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

[redacted]

b2
b7E

[redacted]

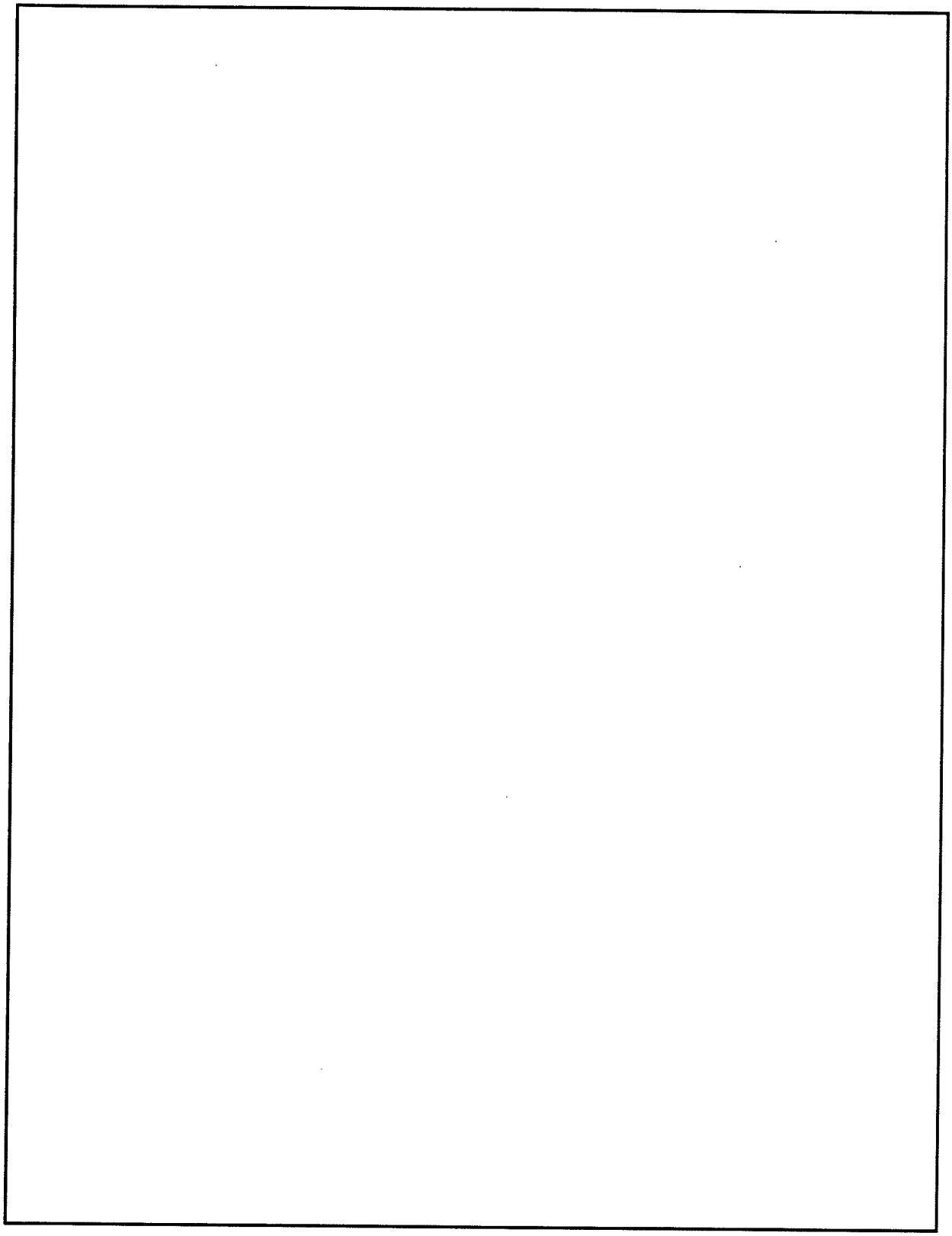
b2
b6
b7C
b7E

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

b2
b6
b7C
b7E

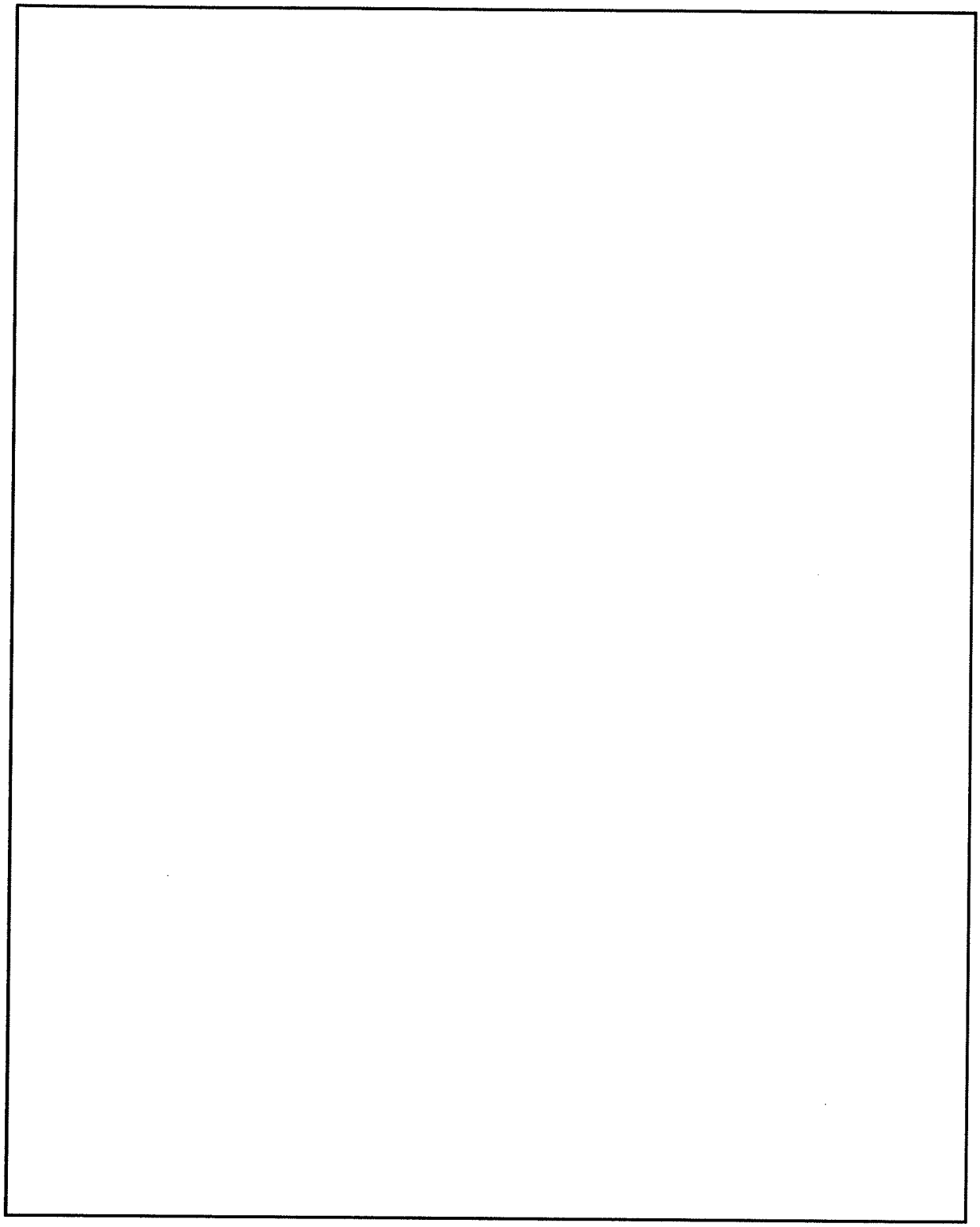
UNCLASSIFIED
NON-RECORD

b2
b7E

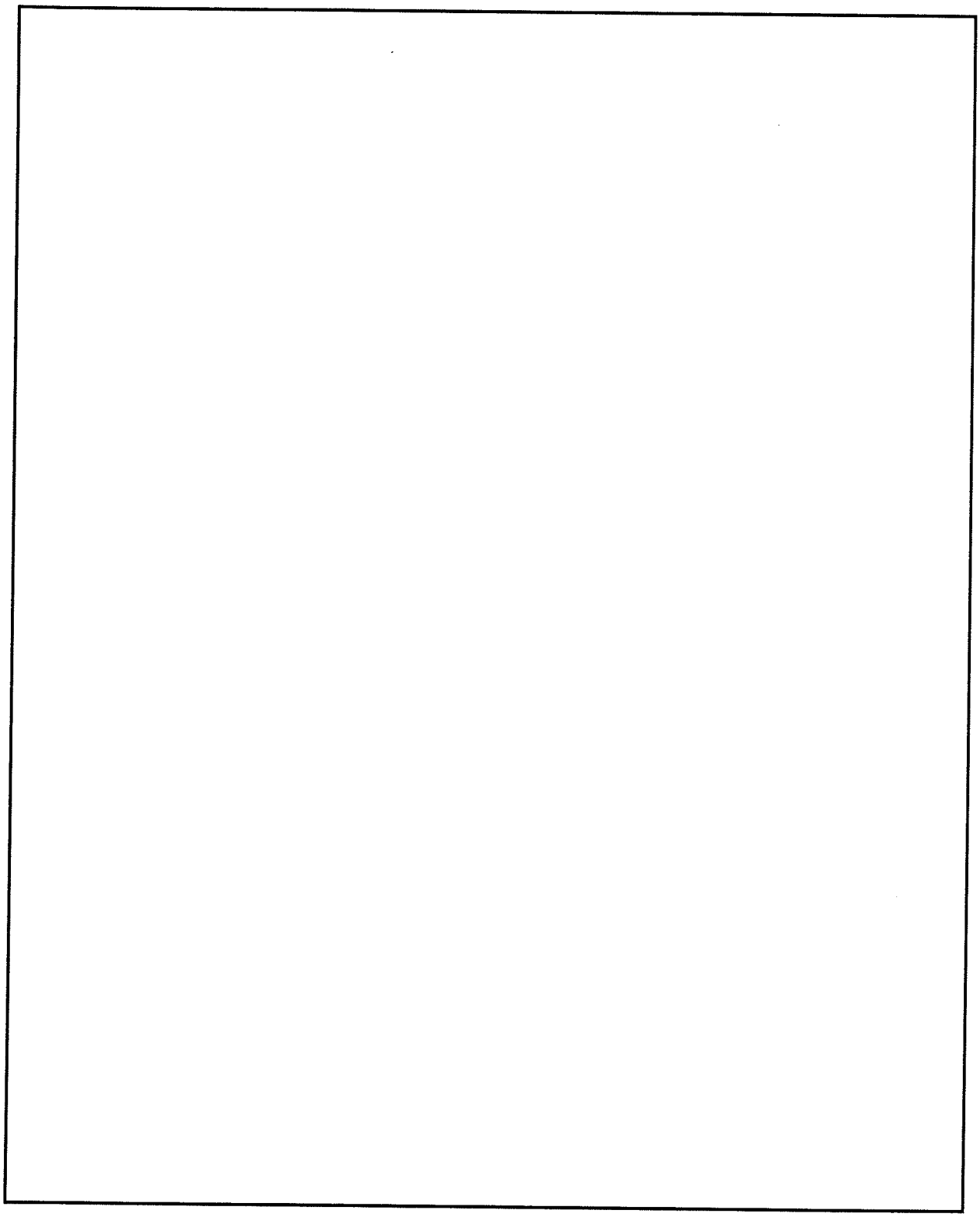


b2
b7E

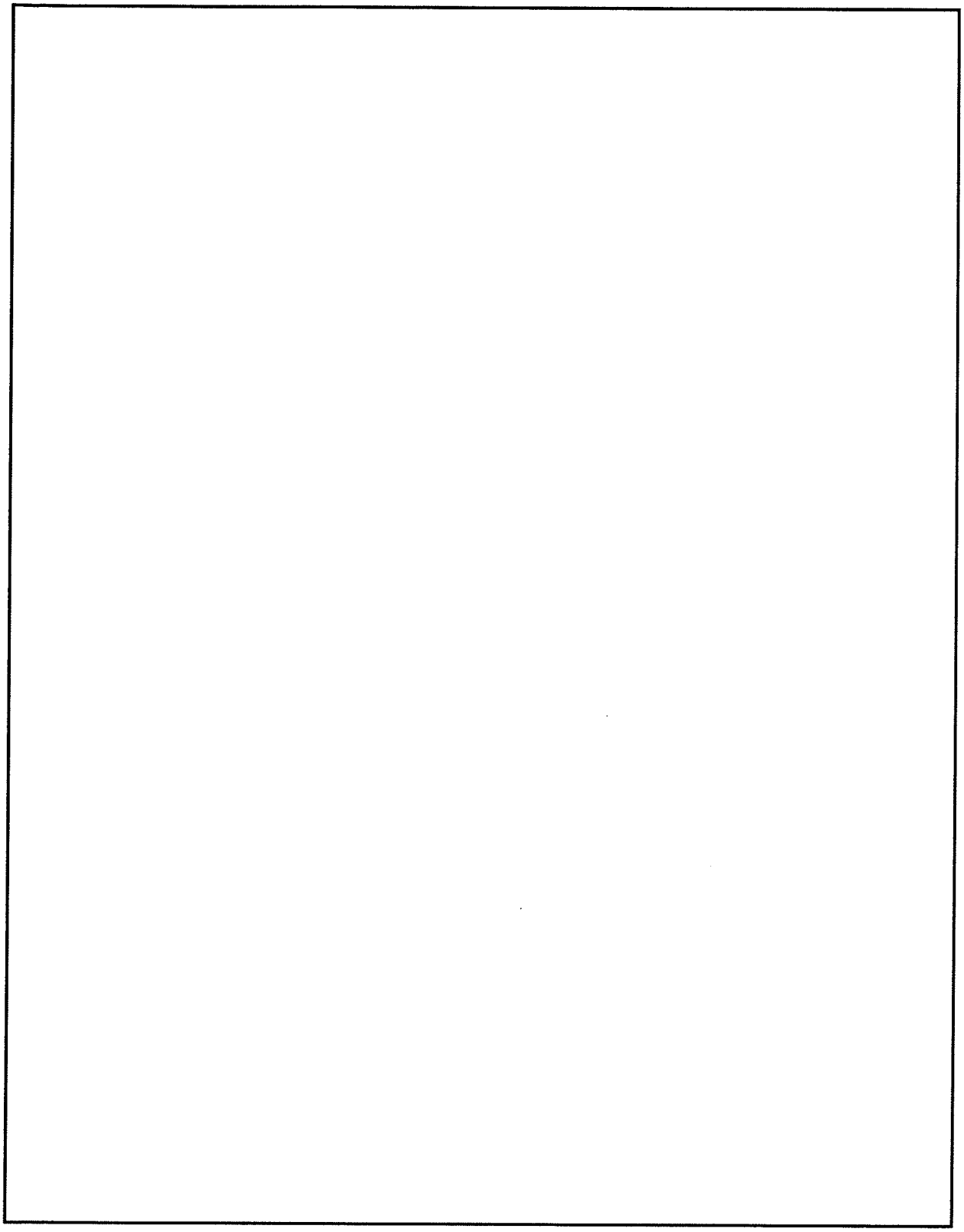
b2
b7E



b2
b7E

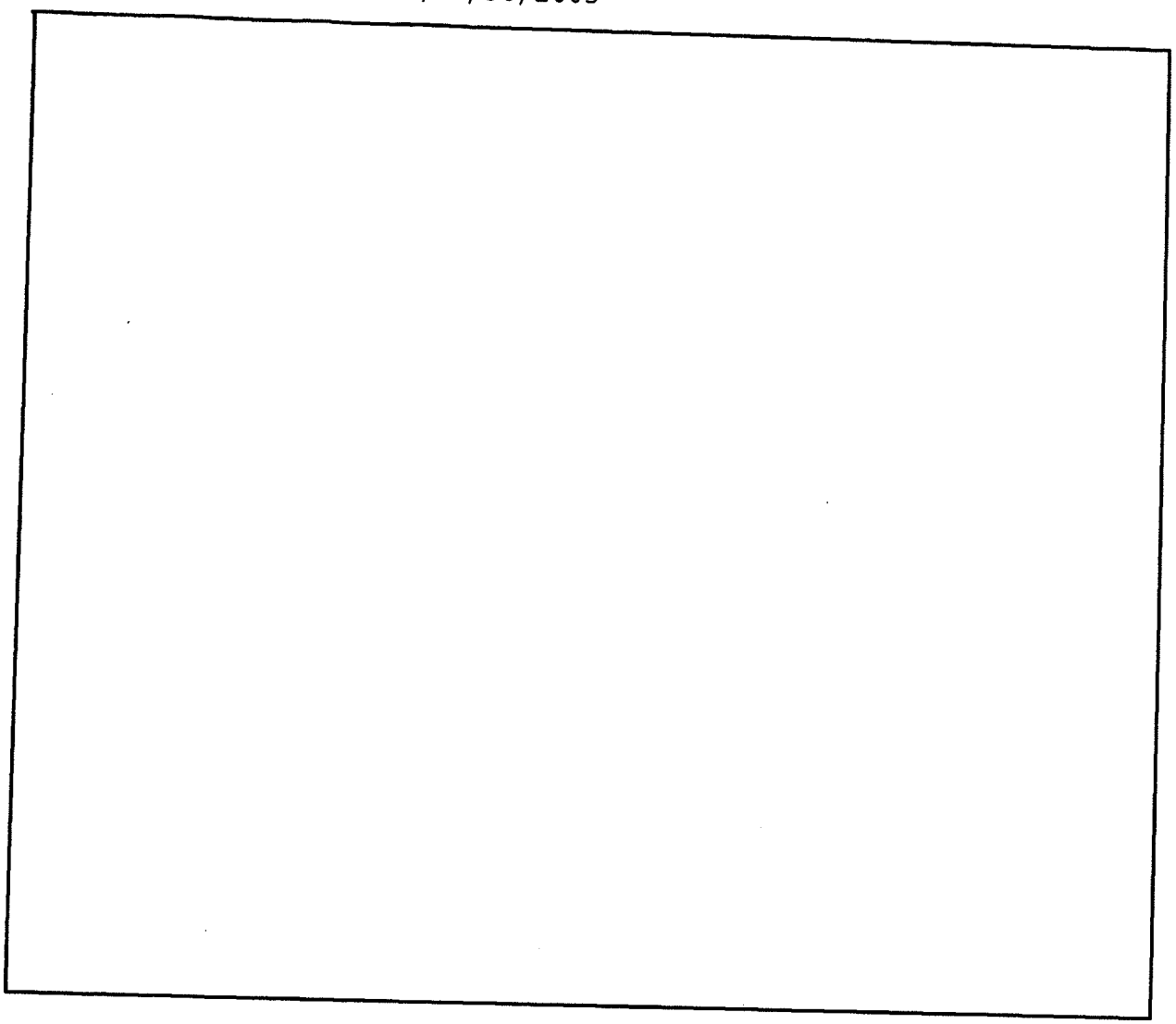


b2
b7E



b2
b7E

b2
b7E



b2
b7E

♦♦

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

b2
b6
b7C
b7A
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

IDW Data Contention and Audit Inventory for 2006

315C [redacted]	1 and 4	ACS	[redacted]	11-Sep-06 2006-11SEP-01A	Provided Audit for these case id's on 28Sept06
315C [redacted]	38 and 39	ACS	[redacted]	11-Sep-06 2006-11SEP-01A	Provided Audit for these case id's on 28Sept06
[redacted]		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.
315C [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]	ALL	ALL	[redacted]	21-Jun-06 2006-21JUN-01A	Provided audit for specific documents.
100 [redacted] 311A [redacted]	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		17-Apr-06	2006-17APR-01A Provided audit for issue.
(S)				27-Apr-06	2006-27APR-01 & 01A Removed 7 documents on 28APR06 and provided requested audit on 01MAY06.
				27-Apr-06	2006-27APR-01 & 01A Removed 7 documents on 28APR06 and provided requested audit on 01MAY06.
66F				6-Mar-06	2006-06MAR-01A Provided audit for issue.

b2
b6
b7C
b1
b7A

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

b2
b7E

b2
b7E

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

b2
b7E

The procedure for secure deletion of individual files 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 was created. There are three usages for b2 b7E

- Usage 1:
- Usage 2
- Usage 3

where

- is the option to create a "delete file" full filename(s) and filepath(s) of the files to be deleted. b2 b7E
- is a text file containing the IDW Document ID's of the files to be deleted.
- 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. b2 b7E
- is the name of the "delete file" containing the full filename(s) and filepath(s) of the files to be deleted. The is created in the same filepath as the The format o is b2 b7E
- 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.

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 from the filesystem updates the Tracking Database with the appropriate "DEL" status for the files. b2 b7E
- Mode 2: Usage 1 followed by Usage 3 updates the Tracking Database with "DEL" status for the files specified in This mode is used to reconcile the Tracking Database when the files have been previously (e.g., manually) deleted off the filesystem.

When executed reads the IDW Document ID values in 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.

[redacted]

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

b6
b7C

Subject: National Research Council Report

CAO Contact Person:

DOJ Notification: **DOJ Date/Time:**

FBI Participants: CIO Zal Zami

Other Participants:

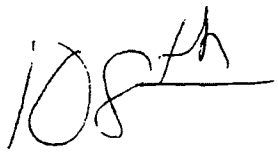
Committees /Subcommittees: HPSCI

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

Details of Briefing:

Zal 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. Zal 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, Zal said Alan Wade (overall) coupled with 5 working groups.

Follow Up Action:



Congressional Affairs Office
Congressional Contacts

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

2005-1 **Event Date:** 1/13/2005

b6
b7C

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

CAO Contact Person: SSA

DOJ Notification: None **DOJ Date/Time:**

b6
b7C

FBI Participants: CIO Zalmai Azmi (Briefer), AD Eleni Kalisch, SSA (OCIO)

Other Participants:

Committees /Subcommittees: Senate Select Committee on Intelligence

b6
b7C

Members/Staff:

Details of Briefing:

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

Follow Up Action:

None

109th

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

b6
b7C

CAO Contact Person:

DOJ Notification: **DOJ Date/Time:**

FBI Participants: Zal Azmi (ACS demo)

Other Participants:

Committees /Subcommittees: House Appropraitions

b6
b7C

Members/Staff:

Details of Briefing:

The staff were provided a demo and briefing on IDW and ACS. 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. 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/iniatives.

b6
b7C
OTHER O/S

Follow Up Action:

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:

b2 b6 b7C b7E **CAO Contact Person:** SSA

DOJ Notification: **DOJ Date/Time:** 1:00:00 PM

FBI Participants: SC Mike Morehart (TFOS) (TFOS, observer)

Other Participants:

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

Members/Staff:

Details of Briefing:

b6 b7C OTHER O/S b2 b7E

Follow Up Action:

b6 b7C OTHER O/S

Congressional Affairs Office
Congressional Contacts

Date Entered: 10/03/2005 | (•) Briefing ( ) Hearing ( ) Other ( ) FOC

OTHER O/S

2005-366 **Event Date:** 8/26/2005

Subject: [redacted] IDW

b6
b7C

CAO Contact Person: SSA [redacted]

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

FBI Participants: SC Mike Morehart, TFOS, UC [redacted] and SSA [redacted]

Other Participants:

Committees /Subcommittees: Senate Appropriations

Members/Staff: [redacted]

Details of Briefing:

[redacted] and provided overview about IDW. Discussed information ingested by IDW and how said information is utilized. Discussed how all info is vetted thorugh 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:

b6
b7C
OTHER O/S **DOJ Notification:** **DOJ Date/Time:**

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 availbility; 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:

CAO Contact Person: SSA

DOJ Notification: **DOJ Date/Time:**

FBI Participants: None

Other Participants:

Committees /Subcommittees: Senate Banking, Housing and Urban Affairs

Members/Staff: Shelby, Hagel, Martinez, Allard

b6
b7C
OTHER O/S

Details of Briefing:

also made reference to a presentation he received from the FBI concerning IDW and how the FBI was able to link information received 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

been automatically scanned and converted into computer text. These scanned documents include Bureau-generated documents related to terrorism, as well as other terrorism-related documents such as those seized in Afghanistan and Pakistan. Also large quantities of data from other agencies, including DIA, NSA, CIA, DOS, and FinCEN have been ingested into IDW.

f. Are all investigative materials obtained by the FBI by subpoena, by NSL or by other means always reviewed contemporaneously and summarized in report form, such that they are accessible through the IDW? If not, why not?

Response:

All investigative materials obtained by the FBI by subpoena, NSL, or by other means (such as that provided by 18 U.S.C. §2703) are reviewed contemporaneously. Not all investigative materials reviewed are deemed pertinent to a case. Those materials that are reviewed and deemed pertinent to a case are either summarized, in which the case summary is loaded into ACS, or the entire document is scanned, if necessary, and uploaded in its entirety into IntelPlus.

Many of the largest IntelPlus file rooms have been imported into IDW, so these documents would be accessible through the IDW in both text form and the original scanned images. Summaries loaded into ACS would be accessible through the IDW, except as noted in answer 11(c).

The only investigative materials that would not be available through the IDW are those that were not deemed pertinent to a case, those that were added to an IntelPlus file room that has not yet been incorporated into IDW, or those that are too sensitive to load into IDW, as described in answer 11(c).

g. What is the time frame for the dataset "case file" material that is currently accessible by IDW? In other words, are FD-302s that were written in 1995, 1990, or even prior to 1985 accessible?

Response:

The time frames for the datasets vary. Except as noted in part (c) above, all data stored in ACS, including FD-302s, are available in IDW. Since ACS was created in 1995, IDW contains ACS data from 1995 to present. IDW also contains millions of scanned paper documents, including those seized from suspected terrorists. Although the FBI knows the dates these documents were added into IDW, the date of origin of many of these documents is unknown.

As additional data sources continue to be added into IDW, most contain records dated prior to the date of ingest. All of this "day back" information will be included in IDW. The specific date ranges of the data will vary by source, and may include data prior to 1985. For example, IDW includes all CIA Intelligence Information Reports (IIR) at the Secret or lower classification levels issued from 1978 to present. Conversely, most data sources provide updates of new data created after the initial date of ingest. These "day forward" updates will continue to be added into IDW and appended to the appropriate data libraries.

h. You gave a "specific example" in order "to show this set of data that included a lot of different things, including case files, but not all case files, but terrorism information." Can you explain what you meant by this statement including the phrase "but not all case files, but terrorism information"?

Response:

The statement was intended to emphasize that the set of data includes terrorism information. The statement could be more clearly conveyed using two sentences: "The IDW included a lot of different types of data, including case files. IDW may not currently include all case file data (as discussed in question 11.c. above), but it does include terrorism information."

12. In early 2003, Director Mueller described the IDW as a future goal of the FBI that would encompass "31 different databases" and would be used to help the FBI conduct "data mining."

a. Please identify and provide a brief explanation of each database currently included in, or currently planned to be included in, the IDW. Approximately when was each database made accessible through IDW?

Response:

The following data sources are currently available through IDW. Other data sources that are planned to be added, pending approval by the Policy Board and the Office of General Counsel's (OGC) review of the Privacy Impact Assessment, are listed below in the response to (b).

Currently Included (Added Prior to January, 2004):

- Automated Case System (ACS), Electronic Case File (ECF)
- Secure Automated Messaging Network (SAMNet) – copies of all messaging traffic sent either from the FBI to other government agencies, or sent from other government agencies to the FBI through the Automated Digital Information Network (AutoDIN).