *System Security Plan*, Version 2.0, dated May 31, 2006, Section 3.1.3.

For files that are unauthorized due to categorization or content issues, the following process applies.

4.1 Deleting Individual Files from IDW-S

In spite of the many precautions taken, it can occur that data for which IDW-S is not authorized is ingested into IDW-S. When such data is discovered on IDW-S it is necessary to delete this data and to update the Document Tracking Database with the appropriate "DEL" status for the file. For this purpose [redacted]

[redacted] was created. There are three usages for [redacted]

b2
b7E

- Usage 1: [redacted]
- Usage 2: [redacted]
- Usage 3: [redacted]

where

- [redacted] is the option to create a "delete file" full filename(s) and filepath(s) of the files to be deleted.
- [redacted] is a text file containing the IDW Document ID's [redacted] of the files to be deleted.
- [redacted] is the option to delete all files with the given IDW Document ID's from the filesystem and to update the Tracking Database with the appropriate "DEL" status for the files.
- [redacted] is the name of the "delete file" containing the full filename(s) and filepath(s) of the files to be deleted. The [redacted] is created in the same filepath as the [redacted]. The format of [redacted] is [redacted]
- [redacted] is an option to update the Tracking Database with "DEL" status for the files but not to perform a delete action on the files. This option is provided for the case where the files have been previously (e.g., manually) deleted off the filesystem.

b2
b7E

b2
b7E

b2
b7E

Note that these three usages enable two modalities with respect to deleting files off of IDW-S:

- Mode 1: Usage 1 followed by Usage 2 deletes files with the IDW Document ID's specified in [redacted] from the filesystem updates the Tracking Database with the appropriate "DEL" status for the files.
- Mode 2: Usage 1 followed by Usage 3 updates the Tracking Database with "DEL" status for the files specified in [redacted]. This mode is used to reconcile the Tracking Database when the files have been previously (e.g., manually) deleted off the filesystem.

b2
b7E

When executed [redacted] reads the IDW Document ID values in [redacted] and for each IDW Document ID the program:

b2
b7E

- Retrieves the filename and filepath from the Tracking Database.
- Generates a batch ID and updates the [redacted] field of the [redacted] table in the Tracking Database with this batch ID.
- Inserts a new DEL event into the [redacted] table in the Tracking Database.
- Enters the notation "Security Delete" into the [redacted] field of the [redacted] table in the Tracking Database.

b2
b7E

b2
b7E

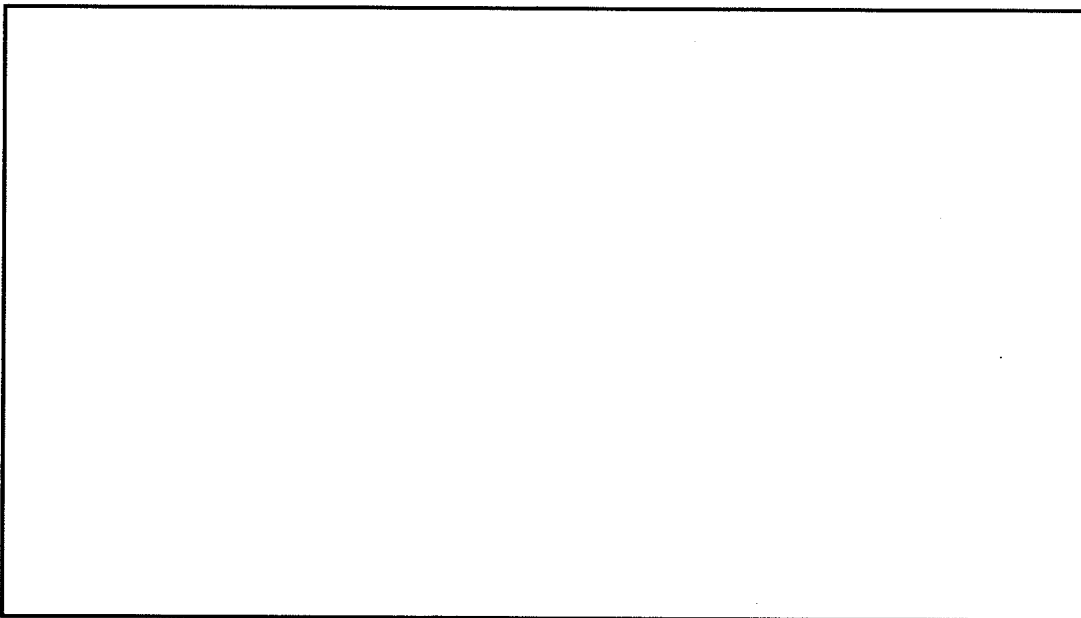
A log file that captures the file deletions and database update actions of [redacted] is created in the location [redacted]

b2
b7E

Auditing:

Specific auditing procedures and requirements are identified in the Federal Bureau of Investigation (FBI) Investigative Data Warehouse (IDW) *System Security Plan*, Version 2.0, dated May 31, 2006, Section 7.6.

IDW-S employs a combination of operating system, network, and application level auditing to record authorized activities and to detect and audit unauthorized system behaviors. All systems perform routine auditing of system and application level security events. Other commercial applications are used by IDW to enhance auditing and monitoring capabilities. Furthermore, specific application auditing provides final correlation of user-to-object access.



b2
b7E

Audit reports can be customized and provided upon request.



Congressional Affairs Office Congressional Contacts

Date Entered: 05/21/2004 Briefing Hearing Other

2004-736 Event Date: 5/12/2004

Subject: National Research Council Report

CAO Contact Person: _____

DOJ Notification: _____ DOJ Date/Time: _____

FBI Participants: CIO Zai Zami

Other Participants: _____

Committees /Subcommittees: HPSCI

Members/Staff: staff: Bob Myhill, Patrick Kelly, Mike Fogarty

Details of Briefing:

Zai advised that the NRC report is outdated and that the NRC would be producing a new, updated report to reflect the changes which the FBI has made to its information technology. He said that the NRC reps did not allow the FBI to respond to the findings before releasing the report. Zai discussed what IDW does (currently 9 data sources - analysis across these data sources) versus VCF (data flow and data generation). In response to Bob's question about who is responsible for enterprise architecture coordination within the IC, Zai said Alan Wade (overall) coupled with 5 working groups.

Follow Up Action:

108th

b6
b7C



Congressional Affairs Office Congressional Contacts

Date Entered: 01/14/2005 Briefing Hearing Other FOC

2005-1 Event Date: 1/13/2005

Subject: VCF Status Briefing for Senate Select Committee on Intelligence (staff only)

CAO Contact Person: SSA [redacted]

DOJ Notification: None DOJ Date/Time: [redacted]

FBI Participants: CIO Zalmay Azmi (Briefer), AD Eleni Kalisch, SSA [redacted] (OCIO)

Other Participants:

Committees /Subcommittees: Senate Select Committee on Intelligence

Members/Staff: [redacted]

b6
b7C

b6
b7C

b6
b7C

Details of Briefing:

[redacted]

This is compared to IDW which is a warehouse containing 47 databases (including ACS) which also can be searched for data (including paper files).

OTHER

O/S

[redacted]

Follow Up Action:

None

109 *th*



Congressional Affairs Office

Congressional Contacts

Date Entered: 02/02/2005 Briefing Hearing Other FOC

2005-21 Event Date: 2/1/2005

OTHER O/S

Subject: IDW [redacted]

CAO Contact Person: [redacted]

b6
b7C

DOJ Notification: [redacted] DOJ Date/Time: [redacted]

FBI Participants: Zal Azmi [redacted] (ACS demo) [redacted]

Other Participants: [redacted]

b6
b7C

Committees /Subcommittees: House Appropriations

Members/Staff: [redacted]

Details of Briefing:

The staff were provided a demo and briefing on IDW and ACS. [redacted] conducted the IDW presentation/demo. He provided details on the sources of information contained in IDW, # of users (currently 6,000), plans for expansion, # of databases (47), privacy issues, mou(s) regarding information sharing with other federal agencies, states and local entities. [redacted] asked if DEA phone application information was contained in IDW. Answer: no due to security issues. A general discussion was held regarding the possibility of creating new IDWs for other crime problems/initiatives. [redacted]

b6
b7C
OTHER O/S

Follow Up Action:

[redacted]

OTHER O/S



Congressional Affairs Office Congressional Contacts

Date Entered: 05/19/2005 Briefing Hearing Other FOC

2005-178 Event Date: 5/20/2005

Subject: [Redacted]

CAO Contact Person: SSA [Redacted]

DOJ Notification: [Redacted] DOJ Date/Time: 1:00:00 PM

FBI Participants: SC Mike Morehart (TFOS) [Redacted] (TFOS, observer)

Other Participants:

Committees /Subcommittees: House Committee on Financial Services, Subcommittee on Oversight and Investigation

Members/Staff: [Redacted]

Details of Briefing:

[Redacted]

b6
b7C
OTHER O/S
b2
b7E

Follow Up Action:

[Redacted]

b6
b7C
OTHER O/S

b2
b6
b7C
b7E



Congressional Affairs Office Congressional Contacts

Date Entered: Briefing Hearing Other FOC

OTHER O/S

Event Date:

Subject:

b6
b7c

CAO Contact Person: SSA

DOJ Notification: DOJ Date/Time:

FBI Participants: SC Mike Morehart, TFOS, UC and SSA

Other Participants:

Committees /Subcommittees:

Members/Staff:

Details of Briefing:

and provided overview about IDW. Discussed information ingested by IDW and how said information is utilized. Discussed how all info is vetted through Privacy Impact and OGC. Then provided real time examples of data mining. There was discussion about the need to expand the system and how it currently hosts 41 million datasets. Discussion on awaiting financing to increase the system to ingest 71 million more data sets.

OTHER O/S

Follow Up Action:



Congressional Affairs Office Congressional Contacts

Date Entered: 08/01/2006 Briefing Hearing Other FOC

2006-721 Event Date: 5/22/2006

Subject: IDW

CAO Contact Person:

DOJ Notification: DOJ Date/Time:

b6
b7C
OTHER O/S

FBI Participants:

Other Participants: CRS

Committees /Subcommittees: at the direction of House Approps SSJC

Members/Staff: not present

Details of Briefing:

IDW background and demonstration; users and availability; weaknesses and improvements needed; data composition; cooperation with outside agencies and DNI; intelligence products; Beta version; batch queries; training; financial resources.

OTHER O/S

Follow Up Action:

OTHER O/S



Congressional Affairs Office Congressional Contacts

Date Entered: 09/13/2006 Briefing Hearing Other FOC

2006-805 Event Date: 9/12/2006

Subject: [Redacted]
 CAO Contact Person: SSA [Redacted]
 DOJ Notification: [Redacted] DOJ Date/Time: [Redacted]
 FBI Participants: None
 Other Participants: [Redacted]
 Committees /Subcommittees: Senate Banking, Housing and Urban Affairs
 Members/Staff: Shelby, Hagel, Martinez, Allard

b6
 b7C
 OTHER O/S

Details of Briefing:

[Redacted]
 [Redacted] also made reference to a presentation he received from the FBI concerning IDW and how the FBI was able to link information received [Redacted] to subjects of ongoing criminal and terrorist investigations.

b2
 b6
 b7C
 b7E

Follow Up Action:

**Responses of the Federal Bureau of Investigation
Based Upon the August 19, 2004 Hearing Before the
Senate Committee on the Judiciary
Regarding "The 9/11 Commission and Recommendations
for the Future of Federal Law Enforcement and Border Security"**

Questions Posed by Senator Hatch

1. The 9/11 Commission has recommended that the position of deputy National Intelligence Director ("NID") for homeland intelligence be filled by either the FBI's executive assistant director for intelligence or the under secretary of homeland security for information analysis and homeland protection. Do you think this recommendation - by failing to specify precisely which official should hold the position - may create an unnecessary conflict between the FBI and the Department of Homeland Security ("DHS")? More generally, do you believe the FBI Office of Intelligence and the DHS Directorate for Information Analysis and Infrastructure perform similar functions, such that the heads of those entities would be interchangeable in the role of a deputy NID?

Response:

The FBI believes the Director of National Intelligence (DNI) should have one principal deputy. We believe the spirit of the 9/11 Commission recommendations can be better achieved through an intelligence coordinating council made up of NSC/HSC principals.

2. You have served in leadership positions within two different components of the Intelligence Community, the National Security Agency and the FBI. Moreover, you have had an opportunity to view the cooperation, or lack of cooperation, among intelligence agencies at the highest levels. If the 9/11 Commission's recommendations are adopted, you could end up serving as a deputy to the NID, as well as reporting to the FBI Director. Based on your experiences, do you think this type of "dual-hatting" can work? In your opinion, are there any conditions that might improve the likelihood of a successful merger of your potential NID and FBI roles?

Response:

We do not think a "dual-hatting" approach is the best answer. We are concerned about dual-hatting deputies who already have full time jobs, we may be replicating the situation underscored by the 9/11 Commission of intelligence community leaders having "too many jobs." In addition, maintaining the operational chain-of-command authority within the agencies that have the

to improve oversight of IT projects, to strengthen oversight of IT contracts, and to ensure that IT investments fully support the FBI's current and future missions.

c. What is the current projection for the final, total cost of the project?

Response:

It is too early to estimate the total cost of the program.

6. John Brennan, the Director of TTIC, testified on August 23, 2004, about the need to build an integrated information technology architecture, accessible to all members of the intelligence community. Do you agree? How would VCF or the Integrated Data Warehouse fit into this new architecture?

Response:

We agree with the need to build a government-wide integrated information architecture as outlined in the President's Executive Order entitled Strengthening the Sharing of Terrorism Information to Protect Americans. In the FBI's work processes, VCF, or its successor software, will be ingest tools (like the Automated Case Support system is now) for the Investigative Data Warehouse (IDW). VCF or its equivalent will be the first point of ingest for investigative and intelligence information and for records collected by Agents and others. IDW then allows the data to be accessed, analyzed, and used in the production of intelligence. IDW minimizes the compartmentalization of intelligence and/or terrorism-related data developed by the FBI and would fit within this new architecture. It would also allow the interchange between agencies, with the proper security and access controls necessary to protect methods and sources.

7. I understand that, after many millions of dollars spent, FBI agents now have the capability of e-mailing each other over a secure network. But I also understand that many field agents are still unable to send secure e-mails to other federal government agencies, or to state and local law enforcement and other entities outside the FBI. Is that true? If so, why does the FBI lack this basic capability, and what if anything is being done about it?

Response:

The FBI is faced with a unique challenge every day. Unlike other law enforcement agencies, we are responsible for communicating with the IC, other federal agencies, and our state and local partners in regional jurisdictions as it relates to our intelligence, counterterrorism prevention and criminal investigative responsibilities. This levies an enormous challenge on our IT resources and staff

The Inspection Division then obtained a copy of the Zyindex database from the OKBOMB investigation, which contained 167,000 documents, and obtained a comparison of the 15,200 documents from the "I" drive tapes, the 167,000 OKBOMB documents, and the documents in the FBI's Automated Case Support system. This comparison identified 891 questionable documents.

A CD-ROM containing the 891 questionable documents was forwarded to the Oklahoma City Division. Based on their knowledge of the documentation provided pursuant to the OKBOMB discovery process, the Oklahoma City Division was asked to determine whether any of these documents that should have been made available for discovery had, in fact, not been provided to the OKBOMB defense team.

The Oklahoma City Division advised that, of the 891 questionable documents, only four had not previously been reviewed by members of the OKBOMB Task Force. Two of the documents were first drafts of FD-302s that were later changed so they could be uploaded to the FBI's Automated Case Support system; one document was an FD-71 complaint form that mentioned OKBOMB and was generated by the Denver Division; and the fourth document was unidentifiable.

c. Were the existence and potential problems caused by the "I-drive" reviewed by the 9-11 Commission?

Response:

While the 9/11 Commission Report does not address the FBI's "I" drives, the 9/11 Commission did review the FBI's data automation and technology processes, finding its information systems "woefully inadequate" during this period (page 77 of the Commission's report).

d. Can analysts access data and documents on the "I-drive" through the Integrated Data Warehouse? If not, why not, and do you plan for this to change.

Response:

The purpose of the Integrated Data Warehouse (IDW) is to facilitate the analysis of data that has been collected and documented by FBI employees. While the IDW will utilize the FBI's network architecture to facilitate the analysis and sharing of data in FBI systems, it will not "see" or pull in data from the "I" drive. This is appropriate because the purpose of the "I" drive is to facilitate the mobility of the FBI's workforce by allowing employees to access their work-in-progress from any computer connected to the FBI network, and documents that have not been reviewed or approved by supervisors may contain inaccurate or incomplete

information. If this information were made available to all analysts, they would risk the possibility of reaching incorrect conclusions based upon unverified data. Once a document is approved, it is uploaded into the FBI's Automated Case Support system, from which information is retrievable and searchable by all employees. Except as described in question 11c, below, these documents could then be accessed by analysts through the IDW.

e. Will the "I-drive" still exist once VCF is implemented? Please explain.

Response:

The "I" drive is a networked computer drive that allows computer users to retrieve items that they are working on from any computer connected to the network. This type of network architecture facilitates the mobile nature of the FBI's workforce, while providing the appropriate security for information and intelligence gathered by the FBI. These network drives are not designed as repositories of information; they are designed to facilitate work that is in progress.

Because VCF, or its successor software, will permit documents to be drafted, reviewed, verified, and approved by supervisors within the workflow process defined by that software, the current use of the "I" drive will no longer be required after that software is deployed. Even then, however, networked drives that allow FBI employees to access their work in progress from any networked computer will still be a necessary part of the FBI's Enterprise Architecture. Consequently, while these shared drives may be called "I" drives or may use some other naming convention, shared drives will continue to have utility in the FBI, though for different purposes than the "I" drive is currently used.

11. During your testimony, you said that "case files" were included in the Integrated Data Warehouse (IDW). It is my understanding that FBI case files include documents such as FD-302's (interview memoranda), electronic communications, documents obtained by the FBI in the course of an investigation (and filed in "1A" envelopes with the case file), transcripts of wiretap recordings, as well as other materials.

a. Please confirm that these items are included in a typical FBI "case file" and explain what, if any, other types of documents or materials are kept in a "case file."

Response:

The above listed items are kept in a case file. In addition to electronic communications (ECs), FD-302s (Form for information that may become testimony), and transcripts, other types of data stored in a case file include

Facsimiles, FD-542s (Investigative Accomplishment Reports), Inserts, Teletypes, Letter Head Memorandums (LHM), Memorandums, and other miscellaneous documents.

b. Are all of these items accessible through the IDW?

Response:

Except for those items described below in item (c), all of these items are accessible through IDW.

c. What if any documents or materials kept or maintained in an FBI "case file" are *not* accessible in IDW, and why? Please be specific.

Response:

Most, but not all, electronic documents or materials kept in an FBI case file are accessible through IDW. A small number of case file documents that identify specific types of data too sensitive for all IDW users are not accessible through IDW. For example, information that reveals the identities of informants, information on public corruption investigations, and some administrative "case files" such as FBI employee disciplinary actions would not be accessible.

Prior to September 11, 2001, information in case files was primarily restricted to agents directly involved with the respective cases. Following September 11, 2001, Director Mueller established an "open data" policy, which permitted FBI analysts to access all data in FBI systems, with the exception of the most sensitive files identified by the EAD for Counterterrorism/Counterintelligence. This policy change allowed counterterrorism analysts to make more effective use of the FBI's collected data.

In accordance with the "open data" policy, the IDW system allows users to access all data in the system, although "need-to-know" principles still apply. The restrictions described above are intended to protect the FBI's most sensitive data from threats such as that posed by Robert Hanssen. To further protect against this type of threat, IDW audits all user activity.

As is further described in part (d) below, the FBI is aggressively developing a more advanced security system that would allow all documents to be included in

the data warehouse, with strict protections applied to the most sensitive documents.

In order to ensure that FBI policies create the most effective counterterrorism environment possible, Director Mueller established an Information Systems Policy Board that is charged with reviewing existing policies, modifying policies when necessary, and establishing new policies as needed to respond to a changing environment.

d. For any documents or materials not accessible through IDW, please detail how the FBI currently searches for data in such documents or materials, and how or whether the search is conducted differently today than it was prior to September 11, 2001. For documents not currently accessible in IDW, when will the FBI will be able to access such materials electronically?

Response:

The documents not available through IDW are currently accessed through their original sources' systems, as they were prior to September 11, 2001. However, the access rules applied to these systems have changed in response to the events of September 11 to provide greater access and enhanced auditing features. This provides a greater ability to locate and disseminate data than the FBI had prior to September 11, 2001.

The FBI is actively working on a project based on the IDW system that will add a more robust security layer, which includes the detailed discretionary access controls required for the FBI's most sensitive files. The FBI anticipates completion of the testing and evaluation of the new technology in the summer of 2005. If additional funding is secured, the FBI will initiate the process of loading the excluded documents described in part (c) above into the system with appropriate protections. Access will then be expanded to the full user base of IDW.

e. Is it true that IDW access to materials in an FBI "case file" is limited to only that information that has been typed by an agent or support personnel into an FD-302 or other report?

Response:

This is not true. There is a great deal of information in IDW other than that which has been typed by an agent or support personnel into an FD-302 or other report. With only the exceptions described in part (c) above, users have access to all electronic data that is stored in ACS, as well as other paper records which have