System Security Plan

Investigative Data Warehouse-SECRET (IDW-S)
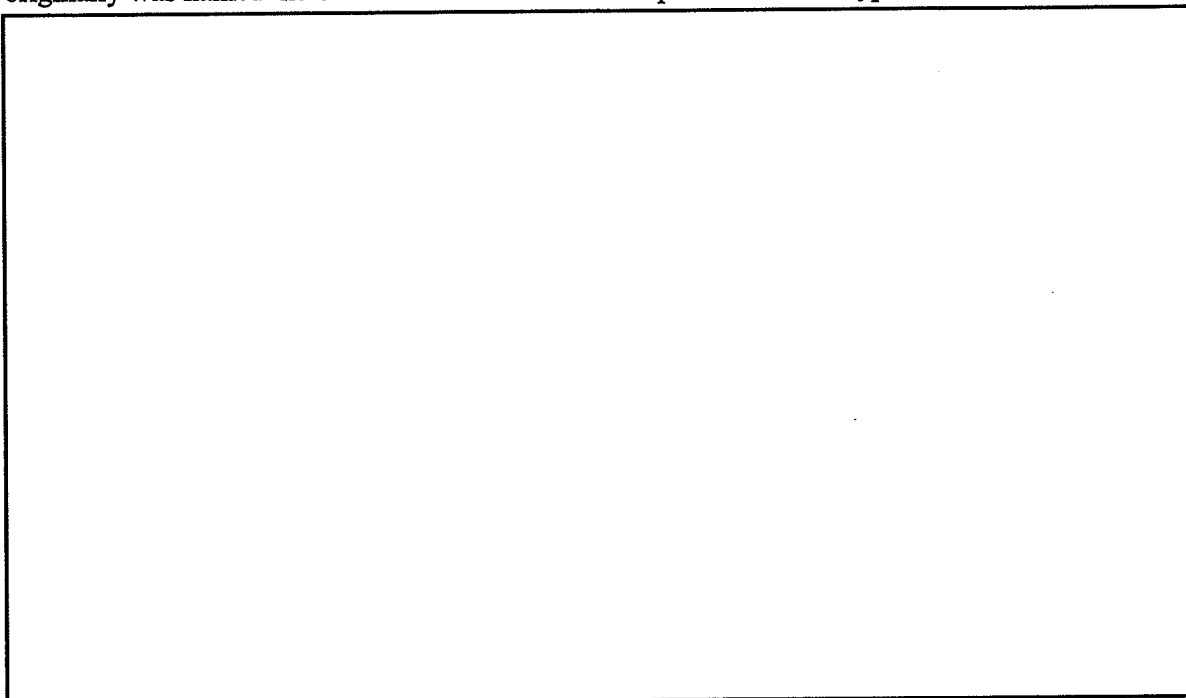
16 January 2004
Version: 1.0

Federal Bureau of Investigation (FBI), Information Resources Division (IRD)

Investigative Data Warehouse (IDW) - Secret System Security Plan

INTRODUCTION

The Federal Bureau of Investigation's (FBI) Investigative Data Warehouse Secret System (IDW-S) is an initial data warehouse, content management and data mining system that will permit FBI investigative, analytical, administrative and intelligence personnel to access aggregated data previously only available through individual applications. The IDW-S system will be authorized to process classified national security data up to, and including, Secret. The IDW-S system is the successor to the Secure Collaboration Operational Prototype Environment (SCOPE), which originally was named the Secure Counter-Terrorism Operational Prototype Environment.
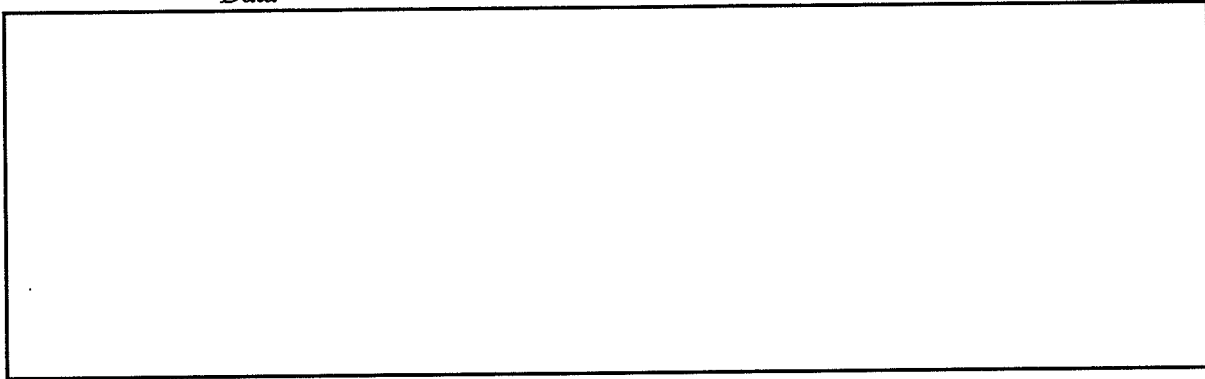
Outside the Scope

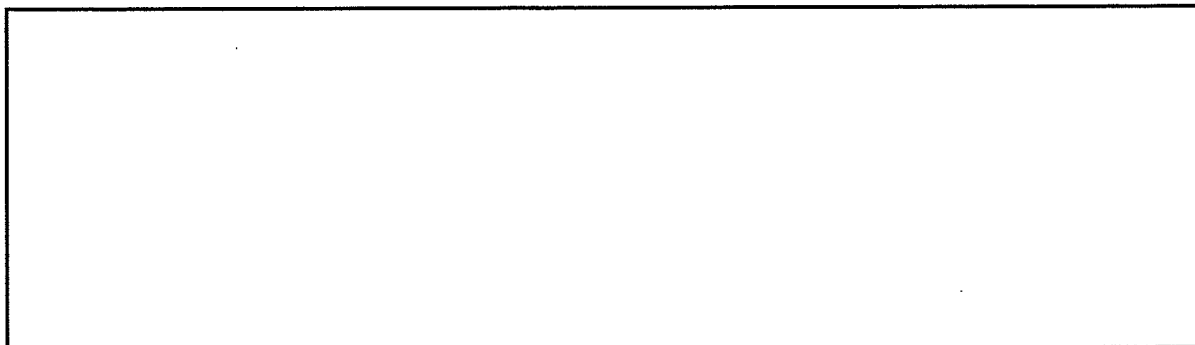Data processed by the system will include the following data sets:

- Approved case files from the FBI's Automated Case Support (ACS) case management system;

- Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents;

- Secure Automated Messaging Network (SAMNet) message traffic;

- IntelPlus File Rooms; and

- Violent Gang and Terrorist Organization File (VGTOF) from the Criminal Justice Information Systems (CJIS) Division;

- Defense Advanced Research Projects Agency (DARPA) Translingual Information Detection, Extraction and Summarization (TIDES) Open Source Data

Outside the Scope
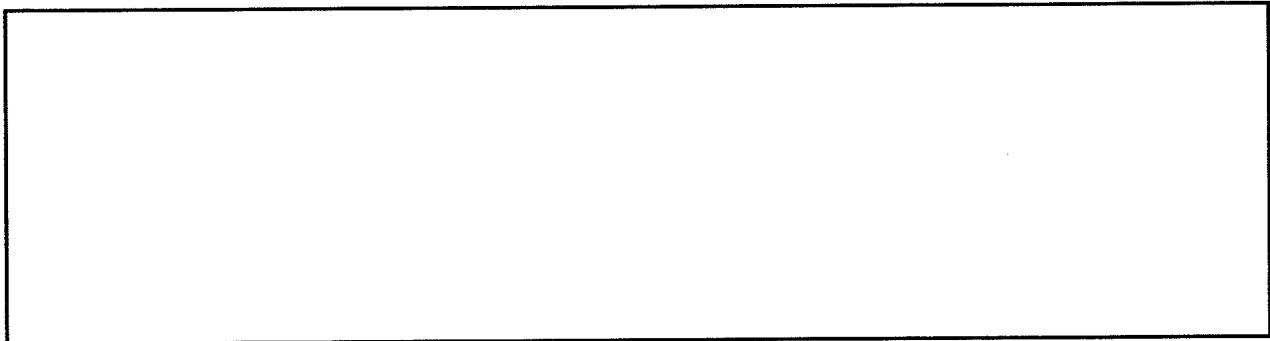
Outside the Scope

1.2.2 Supported Projects

IDW-S is an FBI enterprise program/system and utilizes data feeds from several FBI (and other agency) programs.

PROJECT NAME	CLASSIFICATION / COMPARTMENTS	
Automated Case System (ACS	Secret	
Intel Plus	Secret	
Secure Automated Messaging Network (SAMNet)	Secret	
National Crime Information Center (NCIC)	Sensitive But Unclassified (SBU)	
Document Conversion Laboratory (DocLab)	Secret	

b2
b7E

6

PROJECT NAME	CLASSIFICATION / COMPARTMENTS	
Translingual Information Detection, Extraction and Summarization (TIDES) Program	Unclassified	

b2
b7E
Outside the Scope

3.5. DATA PROCESSED

IDW-S processes data from the following data sources, with the security classification of the source indicated in brackets:

- Automated Case Support (ACS) System, Electronic Case File (ECF) Subsystem [Secret and below]

- IntelPlus [Secret and below]

- Secure Automated Message Network – Secret (SAMNet-S) [Secret and below]

- NCIC Violent Gang and Terrorist Offender File (VGTOF) [Sensitive But Unclassified]

- Joint Intelligence Committee Investigation (JICI) [Secret and below]

- DARPA/TIDES Open Source News [Unclassified]   Outside the Scope

DATASET NAME	DATA SOURCE	TRANSFER METHOD	
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS	FTP	
IntelPlus Filerooms	FBI IntelPlus	FTP	
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	FTP	
VGTOF	FBI National Crime Information Center (NCIC)	CD-ROM	

b2
b7E

23

DATASET NAME	DATA SOURCE	TRANSFER METHOD	
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Multiple	b2 b7E
Open Source News	Translingual Information Detection, Extraction and Summarization (TIDES) Program	CD-ROM	

Data Sources w/Transfer Mechanism

3.5.1 ACS ECF

IDW-S contains a subset of the ECF (Electronic Case File) subsystem of the Automated Case System (ACS). This subset consists of serials in those case classifications/sub classifications that have been officially sanctioned for inclusion in IDW-S. For each such serial, the ECF data includes metadata and text. IDW-S is synchronized against the ECF system once a day, a process which consists of receiving and processing the previous day's increment of ADD, MOD, and DELETE records.
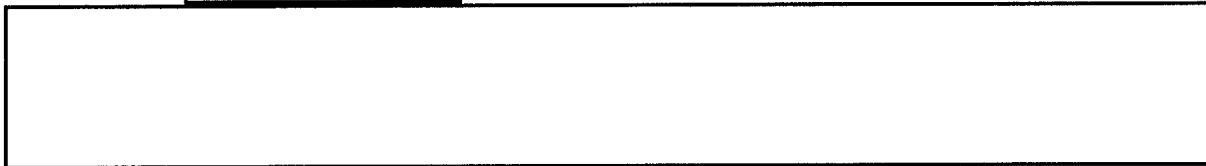
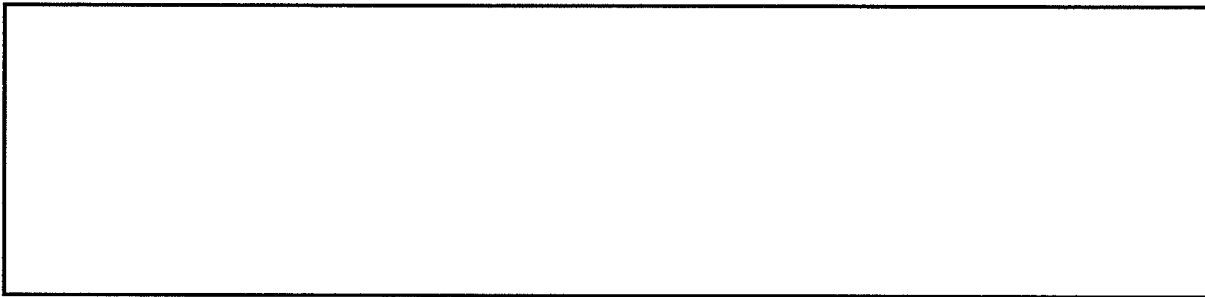## 3.5.2 IntelPlus

Outside the Scope

IDW-S currently contains several IntelPlus counter-terrorism (CT) Filerooms:

-
-
-
-
-
-

b2
b7E

b2
b7E

24

b2
b7E

3.5.3 SAMNet

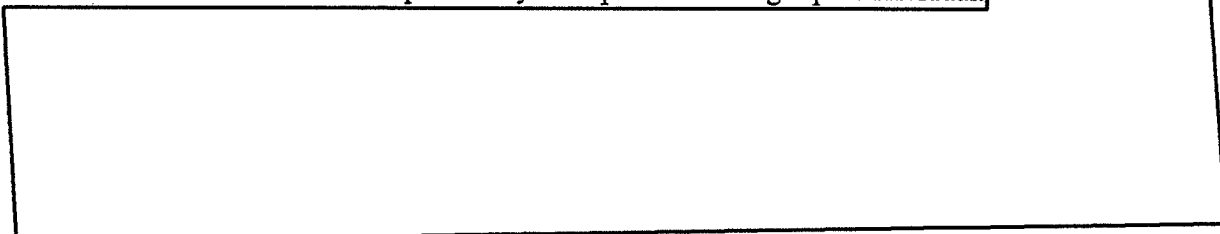The Secure Automated Messaging Network (SAMNet) data source consists of cable traffic messages received by the FBI. _____ SAMNet provides only ADD record types, and SAMNet data is updated in IDW-S three times a day. SAMNet data
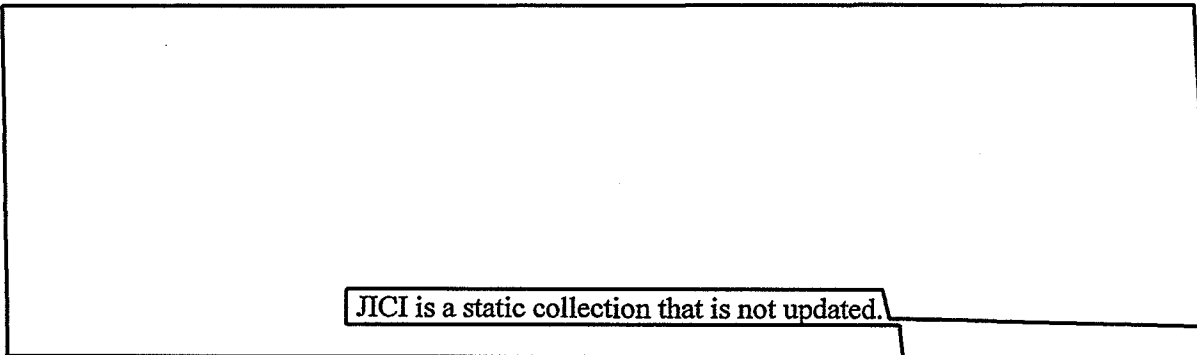
3.5.4 VGTOF

Violent Gang Terrorist Offender File (VGTOF) data is provided by the FBI National Crime Information Center (NCIC). VGTOF data includes two components: Data/metadata for each named individual/offender and potentially multiple JPEG images per individual.

b2
b7E

3.5.5 JICI

b2
b7E

JICI is a static collection that is not updated.

25

3.5.6 Open Source News

The IDW-S V1.0 system contains an Open Source News library collected by the DARPA TIDES Program. These are primarily news source from around the world that are either in English or have been translated into English. Open Source News data is received in the form of text files (one per news article[   ]The Open Source News data goes into IDW-S once a day. Open Source News data is[   ]

b2
b7E

26
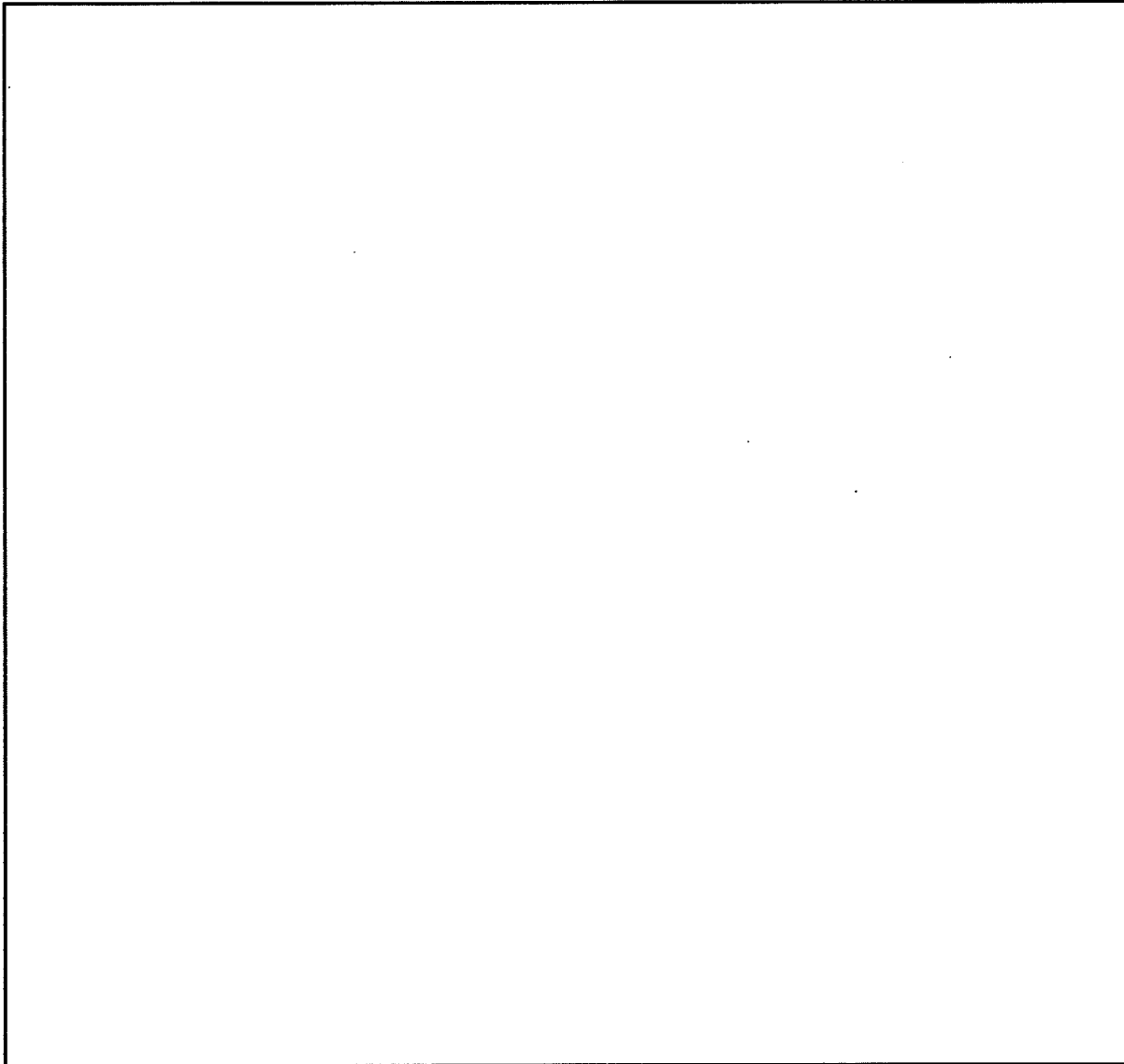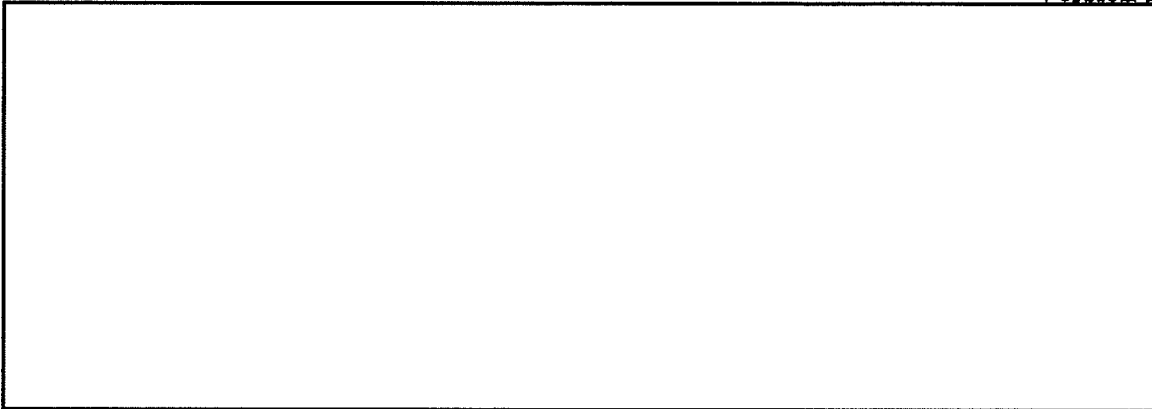
Outside the Scope

3.9.9 Indirect Connections   Outside the Scope

IDW-S connects to the following sources of data:

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	
FBI Automated Case System (ACS	Secret	FBI	FTP	
FBI Intel Plus	Secret	FBI	FTP	
FBI Secure Automated Messaging Network (SAMNet)	Secret	FBI	FTP	
FBI National Crime Information Center (NCIC)	Unclassified/SBU	FBI	CD-ROM	

b2
b7E

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	COMMENTS
FBI Document Conversion Laboratory (DocLab), Records Management Division (RMD), FBIHQ	Secret	FBI	CD/DVD	
Translingual Information Detection, Extraction and Summarization (TIDES) Program, Defense Advanced Research Projects Agency (DARPA)	Unclassified	NA	CD-ROM	
	Unclassified	NA	CD-ROM	

b2
b7E

Indirect Connections

48

System Security Plan

Investigative Data Warehouse-SECRET (IDW-S)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
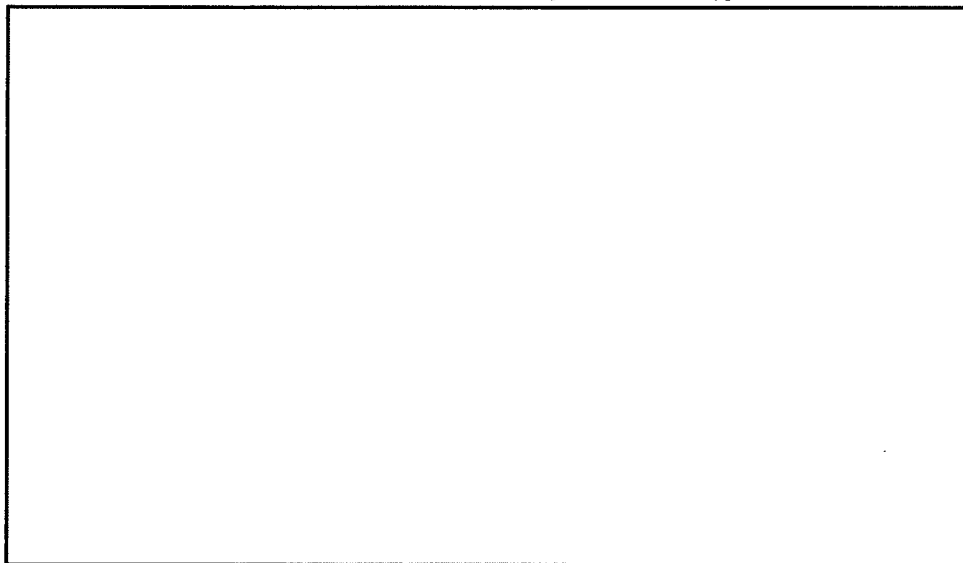DATE 01-07-2008 BY 65179 DMH/BJA/CAL

5 DECEMBER 2003

Version: 0.7

Federal Bureau of Investigation (FBI), Information Resources Division (IRD)

i

Investigative Data Warehouse (IDW) - Secret System Security Plan

INTRODUCTION

The Federal Bureau of Investigation's (FBI) Investigative Data Warehouse Secret System (IDW-S) is an initial data warehouse, content management and data mining system that will permit FBI investigative, analytical, administrative and intelligence personnel to access aggregated data previously only available through individual applications. The IDW-S system will be authorized to process classified national security data up to, and including, Secret. The IDW-S system is the successor to the Secure Collaboration Operational Prototype Environment (SCOPE), which originally was named the Secure Counter-Terrorism Operational Prototype Environment.
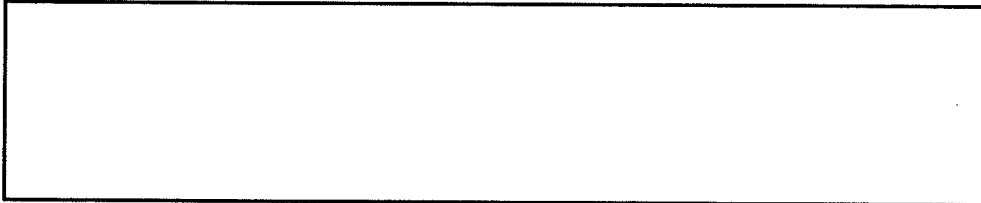
Outside the Scope

Data processed by the system will include the following data sets:

- Approved case files from the FBI's Automated Case Support (ACS) case management system;

- Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents;
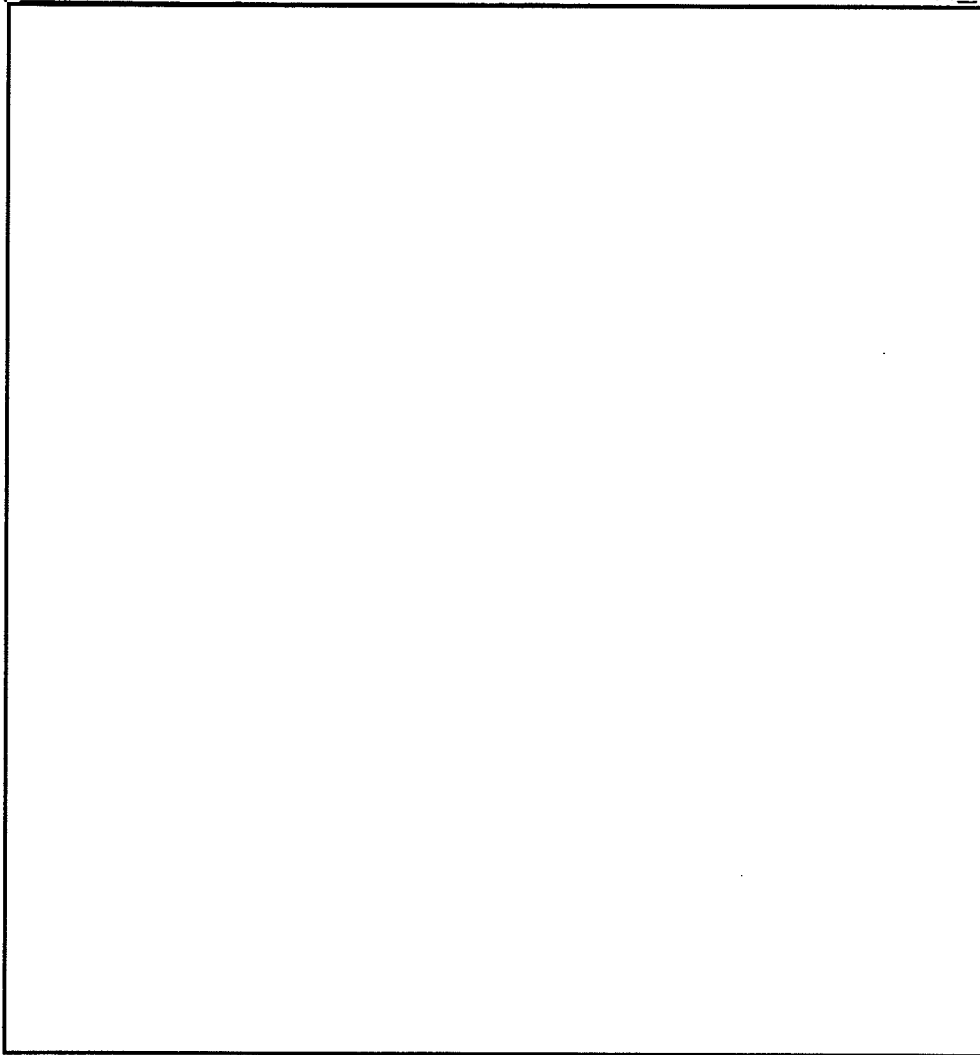
-1-

- Secure Automated Messaging Network (SAMNet) message traffic;

- IntelPlus File Rooms; and

- Violent Gang and Terrorist Organization File (VGTOF") from the Criminal Justice Information Systems (CJIS) Division;

- Defense Advanced Research Projects Agency (DARPA) Translingual Information Detection, Extraction and Summarization (TIDES) Open Source Data

·Outside the Scope

Data Sources

IDW-S contains data from the following data sources with security classification indicated in brackets:

Outside the Scope

- Automated Case Support (ACS) System, Electronic Case File (ECF) Subsystem [Secret and below]

- IntelPlus [Secret and below]

- Secure Automated Message Network – Secret (SAMNet-S) [Secret and below]

- NCIC Violent Gang and Terrorist Offender File (VGTOF) [Sensitive But Unclassified]

- Joint Intelligence Committee Investigation (JICI) [Secret and below]

- DARPA/TIDES Open Source News [Unclassified]

Data from each source is held in an identified source Library against which users can direct the analytical tools.

Data Ingest

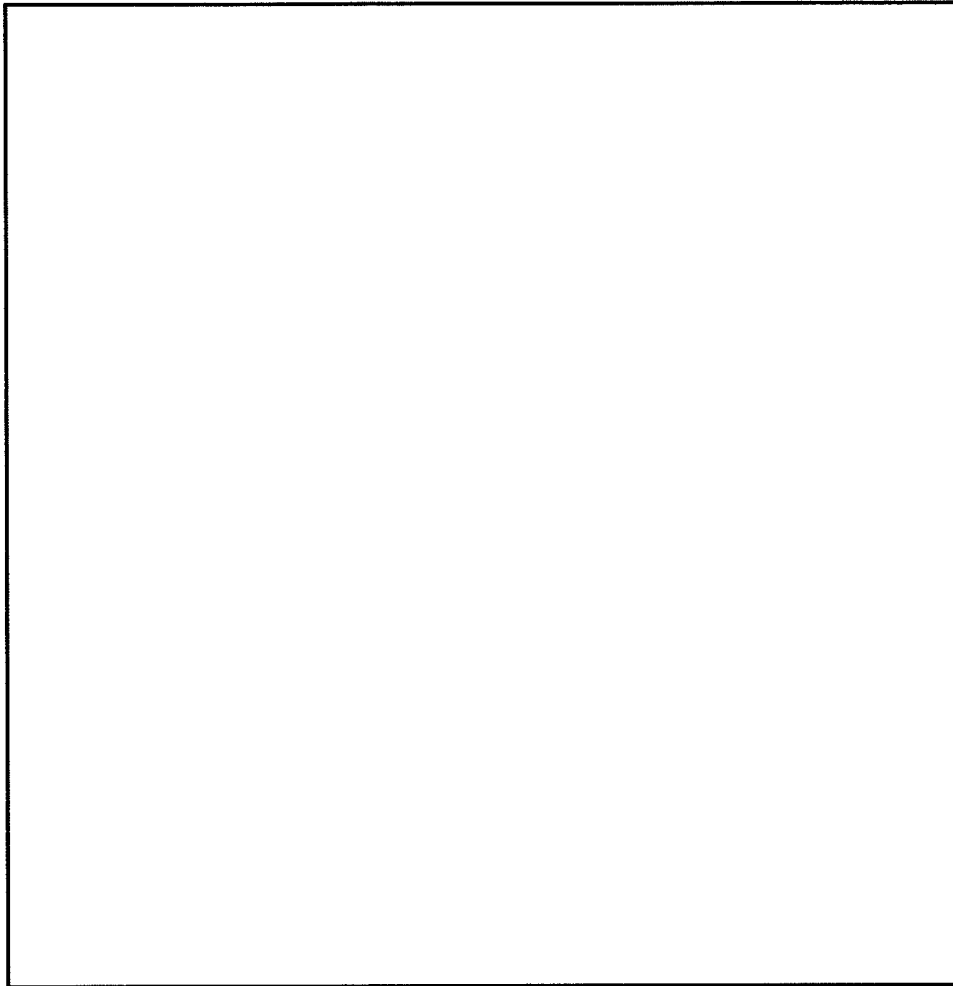IDW-S receives data from sources by FTP over FBINet (ACS ECF, IntelPlus, and SAMNet) and CD-ROM (VGTOF, Open Source News)

- Data is received by the Ingest Subsystem

-

  - Received data is parsed into individual serial records (in the case of ACS ECF), documents (IntelPlus, JICI, Open Source News), messages (SAMNet), or files (VGTOF).

-

Outside the Scope

Outside the Scope

3.5. DATA PROCESSED

IDW-S processes the following data:

3.5.1 ACS ECF

IDW-S contains a subset of the ECF (Electronic Case File) subsystem of the Automated Case System (ACS). This subset consists of serials in those case classifications/sub classifications that

have been officially sanctioned for inclusion in IDW-S. For each such serial, the ECF data includes metadata and text. IDW-S is synchronized against the ECF system once a day, a process which consists of receiving and processing the previous day's increment of ADD, MOD, and DELETE records.

3.5.2 IntelPlus

IDW-S currently contains several IntelPlus counter-terrorism (CT) Filerooms:

Outside the Scope

-
-
-
-
-
-

b2
b7E

3.5.3 SAMNet

The Secure Automated Messaging Network (SAMNet) data source consists of cable traffic messages received by the FBI.

SAMNet provides only ADD record types, and SAMNet data is updated in IDW-S three times a day. SAMNet data is

b2
b7E

3.5.4 VGTOF

Violent Gang Terrorist Offender File (VGTOF) data is provided by the FBI National Crime Information Center (NCIC). VGTOF data includes two components: Data/metadata for each named individual/offender and potentially multiple JPEG images per individual
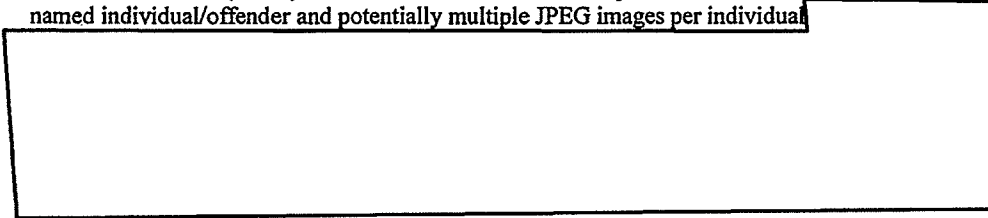
3.5.5 JICI

The Joint Intelligence Committee Investigation (JICI) data collection was created following the September 11 attacks. Paper counter-terrorism files/folders from all FBI Field Offices

b2
b7E
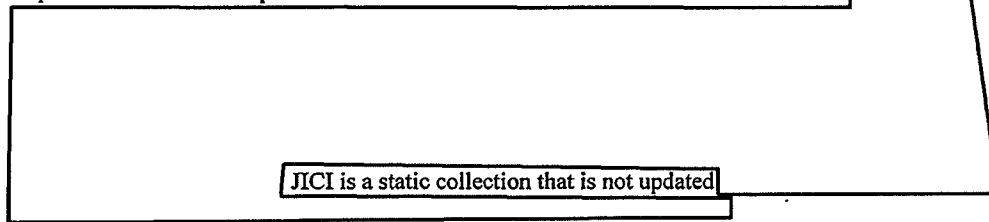
JICI is a static collection that is not updated

3.5.6 Open Source News

The IDW-S V1.0 system contains an Open Source News library collected by the DARPA TIDES Program. These are primarily news source from around the world that are either in English or have been translated into English. Open Source News data is received in the form of text files (one per news article) and   The Open Source News data goes into IDW-S once a day. Open Source News data

Open Source News material is derived from the following sources:

Addis Ababa Tribune - http://www.addistribune.com/
Agencia Brasilia - http://www.radiobras.gov.br/
Al-Ahram (Egypt, weekly English version) - http://weekly.ahram.org.eg/
AllAfrica.com - http://allafrica.com/
Arabic News - http://www.arabicnews.com/ansub/
Asahi Shimbun - http://www.asahi.com/english/
Asia Times (Hong Kong) - http://www.atimes.com/
Bangkok Post - http://www.bangkokpost.net/
Christian Science Monitor - http://www.csmonitor.com/

-23-

Crescent International - http://www.muslimedia.com/mainpage.htm
Daily Telegraph (London, England) - http://news.telegraph.co.uk/
Dawn (Karachi, Pakistan) - http://www.dawn.com/
Debka (Israel) - http://www.debka.com
East Africa Daily Nation - www.nationaudio.com/News/DailyNation/Today/
Gulf News (UAE) - http://www.gulf-news.com/
Ha'aretz (Israel) - http://www.haaretzdaily.com/
IFRC International Federation of the Red Cross - http://www.ifrc.org/
IRIN Integrated Regional Information Network - http://www.irinnews.org/
Iraq Press News Agency - http://www.iraqpress.org/
Islamic Republic News Agency (Iran) - http://www.irna.com/en
Jakarta Post - http://www.thejakartapost.com/
Janes - http://www.janes.com/
Jordan Times - http://www.jordantimes.com/
L'Osservatore Romano - www.vatican.va/news_services/or/or_eng/text.html
Lagos (Nigeria) Guardian - http://www.guardiannewsngr.com/
Lahore (Pakistan) Nation - http://www.nation.com.pk/
Lebanon Daily Star (Beirut) - http://www.dailystar.com.lb/
Malaysian Star - http://thestar.com.my/
Manila Bulletin - http://www.mb.com.ph/
Manila Times - http://www.manilatimes.net/
Miami Herald - http://www.miami.com/
Moscow Times - http://www.themoscowtimes.com/
National Post and CP - http://www.canada.com/
New Straits Times (Kuala Lumpur) - http://www.emedia.com.my/Current_News/NST/
PETRA (Jordanian News Agency) - http://www.petra.gov.jo
Pakistan Observer (Islamabad) - http://pakobserver.net/
Palestine Chronicle - http://palestinechronicle.com/
People's Daily (China) - http://english.peopledaily.com.cn/
Philippine Star - http://www.philstar.com/philstar/
Pravda - http://english.pravda.ru/
ProMed - epidemiology mailing list
Russian Information Agency Novosti - http://en.rian.ru/
Russian Issues (Misc. Russian news) - http://www.therussianissues.com/
Russian Observer - http://www.russianobserver.com/
SABA (The News Agency of Yemen) - http://www.sabanews.gov.ye
Saudi Gazette - http://www.saudigazette.com.sa/sgazette/
South African Dispatch - http://www.dispatch.co.za/
Sydney Morning Herald - http://www.smh.com.au
Tehran Times - http://www.tehrantimes.com/
Times of India - http://timesofindia.indiatimes.com/cms.dll
UNHCR UN High Commissioner on Refugees - http://www.unhcr.ch/

Ummah News - http://www.ummahnews.com/
Uzbekistan Report - http://www.uzreport.com/eng/
Washington Post - http://www.washingtonpost.com/
XinHua News Service - http://www.xinhuanet.com/english/
Yemen Times (weekly) - http://www.yementimes.com/
Yomiuri Shimbun (Japan) - http://www.yomiuri.co.jp/

3.5.7 Summary of Data Sources

| DATASET NAME	DATA SOURCE	TRANSFER METHOD
ACS	FBI Automated Case System (ACS)	FTP
IntelPlus	FBI Intel Plus	FTP
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	FTP
VGTOF	FBI National Crime Information Center (NCIC)	CD-ROM
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Multiple

b2
b7E

Outside the Scope

-25-

Investigative Data Warehouse (IDW) - Secret
System Security Plan
19 December 2003
Version 0.8

DATASET NAME	DATA SOURCE	TRANSFER METHOD	
Open Source News	Translingual Information Detection, Extraction and Summarization (TIDES) Program, Defense Advanced Research Projects Agency (DARPA)	CD-ROM	

b2
b7E
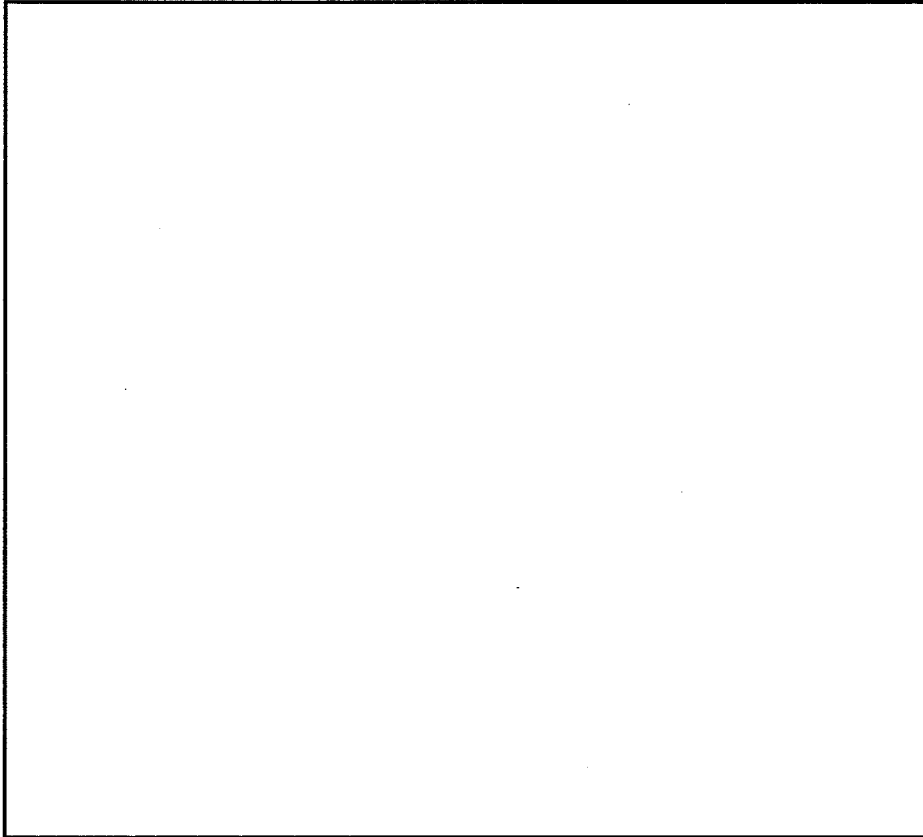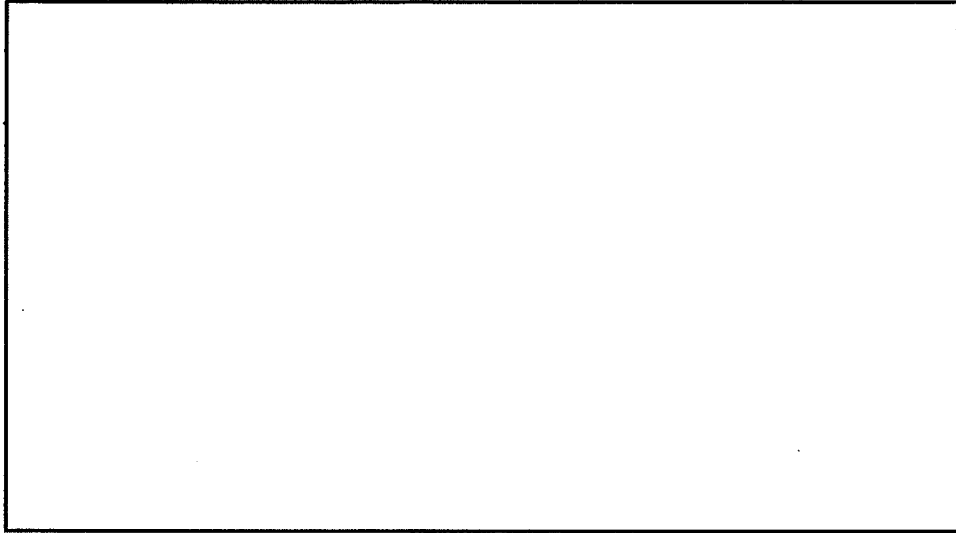
Outside the Scope

Outside the Scope

3.9.9 Indirect Connections

IDW-S connects to the following sources of data:

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	
FBI Automated Case System (ACS)	Secret	FBI	FTP	
FBI Intel Plus	Secret	FBI	FTP	

b2
b7E

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	COMMENTS
FBI Secure Automated Messaging Network (SAMNet)	Secret	FBI	FTP	
FBI National Crime Information Center (NCIC)	Unclassified/SBU	FBI	CD-ROM	
FBI Document Conversion Laboratory (DocLab), Records Management Division (RMD), FBIHQ	Secret	FBI	Multiple	
Translingual Information Detection, Extraction and Summarization (TIDES) Program, Defense Advanced Research Projects Agency (DARPA)	Unclassified	NA	CD-ROM	

b2
b7E

Outside the Scope

Investigative Data Warehouse (IDW) - Secret
System Security Plan
19 December 2003
Version 0.8

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	COMMENTS
	Unclassified	NA	CD-ROM	

Indirect Connections

b2
b7E

-42-

Federal Bureau of Investigation
Information Resources Division
Data Management Section

Investigative Data Warehouse
Maintenance Manual
Version 1.1 for Authority to Operate
June 11, 2004

1 Introduction

The Federal Bureau of Investigation (FBI) Integrated Data Warehouse (IDW) is a data warehouse, content management, and data mining system that will permit FBI investigative, analytical, administrative, and intelligence personnel to access aggregated data previously available only through individual applications. The IDW-S system will be authorized to process classified national security data up to, and including, the Secret level.
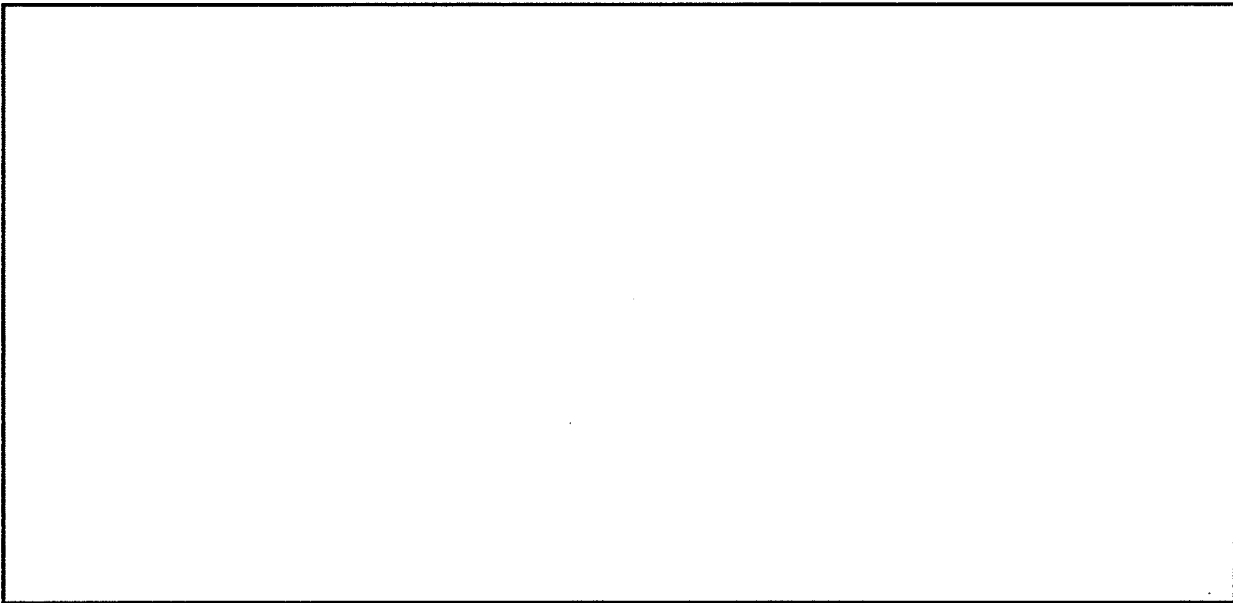
```
┌─────────────────────────────────────────────────────────────┐
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
│                                                               │
└─────────────────────────────────────────────────────────────┘
```

Data processed by the system will include the following data sets: Outside the Scope

- Approved case files from the FBI's Automated Case Support (ACS) case management system;

- Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents;

- Secure Automated Messaging Network (SAMNet) message traffic;

- IntelPlus File Rooms;

- Violent Gang and Terrorist Organization File (VGTOF) from the Criminal Justice Information Systems (CJIS) Division; and

- Open Source Data

Note: Hardcopy versions of this document must be verified for correct version number with the IDW O&M Document Control Library.

MM NG-OM-004.11ATO

FOR OFFICIAL USE ONLY

Page 1

System Administrator Manual
(SAM)

IDW Operational Services

Version 1.1 ATO

copy

SAM NG-OM-005.11ATO

Federal Bureau of Investigation

Information Resources Division

Data Management Section

Investigative Data Warehouse

System Administrators Manual

Version 1.1 for Authority to Operate

June 11, 2004

Note: Hardcopy versions of this document must be verified for correct version number with the IDW CM Document Control Library.

SAM NG-OM-005.11ATO

FOR OFFICIAL USE ONLY
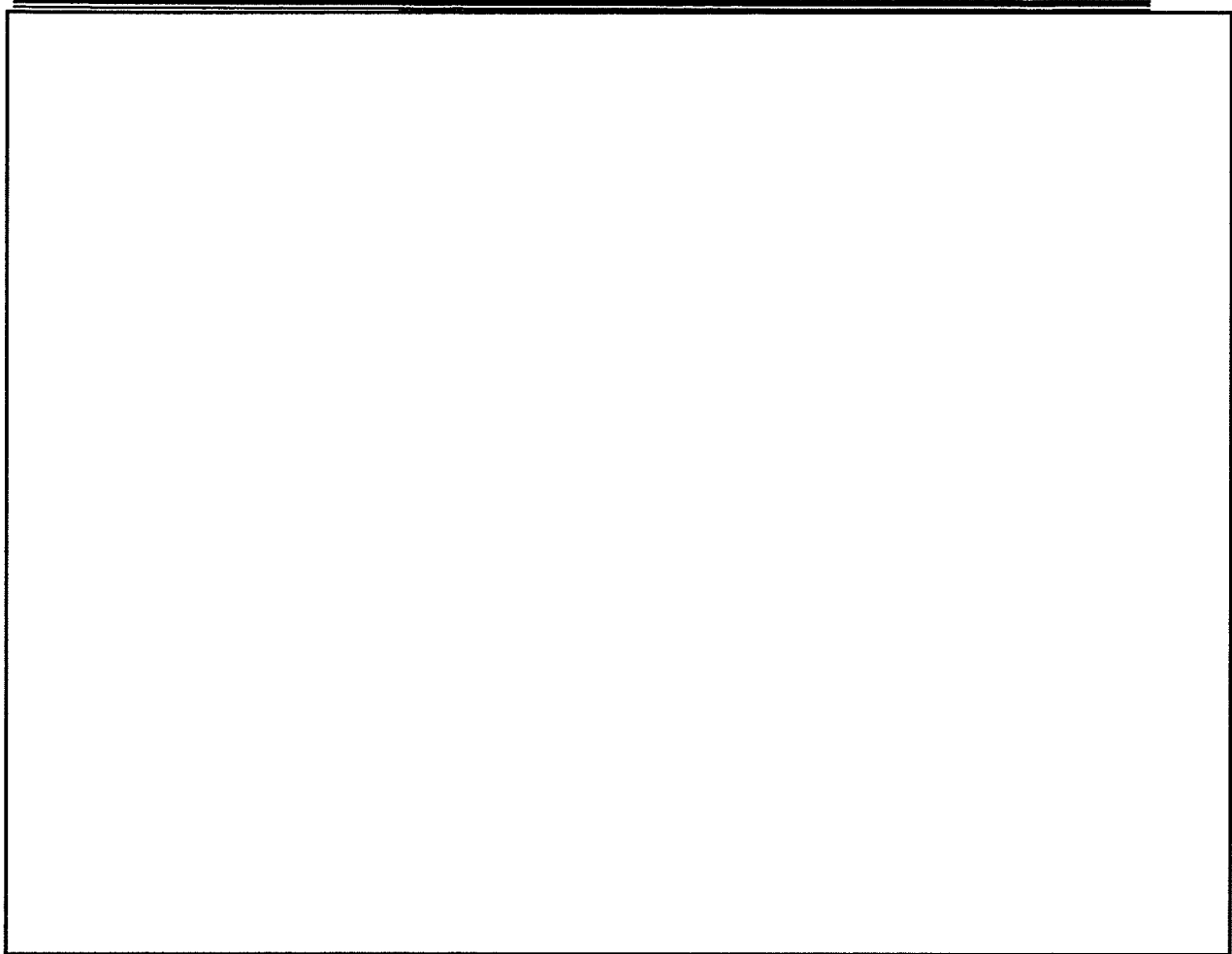
Outside the Scope

1.4.1.1 Data Sources

The FBI maintains large databases of records. These records are recorded in both standard and vendor/developer unique formats.

b2
b7E

Data processed by the system includes the following sources:

- Approved case files from the FBI's Automated Case Support (ACS) management system;
- Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents;
- Secure Automated Messaging Network (SAMNet) message traffic;
- IntelPlus (INTEL+) File Rooms;

- Violent Gang and Terrorist Organization File (VGTOF) from the Criminal Justice Information Systems (CJIS) Division;
- Defense Advanced Research Projects Agency (DARPA) Translingual Information Detection, Extraction and Summarization (TIDES) Open Source Data.

Note: Hardcopy versions of this document must be verified for correct version number with the IDW CM Document Control Library.

SAM NG-OM-005.11ATO
FOR OFFICIAL USE ONLY
Page 3

Outside the Scope

FEDERAL BUREAU OF INVESTIGATION

OFFICE OF THE PROGRAM MANAGEMENT EXECUTIVE

Security Concept of Operations (S-CONOPS)
Investigative Data Warehouse (IDW)

Document Version 1.1

June 18, 2004

i

Outside the Scope

The table below lists the data and sources for the Operational Subsystem.

10

UNCLASSIFIED//FOR OFFICIAL USE ONLY

DATASET NAME	DATA SOURCE	CLASSIFICATION
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below
IntelPlus Filerooms	FBI IntelPlus	Secret and below
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below
VGTOF	FBI National Crime Information Center (NCIC)	SBU
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below
Open Source News	MiTAP	Unclassified

Comment: ACS = Automated Case Support

b2
b7E

Outside the Scope

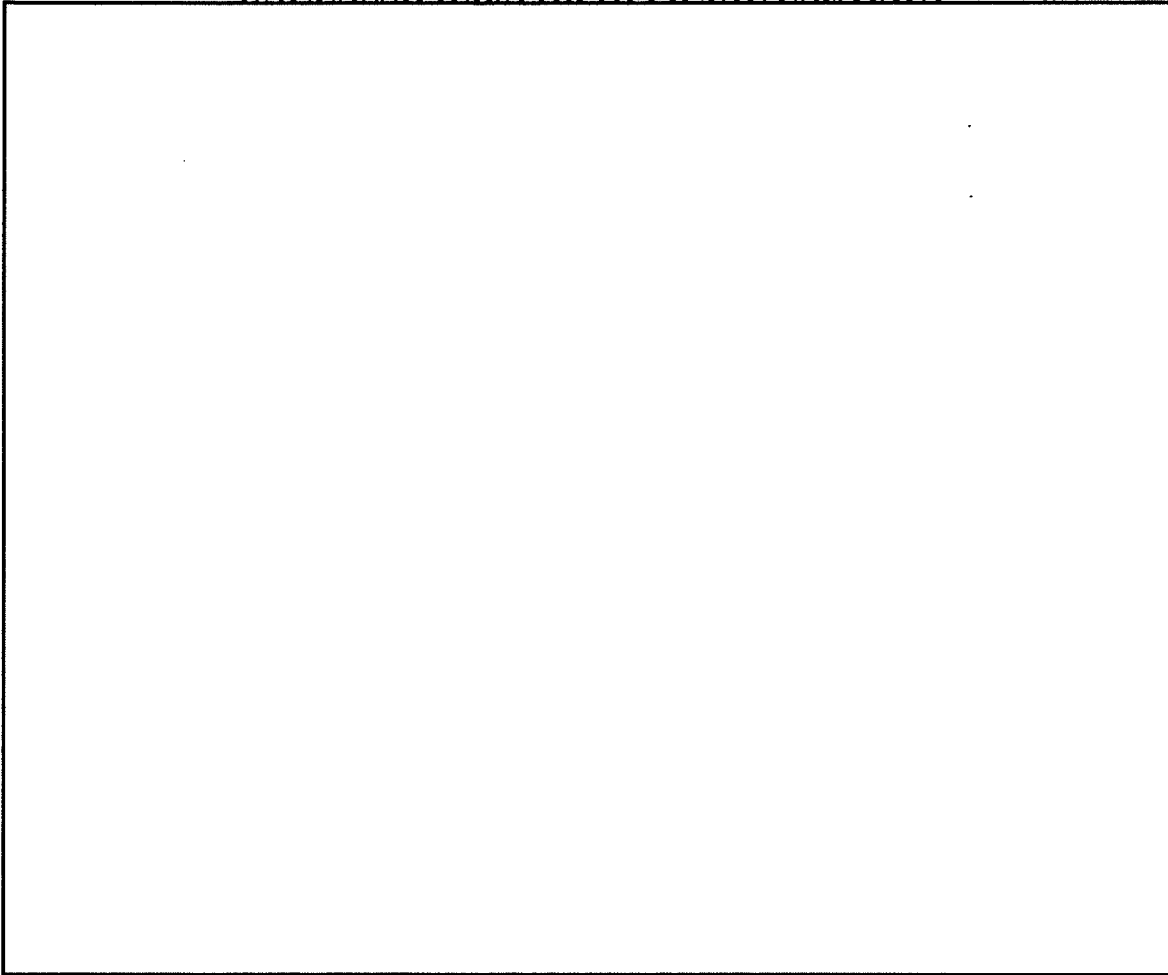**Operational Subsystem Data Sources**

The data flow begins at the external data sources. These sources include various FBI databases including ACS, SAMNET, Intelplus and several others.

Outside the Scope

The table below lists the data and sources for the SPT Subsystem.

Outside the Scope

12

DATASET TYPE	DATA SOURCE	CLASSIFICATION	
FBI Case Data	FBI Automated Case System (ACS)	Secret and below	
Financial Center (FinCen) Data		SBU	
Various Lists of Data	Various Sources, e.g., Transportation Security Administration (TSA)	SBU	
Various CTD Datasets	FBI Counterterrorism Division (CTD)	Secret and below	
Telephone Data	Database of telephone numbers from ACS indexed by phone number, names, addresses, and case numbers	Secret and below	

b2
b7E

SPT Data Sets

Outside the Scope

13

Jarmel-sanchez

HighView Image
06/16/08   07:33

FEDERAL BUREAU OF INVESTIGATION

OFFICE OF THE PROGRAM MANAGEMENT EXECUTIVE

Security Concept of Operations (S-CONOPS)
Investigative Data Warehouse (IDW)

(IDW-S, IDW-I, SPT Subsystem, & DocLab)
Document Version 1.1

June 18, 2004

DATASET NAME	DATA SOURCE	CLASSIFICATION
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below
IntelPlus Filerooms	FBI IntelPlus	Secret and below
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below
VGTOF	FBI National Crime Information Center (NCIC)	SBU
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below
Open Source News	MiTAP	Unclassified

b2
b7E

Operational Subsystem Data Sources

The data flow begins at the external data sources. These sources include various FBI databases including ACS, SAMNET, Intelplus and several others.

Outside the Scope

Outside the Scope

2.3.2   Special Projects Team (SPT) Subsystem

The Special Projects Team (SPT) Subsystem allows for the rapid import of new specialized data sources. These data sources are not made available to the general IDW users but instead are provided to a small group of users who have a demonstrated "need-to-know". The SPT System is similar in function to the IDW-S system. With the main difference is a different set of data sources. The SPT System allows it's users to access not only the standard IDW Data Store but the specialized SPT Data Store.

The table below lists the data and sources for the SPT Subsystem.

DATASET TYPE	DATA SOURCE	CLASSIFICATION
FBI Case Data	FBI Automated Case System (ACS)	Secret and below
Financial Center (FinCen) Data		SBU
Various Lists of Data	Various Sources, e.g., Transportation Security Administration (TSA)	SBU
Various CTD Datasets	FBI Counterterrorism Division (CTD)	Secret and below
Telephone Data	Database of telephone numbers from ACS indexed by phone number, names, addresses, and case numbers	Secret and below

b2
b7E

SPT Data Sets

Outside the Scope

FEDERAL BUREAU OF INVESTIGATION

Office of IT Program Management

INVESTIGATIVE DATA WAREHOUSE

DEVELOPMENT SYSTEM (IDW-D)

SYSTEM SECURITY PLAN

DOCUMENT VERSION 1.2

AUGUST 2005

Examples of unclassified operational data processed by the IDW-D system include:

-
-
- Violent Gang and Terrorist Organization File (VGTOF)

b2
b7E

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Draft
Investigative Data Warehouse Secret Development System
System Security Plan
17 August 2004
Draft Version 0.6

# FEDERAL BUREAU OF INVESTIGATION

Office of IT Program Management

INVESTIGATIVE DATA WAREHOUSE

CLASSIFIED DEVELOPMENT SYSTEM (IDW-DS)

SYSTEM SECURITY PLAN

DOCUMENT VERSION 0.6

17 AUGUST 2004

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Draft
Investigative Data Warehouse Secret Development System
System Security Plan
17 August 2004
Draft Version 0.6

Outside the Scope

- Approved case files from the FBI's Automated Case Support (ACS) Electronic Case File (ECF) case management system,

- Secure Automated Messaging Network (SAMNet) message traffic,

- IntelPlus File Rooms,

-

-

-

b2
b7E

- Universal Name Index (UNI), and

- Violent Gang and Terrorist Organization File (VGTOF") from the Criminal Justice Information Systems (CJIS) Division.

Outside the Scope

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Draft
Investigative Data Warehouse Secret Development System
System Security Plan
17 August 2004
Draft Version 0.6

Outside the Scope

- Approved case files from the FBI's ACS ECF case management system;

- Electronic versions of the JICI) defined archived documents;

- SAMNet message traffic;

UNCLASSIFIED // FOR OFFICIAL USE ONLY
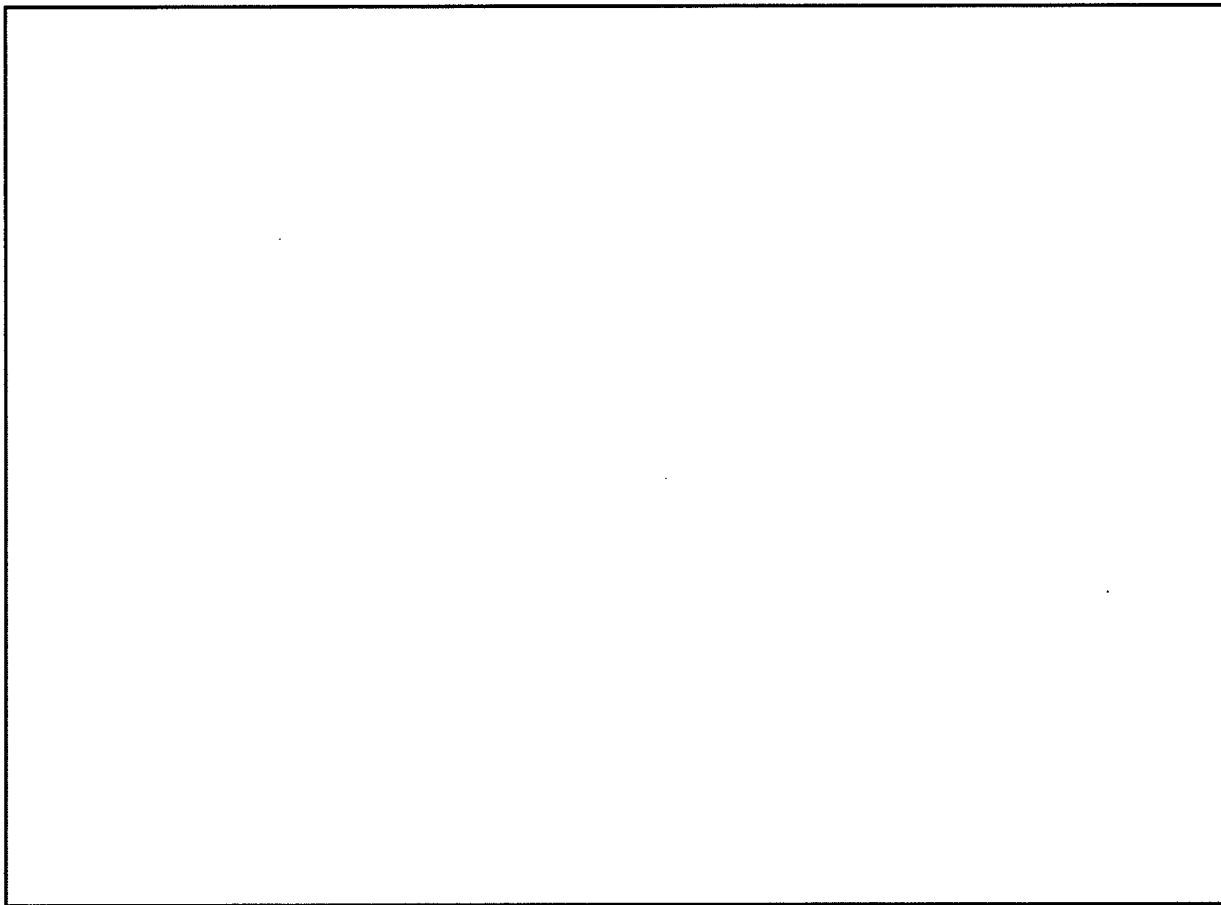Draft
Investigative Data Warehouse Secret Development System
System Security Plan
17 August 2004
Draft Version 0.6

- IntelPlus File Rooms;

[ ]

[ ]

[ ]

b2
b7E

- UNI, and

- VGTOF from CJIS Division.

Outside the Scope

-31-

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Draft
Investigative Data Warehouse Secret Development System
System Security Plan
25 October 2004
Draft Version 0.7

FEDERAL BUREAU OF INVESTIGATION

Office of IT Program Management

INVESTIGATIVE DATA WAREHOUSE

CLASSIFIED DEVELOPMENT SYSTEM (IDW-DS)

SYSTEM SECURITY PLAN

DOCUMENT VERSION 0.7

25 OCTOBER 2004

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Draft
Investigative Data Warehouse Secret Development System
System Security Plan
25 October 2004
Draft Version 0.7
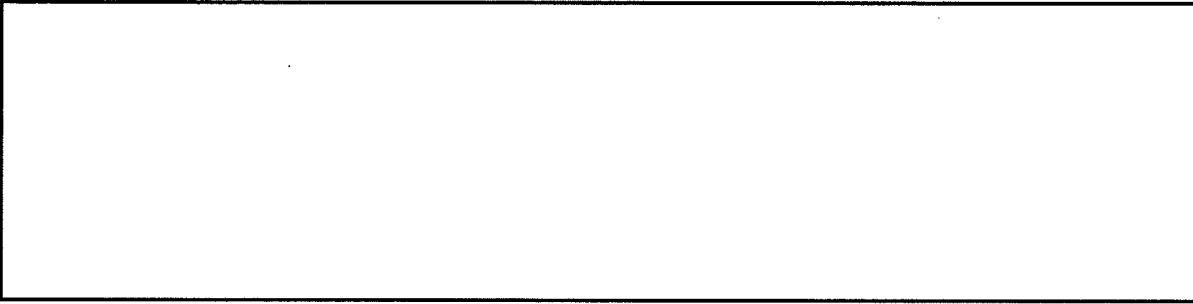
[   ]

- Approved case files from the FBI's Automated Case Support (ACS) Electronic Case File (ECF) case management system,

- Secure Automated Messaging Network (SAMNet) message traffic,

- IntelPlus File Rooms,

- [   ]

- [   ]   b2
                                                                               b7E
- [   ]

- Universal Name Index (UNI), and

- Violent Gang and Terrorist Organization File (VGTOF") from the Criminal Justice Information Systems (CJIS) Division.

[   ]

Outside the Scope

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Draft
Investigative Data Warehouse Secret Development System
System Security Plan
25 October 2004
Draft Version 0.7
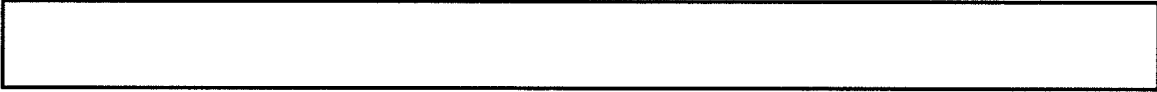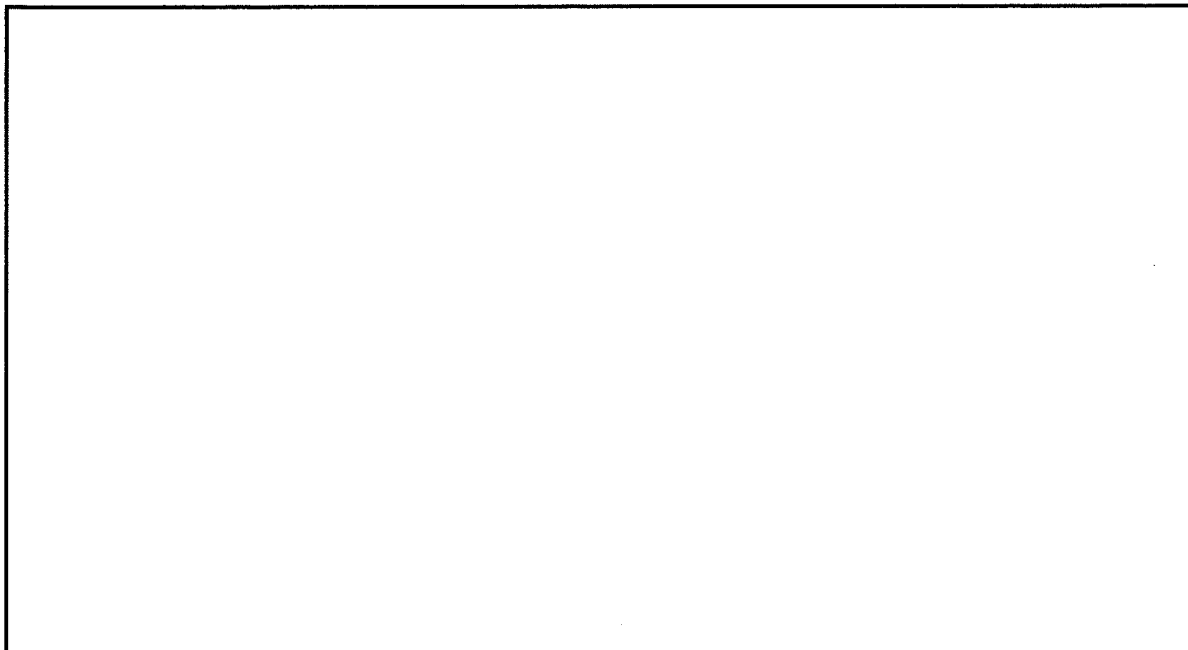
3.5. DATA PROCESSED

Outside the Scope
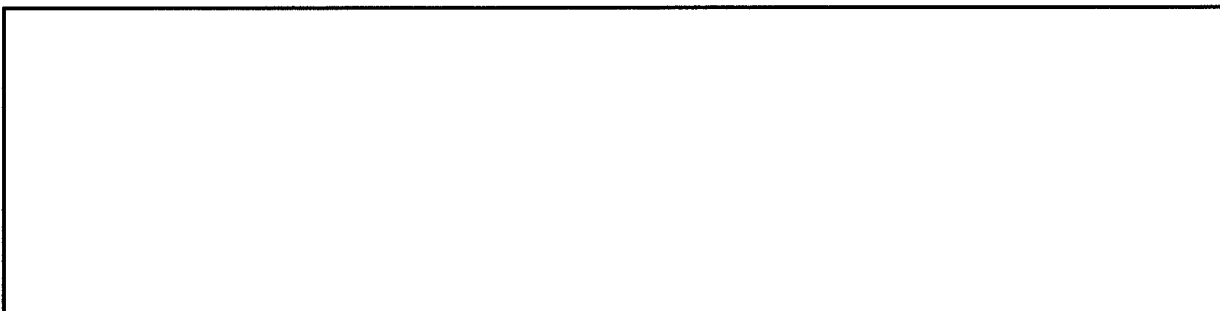
The IDW-DS system includes the following types of data. Representative samples of these data sets are used. Enough data is available in order to support development while minimizing the security risk.

- Approved case files from the FBI's ACS ECF case management system;

- Electronic versions of the JICI) defined archived documents;

- SAMNet message traffic;

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Draft
Investigative Data Warehouse Secret Development System
System Security Plan
25 October 2004
Draft Version 0.7

- IntelPlus File Rooms;

b2
b7E

- UNI, and

- VGTOF from CJIS Division.

-31-

Outside the Scope

Jarmel-sanchez

FEDERAL BUREAU OF INVESTIGATION

INFORMATION RESOURCES DIVISION

DATA AND INFORMATION MANAGEMENT SECTION
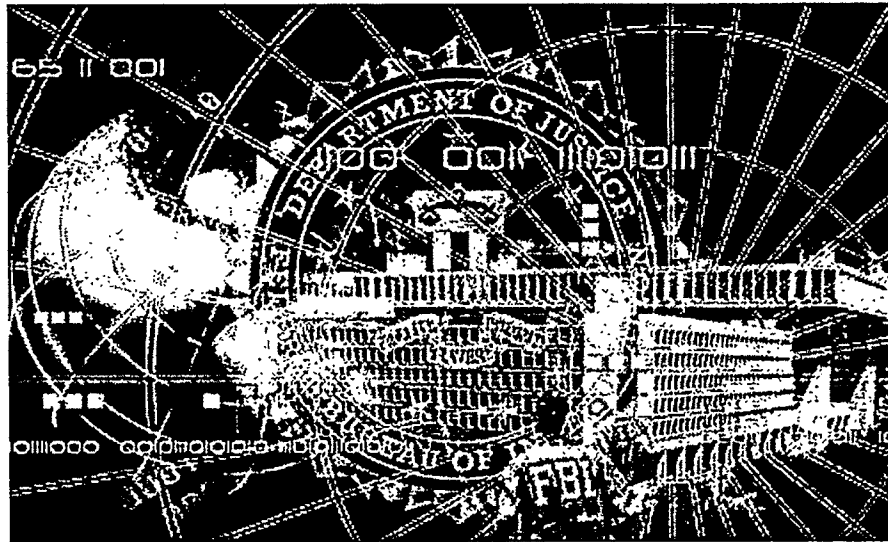
INVESTIGATIVE DATA WAREHOUSE – SECRET (IDW-S)

SYSTEM SECURITY PLAN

DOCUMENT VERSION 1.3

23 JUNE 2004

3.1.3.1 IDW-S Core Subsystem Data and Data Processing

The IDW-S Core Subsystem holds and processes data from the following approved data sources:

- Serialized Electronic Case File (ECF) documents in approved case files from the FBI's Automated Case Support (ACS) system
- IntelPlus Headquarters CT FileRooms
- Secure Automated Messaging Network (SAMNet) message traffic
- Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents
- Violent Gang and Terrorist Organization File (VGTOF) from the Criminal Justice Information Systems (CJIS) Division
- Open Source News

-25-
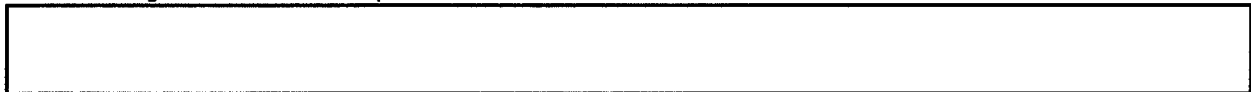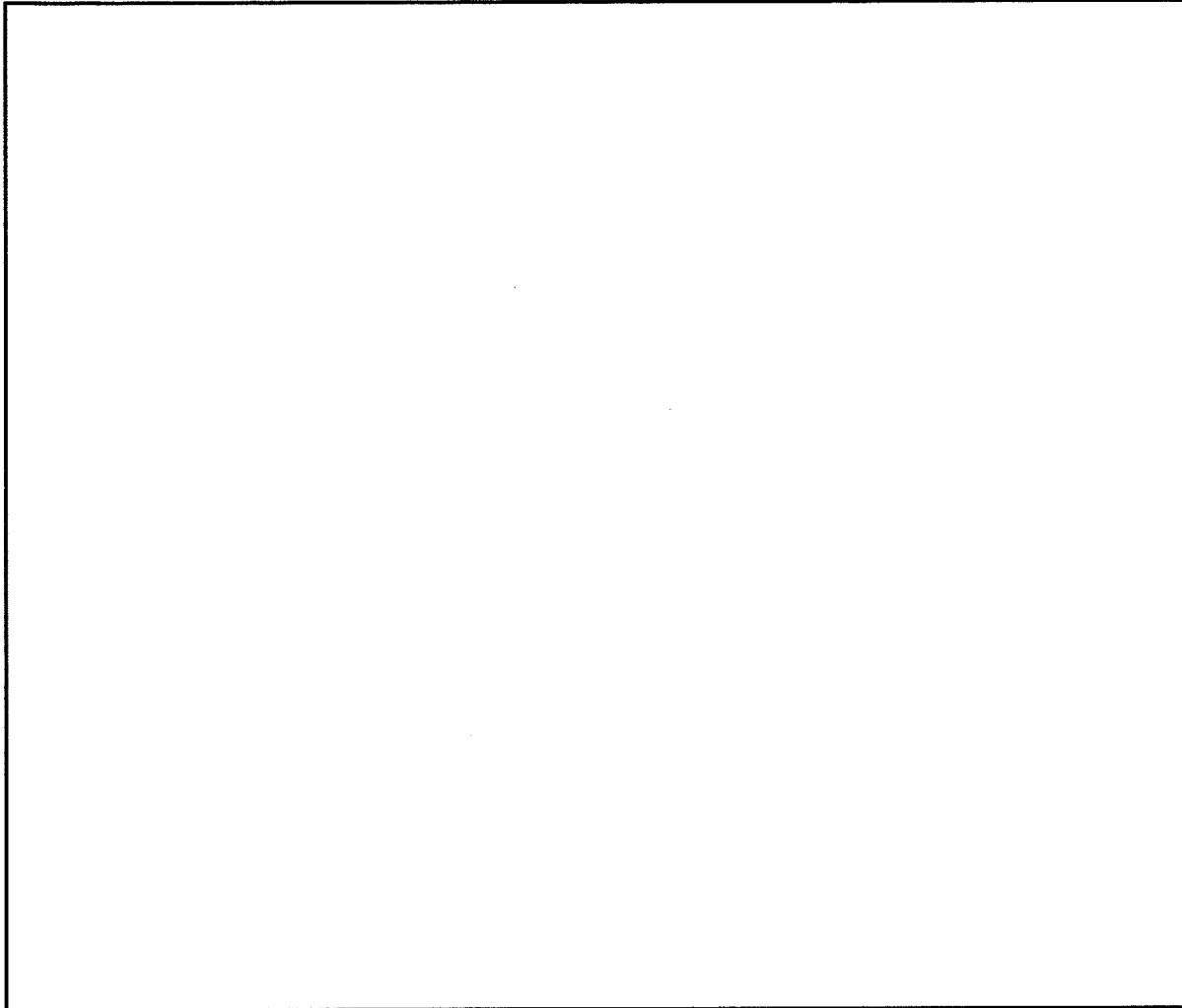
Outside the Scope

3.9.9 Indirect Connections

Outside the Scope

3.9.9.1 IDW-S Core Subsystem Indirect Connections

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	
FBI Automated Case System (ACS)	Secret	FBI	FTP	

b2
b7E

-46-

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	
FBI Intel Plus	Secret	FBI	FTP	
FBI Secure Automated Messaging Network (SAMNet)	Secret	FBI	FTP	
FBI Document Conversion Laboratory (DocLab), Records Management Division (RMD), FBIHQ	Secret	FBI	CD/DVD	
Transfer By CD-ROM, Disk, etc. (No connections to IDW-S)				
FBI National Crime Information Center (NCIC)	Unclassified/SBU	FBI	CD-ROM	
MiTAP	Unclassified	NA	CD-ROM	

b2
b7E

-47-

FEDERAL BUREAU OF INVESTIGATION

OFFICE OF THE PROGRAM MANAGEMENT EXECUTIVE

Security Concept of Operations (S-CONOPS)
Investigative Data Warehouse (IDW)

Document Version 1.2.2

December 22, 2004

Outside the Scope

The table below lists the data and sources for the Operational Subsystem.

DATASET NAME	DATA SOURCE	CLASSIFICATION
ACS Electronic Case Files (ECF)	FBI Automated Case Support (ACS)	Secret and below
IntelPlus Filerooms	FBI IntelPlus	Secret and below
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below
VGTOF	FBI National Crime Information Center (NCIC)	SBU
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below
Open Source News	MiTAP	Unclassified

b2
b7E

Operational Subsystem Data Sources

Outside the Scope

The table below lists the data and sources for the SPT Subsystem.   Outside the Scope

DATASET TYPE	DATA SOURCE	CLASSIFICATION
FBI Case Data	FBI Automated Case System (ACS)	Secret and below
Financial Center (FinCen) Data		SBU
Various Lists of Data	Various Sources, e.g., Transportation Security Administration (TSA)	SBU
Various CTD Datasets	FBI Counterterrorism Division (CTD)	Secret and below
Telephone Data	Database of telephone numbers from ACS indexed by phone number, names, addresses, and case numbers	Secret and below

b2
b7E

SPT Data Sets

Outside the Scope

FEDERAL BUREAU OF INVESTIGATION
INFORMATION RESOURCES DIVISION
DATA AND INFORMATION MANAGEMENT SECTION

INVESTIGATIVE DATA WAREHOUSE – SECRET (IDW-S)

SYSTEM SECURITY PLAN

DOCUMENT VERSION 1.4

15 JANUARY 2005

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-22-2008 BY 65179 dmh/bja/cal

Outside the Scope

Automated Transfer of Raw Data to IDW-S

Raw data is automatically transferred to the IDW-S system from approved data sources in accordance with an Interconnection Agreement, Memorandum of Understanding, Memorandum of Agreement or Interface Control Document. IDW-S V1 receives update data by the following means:

- ACS update data is transmitted to the IDW-S system
- IntelPlus update data is transmitted to the IDW-S system
- SAMNet update data is transmitted to the IDW-S system
- VGTOF data is transmitted to the IDW-S system
- Open Source News data is transmitted to the IDW-S system
- The JICI library is static and is not updated on IDW-S V1.

b2
b7E

(blank box)

3.5.1 Data Processed

Outside the Scope

3.5.1.1 IDW-S Core Subsystem Data Processed

Table 3.5.1.1 below outlines the IDW-S datasets and information about transfer and ingest processing for each source.

DATASET NAME	DATA SOURCE	CLASSIFICATION	
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below	

b2
b7E

DATASET NAME	DATA SOURCE	CLASSIFICATION	
IntelPlus Filerooms	FBI IntelPlus	Secret and below	
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below	
VGTOF	FBI National Crime Information Center (NCIC)	SBU	
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below	
Open Source News	MiTAP	Unclassified	

Table 3.5.1.1 IDW-S Data Sets

b2
b7E

Outside the Scope

3.9.9 Indirect Connections

3.9.9.1 IDW-S Core Subsystem Indirect Connections

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	
FBI Automated Case System (ACS)	Secret	FBI	FTP	
FBI Intel Plus	Secret	FBI	FTP	
FBI Secure Automated Messaging Network (SAMNet)	Secret	FBI	FTP	
FBI National Crime Information Center (NCIC)	Unclassified/SBU	FBI	CD-ROM	
FBI Document Conversion Laboratory (DocLab), Records Management Division (RMD), FBIHQ	Secret	FBI	CD/DVD	

b2
b7E

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	
MiTAP – Open Source News	Unclassified	NA	CD-ROM	

b2
b7E

Outside the Scope

Federal Bureau of Investigation
Information Resources Division
Data Management Section

Investigative Data Warehouse
Privileged Users Guide
Version 1.1 for Authority to Operate
June 11, 2004

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-22-2008 BY 65179 dmh/bja/cal

Outside the Scope

IDW-S contains data from the following data sources with security classification indicated in brackets:

Automated Case Support (ACS) System, Electronic Case File (ECF) Subsystem [Secret and below]

IntelPlus [Secret and below]

Secure Automated Message Network – Secret (SAMNet-S) [Secret and below]

NCIC Violent Gang and Terrorist Offender File (VGTOF) [Sensitive But Unclassified]

Joint Intelligence Committee Investigation (JICI) [Secret and below]

DARPA/TIDES Open Source News [Unclassified]

Data from each source is held in an identified source Library against which users can direct the analytical tools.

b2
b7E

IDW receives data from sources [   ] over FBINet (ACS ECF, IntelPlus, and SAMNet) and [   ] (VGTOF, Open Source News).

Outside the Scope

Federal Bureau of Investigation
Information Resources Division
Data Management Section

Investigative Data Warehouse
Security Operations Manual
Version 1.1 for Authority to Operate
June 11, 2004

Data used in the SES subsystem comes from
- The standard, customary, data sources for the IDW
- Several SES-unique data sources which are provided for use by a subset of the IDW users.

The SES-specific data sources will include
- Financial Center (FinCen)
-
- NoFly
- Selectee
-
-
-
-
- Unified Name Index (UNI) extracts
-

b2
b7E

Outside the Scope

Note: Hardcopy versions of this document must be verified for correct version number with the IDW CM Document Control Library.

SECOM NG-OM-006.11ATO
FOR OFFICIAL USE ONLY
Page 0
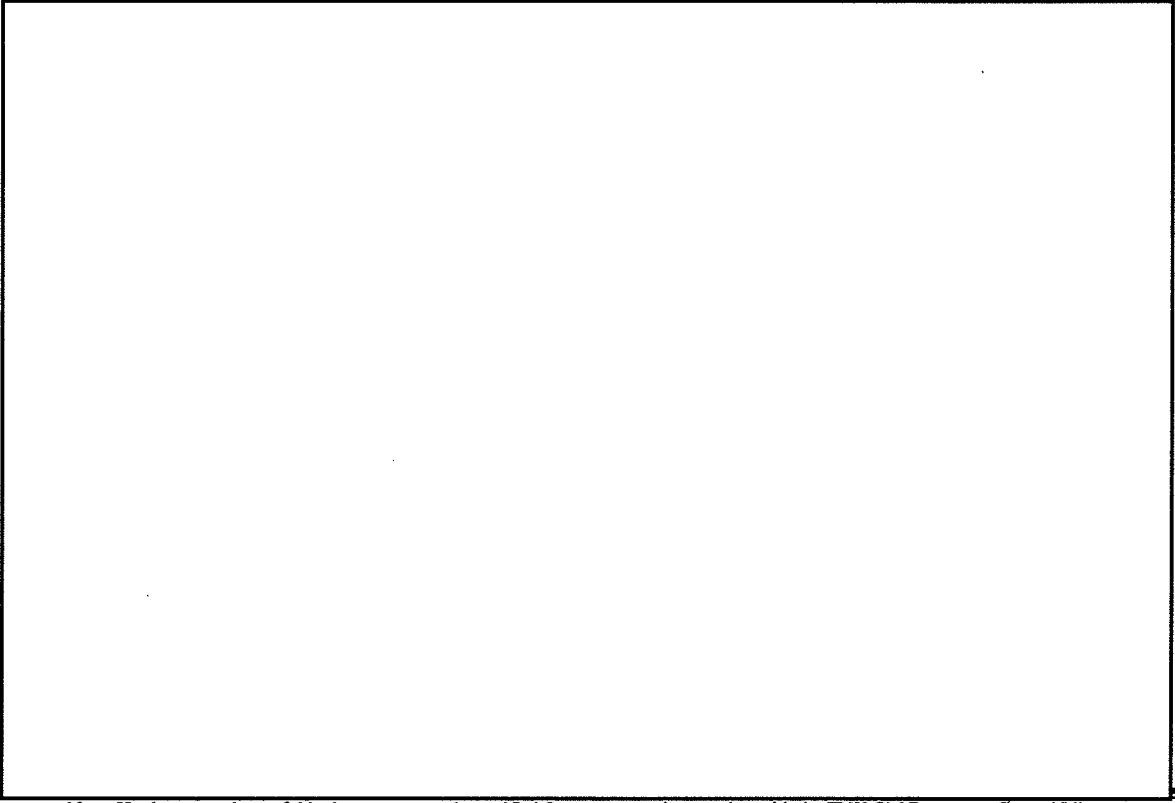
2 System Security Overview

Outside the Scope

Data processed by the system will include the following data sets:
- Approved case files from the FBI's Automated Case Support (ACS) case management system;
- Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents;
- Secure Automated Messaging Network (SAMNet) message traffic;
- IntelPlus File Rooms; and

- Violent Gang and Terrorist Organization File (VGTOF") from the Criminal Justice Information Systems (CJIS) Division;
- Defense Advanced Research Projects Agency (DARPA) Translingual Information Detection, Extraction and Summarization (TIDES) Open Source Data

Outside the Scope

Note: Hardcopy versions of this document must be verified for correct version number with the IDW CM Document Control Library.
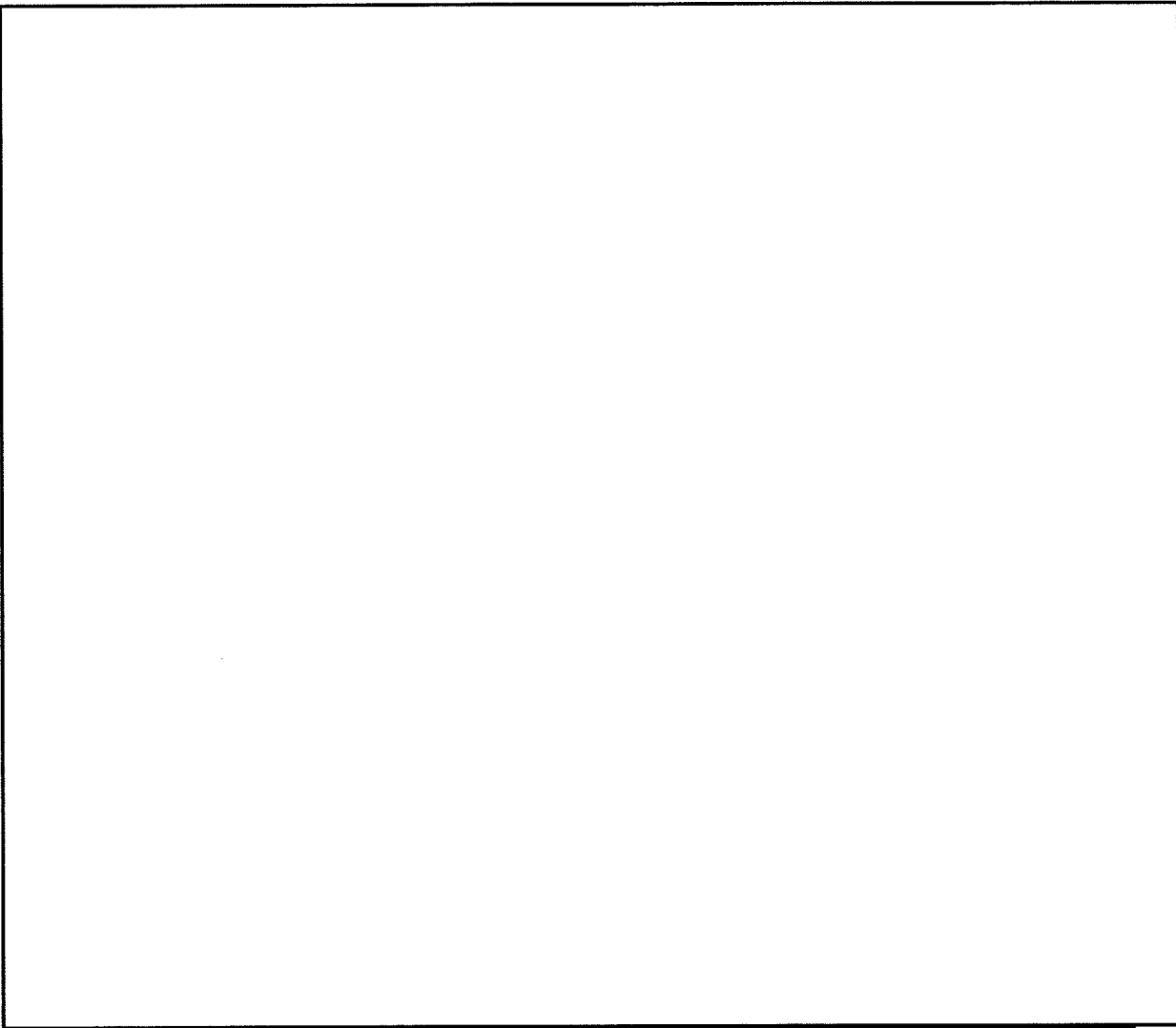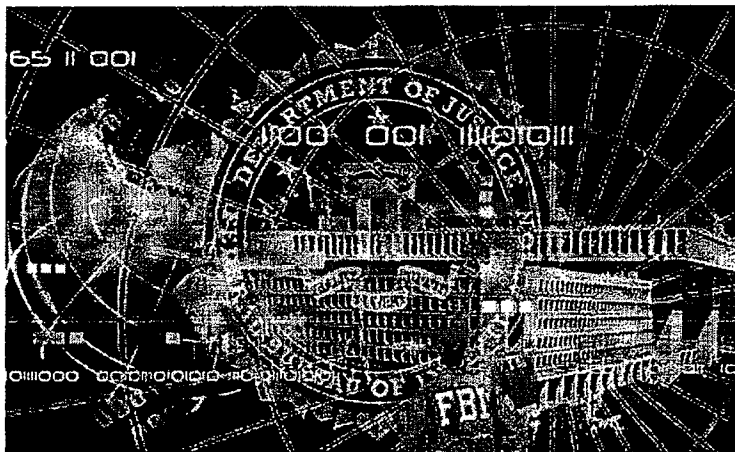
SECOM NG-OM-006.11ATO
FOR OFFICIAL USE ONLY
Page 0

IDW contains data from the following data sources with security classification indicated in brackets:

- Automated Case Support (ACS) System, Electronic Case File (ECF) Subsystem [Secret and below]
- IntelPlus [Secret and below]
- Secure Automated Message Network – Secret (SAMNet-S) [Secret and below]
- NCIC Violent Gang and Terrorist Offender File (VGTOF) [Sensitive But Unclassified]
- Joint Intelligence Committee Investigation (JICI) [Secret and below]
- DARPA/TIDES Open Source News [Unclassified]   Outside the Scope

Note: Hardcopy versions of this document must be verified for correct version number with the IDW CM Document Control Library.

SECOM NG-OM-006.11ATO
FOR OFFICIAL USE ONLY
Page 0

FEDERAL BUREAU OF INVESTIGATION
INFORMATION RESOURCES DIVISION
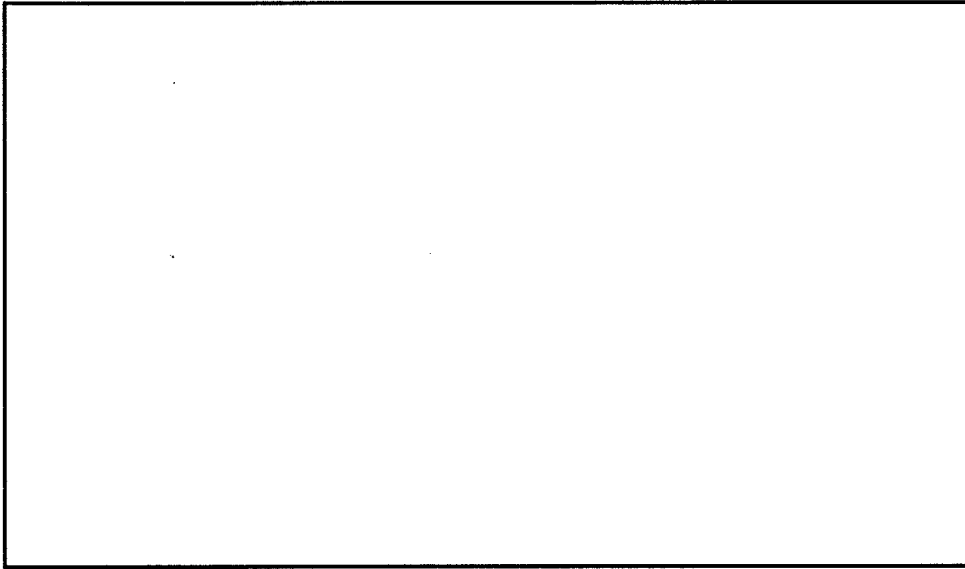## DATA AND INFORMATION MANAGEMENT SECTION

INVESTIGATIVE DATA WAREHOUSE – SECRET (IDW-S)

SYSTEM SECURITY PLAN

DOCUMENT VERSION 1.4

20 DECEMBER 2004

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-17-2008 BY 65179 dmh/bja/cal

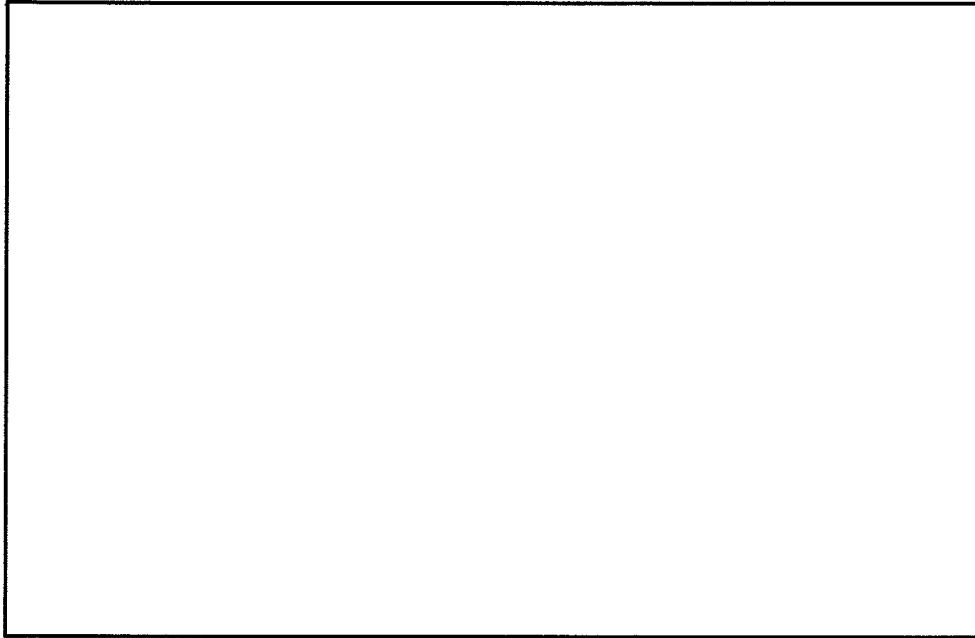'Outside the Scope

Automated Transfer of Raw Data to IDW-S

Raw data is automatically transferred to the IDW-S system from approved data sources in accordance with an Interconnection Agreement, Memorandum of Understanding, Memorandum of Agreement[   ]receives update   b2
data by the following means: b7E

- ACS update data is
- IntelPlus update data
- SAMNet update data

- VGTOF data
- Open Source News data
- The JICI library is static and is not updated

'Outside the Scope

3.5.1.1 IDW-S Core Subsystem Data Processed

'Outside the Scope

Table 3.5.1.1 below outlines the IDW-S datasets and information about transfer and ingest processing for each source.
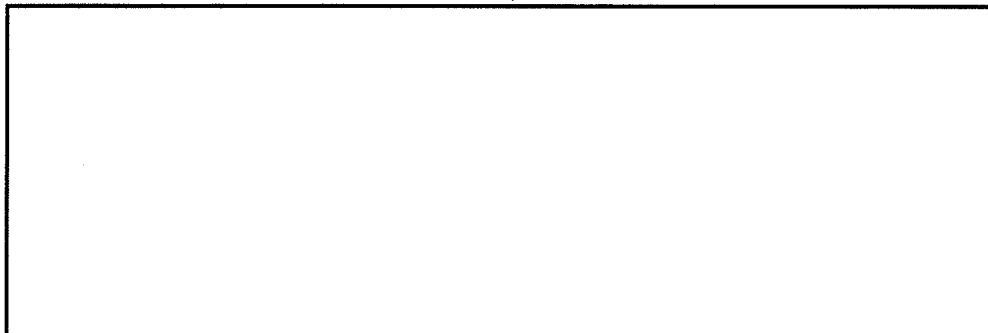
DATASET NAME	DATA SOURCE	CLASSIFICATION	
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below	

b2
b7E

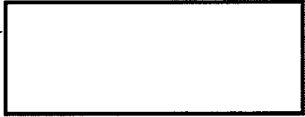| DATASET NAME	DATA SOURCE	CLASSIFICATION
IntelPlus Filerooms	FBI IntelPlus	Secret and below
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below
VGTOF	FBI National Crime Information Center (NCIC)	SBU
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below
Open Source News	MiTAP	Unclassified

b2
b7E

Table 3.5.1.1 IDW-S Data Sets

b2
b7E

-44-

3.9.9 Indirect Connections

3.9.9.1 IDW-S Core Subsystem Indirect Connections

SYSTEM NAME	CLASSIFICATION COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD
FBI Automated Case System (ACS)	Secret	FBI	FTP
FBI Intel Plus	Secret	FBI	FTP
FBI Secure Automated Messaging Network (SAMNet)	Secret	FBI	FTP
FBI National Crime Information Center (NCIC)	Unclassified/SBU	FBI	CD-ROM
FBI Document Conversion Laboratory (DocLab), Records Management Division (RMD), FBIHQ	Secret	FBI	CD/DVD

Outside the Scope

b2
b7E

-51-

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
20 December 2004
Version 1.4

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD
MiTAP – Open Source News	Unclassified	NA	CD-ROM

b2
b7E

Outside the Scope

FEDERAL BUREAU OF INVESTIGATION

OFFICE OF THE PROGRAM MANAGEMENT EXECUTIVE

Security Concept of Operations (S-CONOPS) Investigative Data Warehouse (IDW)
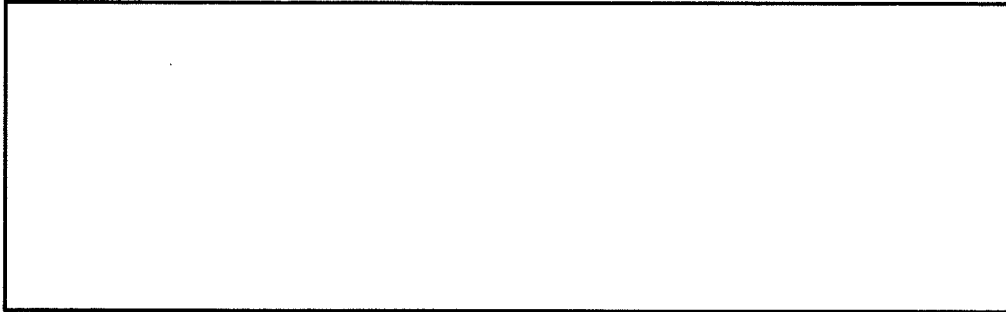
Document Version 1.2.3

February 7, 2004
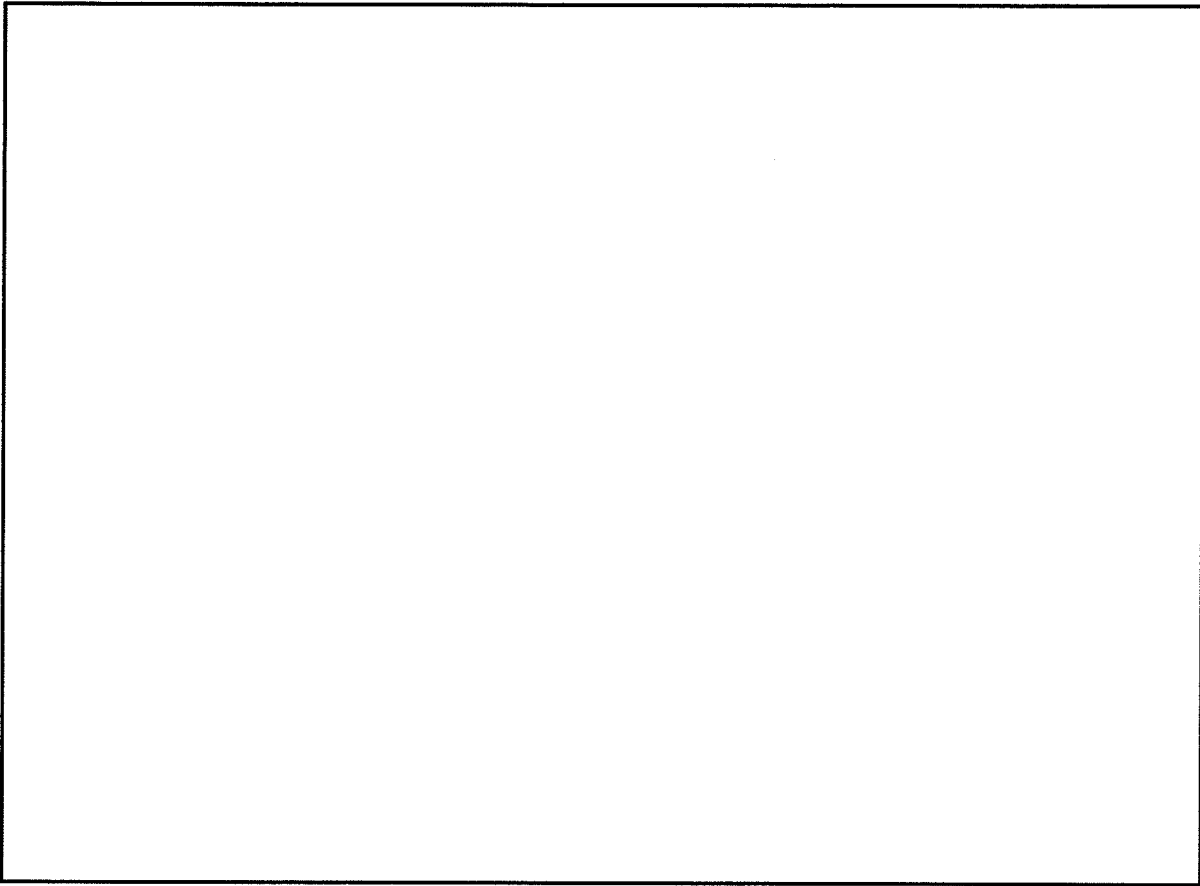
Outside the Scope

2.3.1 IDW-S Operational Subsystem

The table below lists the data and sources for the Operational Subsystem.

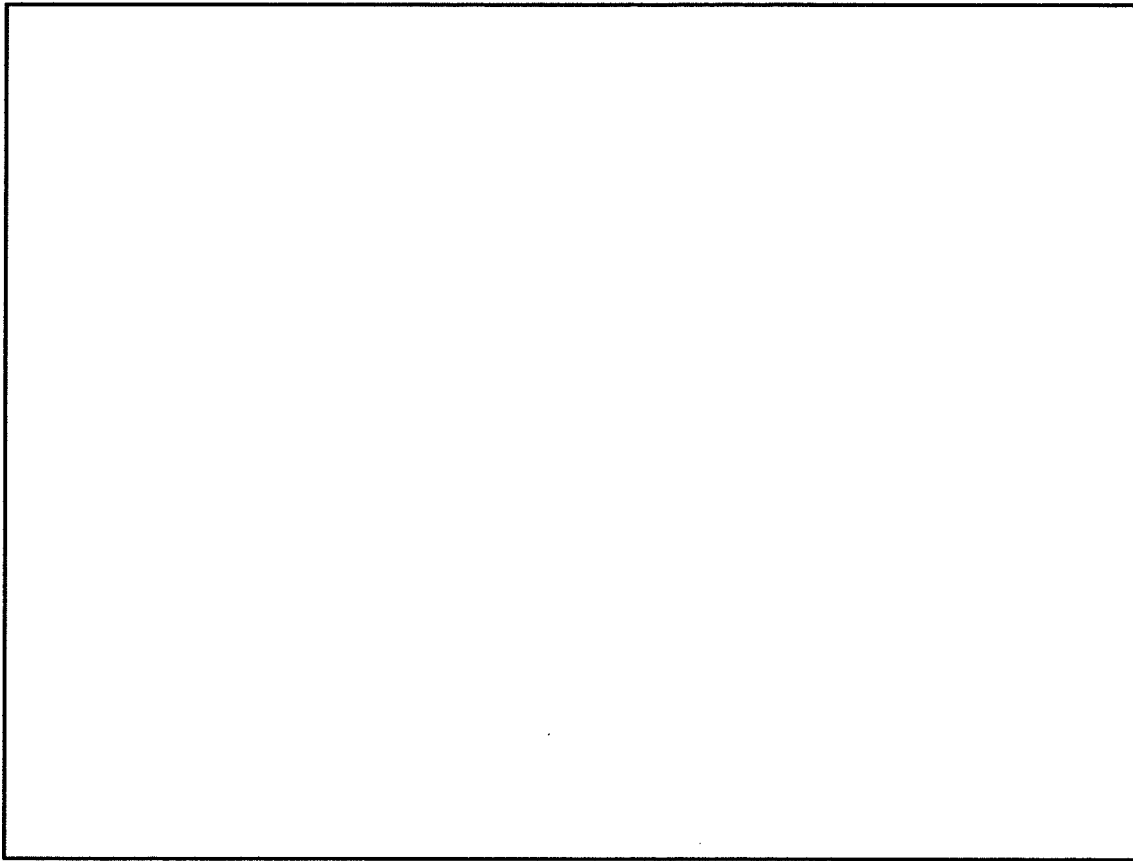| DATASET NAME	DATA SOURCE	CLASSIFICATION
ACS Electronic Case Files (ECF)	FBI Automated Case Support (ACS)	Secret and below
IntelPlus Filerooms	FBI IntelPlus	Secret and below
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below
VGTOF	FBI National Crime Information Center (NCIC)	SBU
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below
Open Source News	MiTAP	Unclassified

Operational Subsystem Data Sources

b2
b7E

The data flow begins at the external data sources. These sources include various FBI databases including ACS, SAMNET, Intelplus and several others.

Outside the Scope
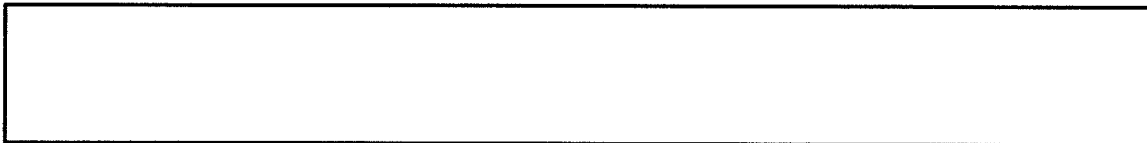
2.3.2   Special Projects Team (SPT) Subsystem

The table below lists the data and sources for the SPT Subsystem.

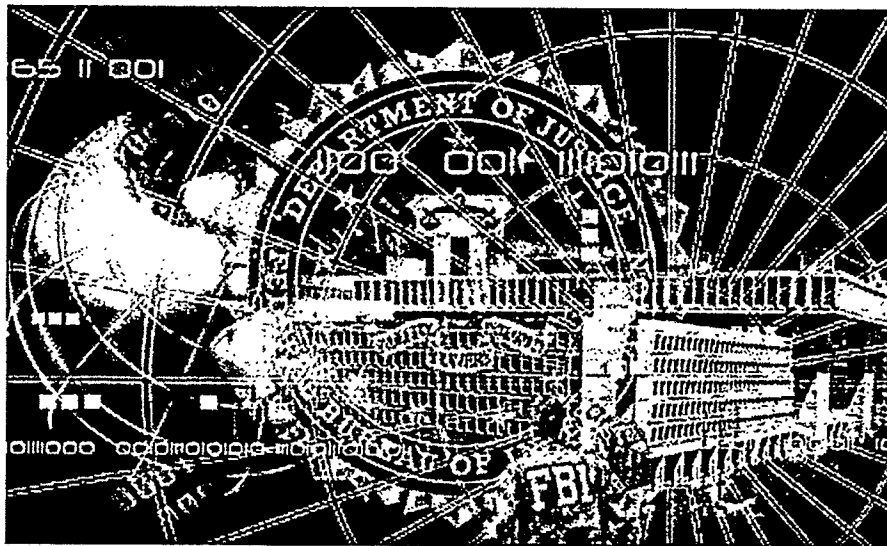| DATASET TYPE	DATA SOURCE	CLASSIFICATION	
FBI Case Data	FBI Automated Case System (ACS)	Secret and below	
Financial Center (FinCen) Data		SBU	
Various Lists of Data	Various Sources, e.g., Transportation Security Administration (TSA)	SBU	
Various CTD Datasets	FBI Counterterrorism Division (CTD)	Secret and below	
Telephone Data	Database of telephone numbers from ACS indexed by phone number, names, addresses, and case numbers	Secret and below	

b2
b7E

SPT Data Sets

Outside the Scope

FEDERAL BUREAU OF INVESTIGATION

INFORMATION RESOURCES DIVISION

DATA AND INFORMATION MANAGEMENT SECTION
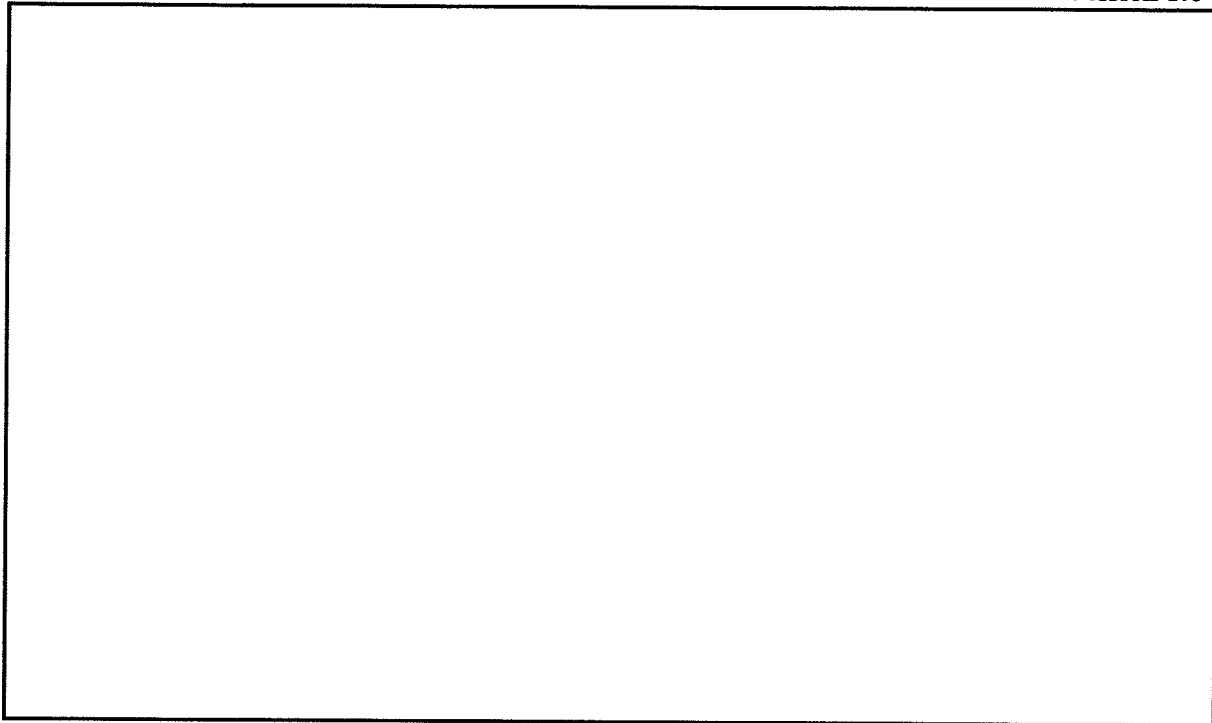

INVESTIGATIVE DATA WAREHOUSE – SECRET (IDW-S)

SYSTEM SECURITY PLAN

DOCUMENT VERSION 1.6

25 JANUARY 2005

Outside the Scope

Automated Transfer of Raw Data to IDW-S

Raw data is automatically transferred to the IDW-S system from approved data sources in accordance with an Interconnection Agreement, Memorandum of Understanding, Memorandum of Agreement or Interface Control Document. IDW-S V1 receives update data by the following means:

- ACS update data is transmitted to the IDW-S system

- IntelPlus update data is transmitted to the IDW-S system

- SAMNet update data is transmitted to the IDW-S system

- VGTOF data is transmitted to the IDW-S system
- Open Source News data is transmitted to the IDW-S system
- The JICI library is static and is not updated on IDW-S V1.

b2
b7E

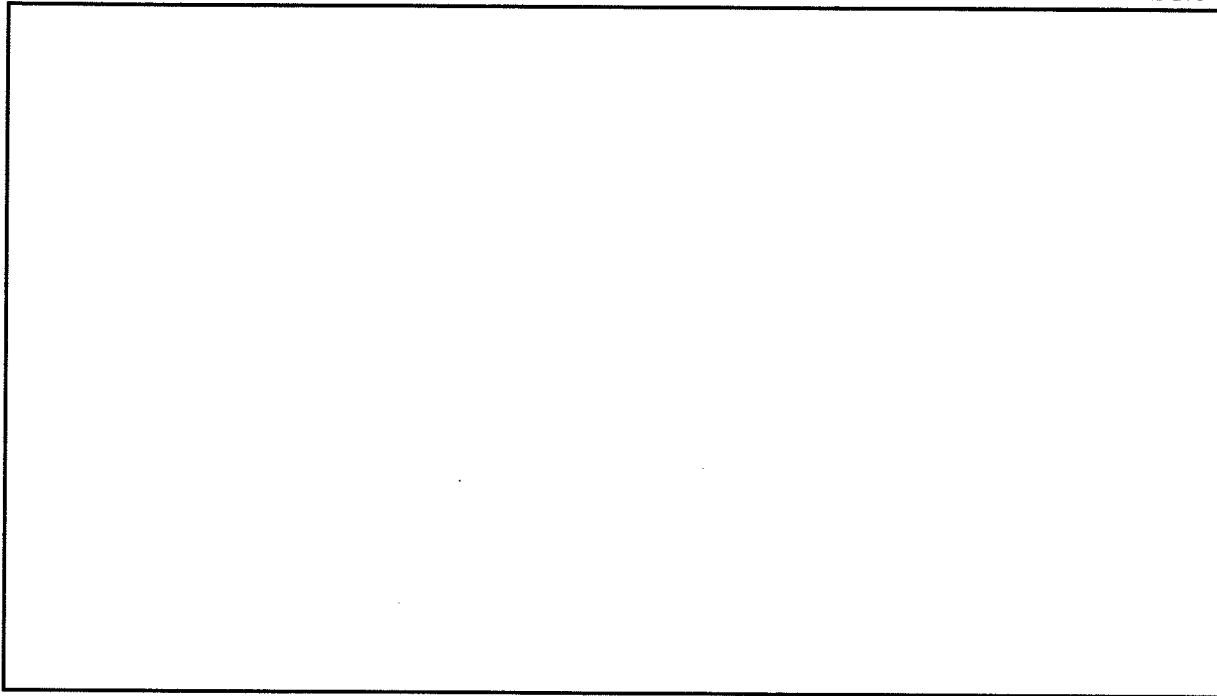data into individual serial records (in the case of ACS ECF),
documents (IntelPlus, JICI, Open Source News), messages (SAMNet), or files
(VGTOF).

Outside the Scope

Outside the Scope

3.5.1 Data Processed

3.5.1.1 IDW-S Core Subsystem Data Processed

Table 3.5.1.1 below outlines the IDW-S datasets and information about transfer and ingest processing for each source.
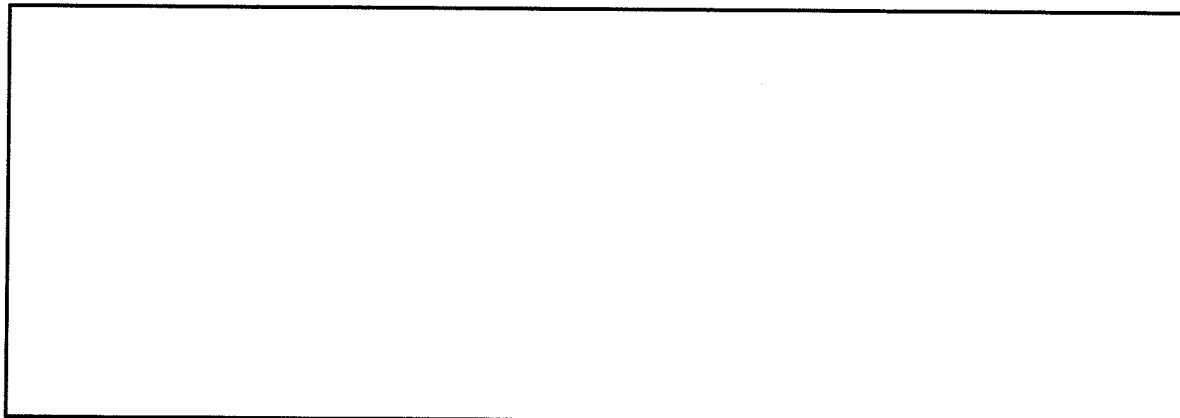
DATASET NAME	DATA SOURCE	CLASSIFICATION	
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below	

b2
b7E

DATASET NAME	DATA SOURCE	CLASSIFICATION	
IntelPlus Filerooms	FBI IntelPlus	Secret and below	
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below	
VGTOF	FBI National Crime Information Center (NCIC)	SBU	
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below	
Open Source News	MiTAP	Unclassified	

b2
b7E

Table 3.5.1.1 IDW-S Data Sets
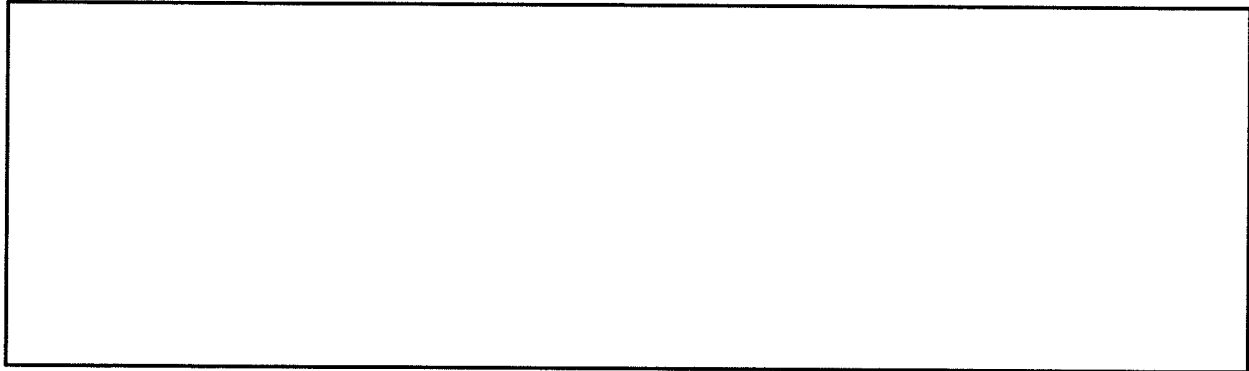
-38-

Outside the Scope

3.9.9 Indirect Connections

3.9.9.1 IDW-S Core Subsystem Indirect Connections

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD
FBI Automated Case System (ACS)	Secret	FBI	FTP
FBI Intel Plus	Secret	FBI	FTP
FBI Secure Automated Messaging Network (SAMNet)	Secret	FBI	FTP
FBI National Crime Information Center (NCIC)	Unclassified/SBU	FBI	CD-ROM
FBI Document Conversion Laboratory (DocLab), Records Management Division (RMD), FBIHQ	Secret	FBI	CD/DVD

b2
b7E

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD
MiTAP – Open Source News	Unclassified	NA	CD-ROM

b2
b7E

Outside the Scope

INVESTIGATIVE DATA WAREHOUSE

User Reference for
IDW Version 1.1
Applications

IDW Training Office
Federal Bureau of Investigation
Department of Justice
935 Pennsylvania Street • Room 10184
Washington, D.C. 20535
Phone 202.324.2606

Data Sources

1. ACS: Automated Case Support. **(CT Case Files)** Archived Investigative dating back through calendar year 1995. Updates pushed (FTP) to IDW once per day.

2. Intel Plus: Updates pushed (FTP) to IDW as needed (usually once per day).
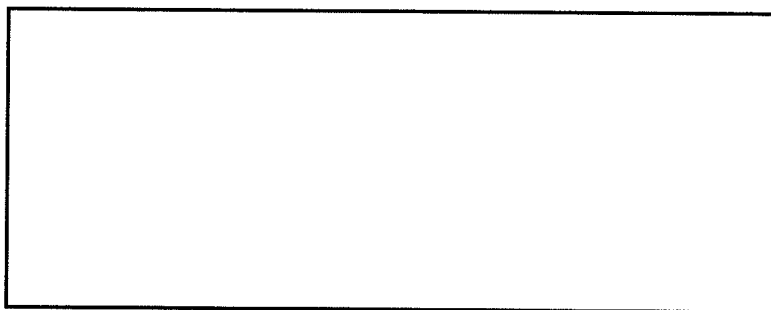
b2
b7E

3. JICI: Archived data from the Joint Intelligence Committee Investigation (JICI) regarding 9/11 as directed by the Congress of the United States. (Static file system)

4. ORCON: Parsed data from SAMNet and ACS data collections with this caveat. Pushed to IDW once per day.

5. SAMNet: SECRET and below cable traffic to/from FBI Headquarters. Pulled (FTP) from SAMNet server (IDW chronological job runs every 10 minutes; SAMNet posts new data 3 times per day).

6. TFRG: Terrorist Financial records. Updates pushed (FTP) to IDW once per day.

7. VGTOF: Violent Gang & Terrorist Offense File. Updated data file is provided in entirety by CD on a weekly basis.

8. OSINT: Open Source Research (OSINT): Current from the MiTAP server.

SYSTEM SECURITY PLAN

INVESTIGATIVE DATA WAREHOUSE-SECRET (IDW-S)

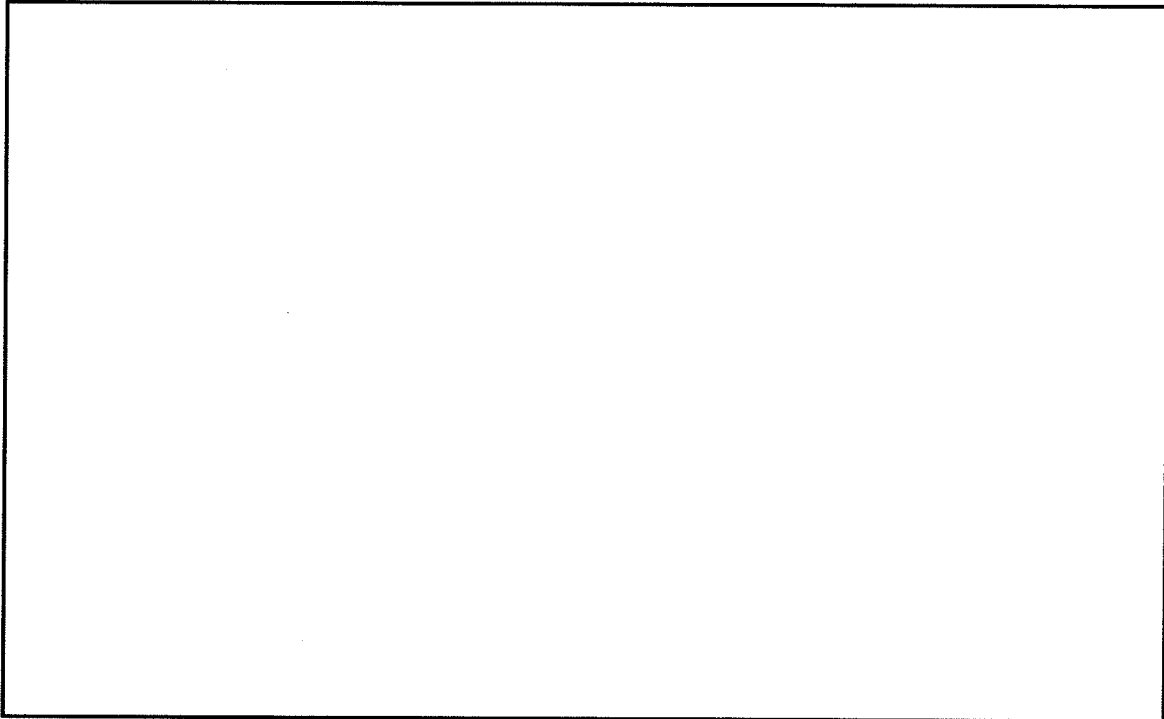## 21 NOVEMBER 2003

VERSION: 0.5

EDERAL BUREAU OF INVESTIGATION (FBI), INFORMATION RESOURCES DIVISION (IRD)

INVESTIGATIVE DATA WAREHOUSE (IDW) - SECRET

SYSTEM SECURITY PLAN

INTRODUCTION

The Federal Bureau of Investigation's (FBI) Investigative Data Warehouse (IDW-S) is an initial data warehouse, content management and data mining system that will permit FBI investigative, analytical, administrative and intelligence personnel to access aggregated data previously only available through individual applications. The IDW-S system will be authorized to process classified national security data up to, and including, Secret. The IDW-S system is the successor of the Secure Counter-Terrorism/Collaboration Operational Prototype Environment (SCOPE").
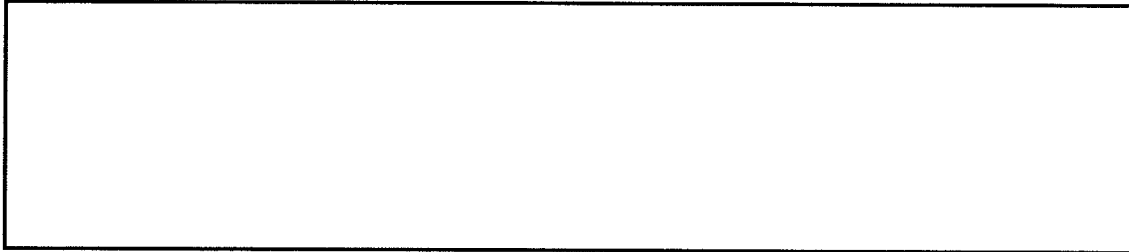
Data processed by the system will include the following data sets: Outside the Scope

- Approved case files from the FBI's Automated Case Support (ACS) case management system;

- Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents;

-1-

- Secure Automated Messaging Network (SAMNet) message traffic;

- IntelPlus File Rooms; and

- Violent Gang and Terrorist Organization File (VGTOF") from the Criminal Justice Information Systems (CJIS) Division;

- Defense Advanced Research Projects Agency (DARPA) Translingual Information Detection, Extraction and Summarization (TIDES) Open Source Data

Outside the Scope

-2-

Data Sources   Outside the Scope

IDW-S contains data from the following data sources with security classification indicated in brackets:

- Automated Case Support (ACS) System, Electronic Case File (ECF) Subsystem [Secret and below]

- IntelPlus [Secret and below]

- Secure Automated Message Network – Secret (SAMNet-S) [Secret and below]

- NCIC Violent Gang and Terrorist Offender File (VGTOF) [Sensitive But Unclassified]

- Joint Intelligence Committee Investigation (JICI) [Secret and below]

- DARPA/TIDES Open Source News [Unclassified]

Data Ingest

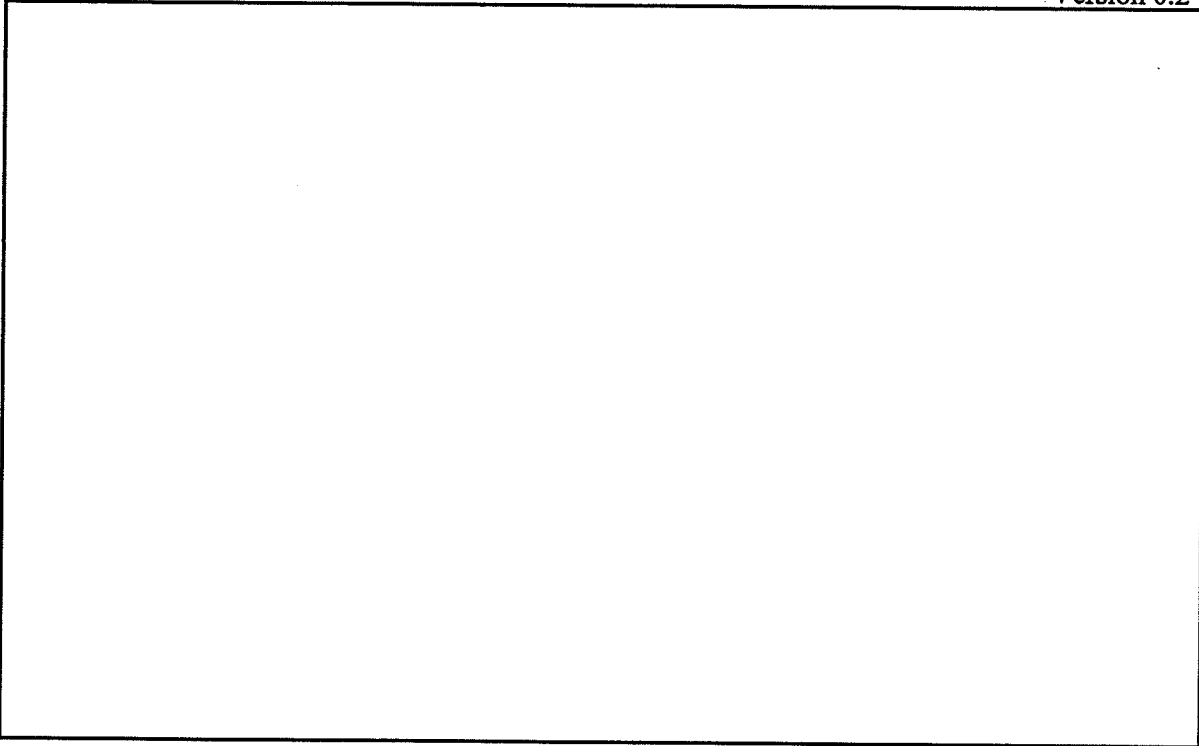IDW-S receives data from sources [ ] (ACS ECF, IntelPlus, SAMNet) and [ ] (VGTOF, Open Source News).

b2
b7E

- [ ]

- [ ]

  - Received data [ ] into individual serial records (in the case of ACS ECF), documents (IntelPlus, JICI, Open Source News), messages (SAMNet), or files (VGTOF).

- [ ]

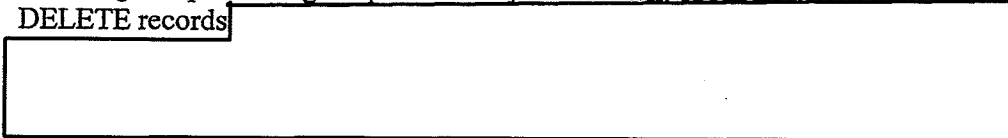-16-   Outside the Scope

Outside the Scope

3.5. DATA PROCESSED

IDW-S processes the following data:

3.5.1 ACS ECF

IDW-S contains a subset of the ECF (Electronic Case File) subsystem of the
Automated Case System (ACS). This subset consists of serials in those case
classifications/subclassifications that have been officially sanctioned for inclusion
in IDW. For each such serial, the ECF data includes metadata and text. IDW-S is
synchronized against the ECF system once a day, a process which consists of
receiving and processing the previous day's increment of ADD, MOD, and
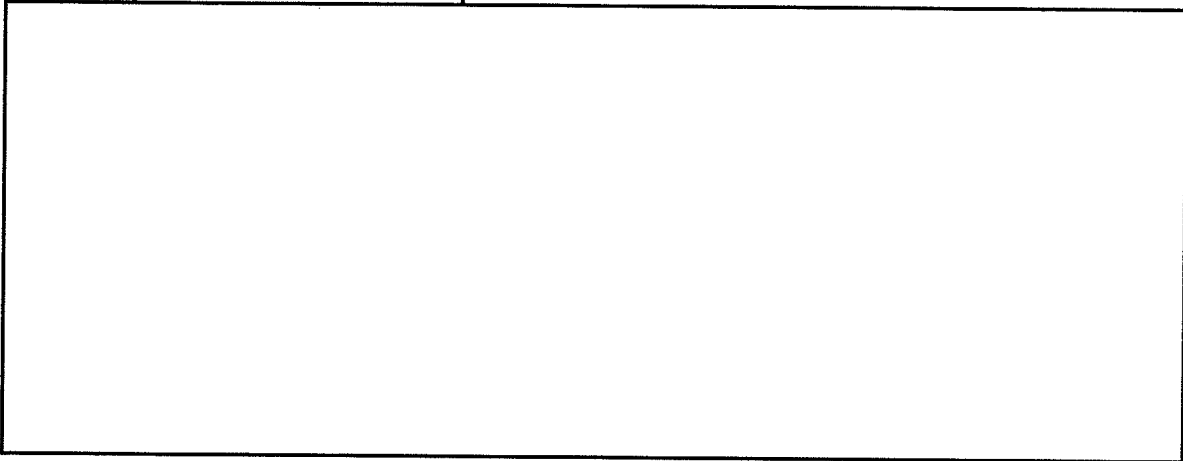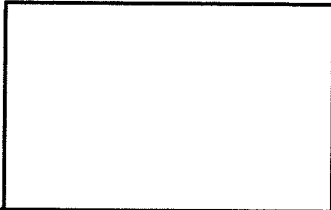DELETE records

b2
b7E

3.5.2 IntelPlus

IDW-S currently contains several IntelPlus counter-terrorism (CT) Filerooms:

-
-

-22-

b2
b7E

3.5.3   SAMNet

The Secure Automated Messaging Network (SAMNet) data source consists of cable
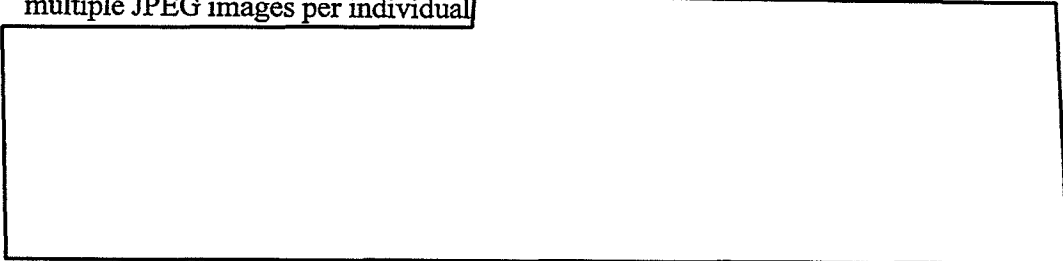traffic messages received by the FBI.

b2
b7E

SAMNet provides only ADD record
types, and SAMNet data is updated in IDW-S three times a day. SAMNet data
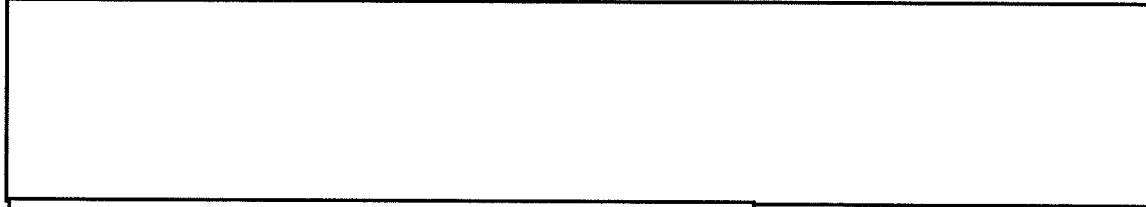
3.5.4   VGTOF

Violent Gang Terrorist Offender File (VGTOF) data is provided by the FBI
National Crime Information Center (NCIC). VGTOF data includes two
components: Data/metadata for each named individual/offender and potentially
multiple JPEG images per individual

b2
b7E

-23-

3.5.5 JICI

The Joint Intelligence Committee Investigation (JICI) data collection was created following the September 11 attacks. Paper counter-terrorism files/folders from all FBI Field Offices

JICI is a static collection that is not updated.

b2
b7E

3.5.6 Open Source News

The IDW-S V1.0 system contains an Open Source News library collected by the DARPA TIDES Program. These are primarily news source from around the world that are either in English or have been translated into English. Open Source News data is received in the form of text files (one per news article) The Open Source News data goes into IDW-S once a day. Open Source News data is

Open Source News material is derived from the following sources:

Addis Ababa Tribune - http://www.addistribune.com/
Agencia Brasilia - http://www.radiobras.gov.br/
Al-Ahram (Egypt, weekly English version) - http://weekly.ahram.org.eg/
AllAfrica.com - http://allafrica.com/
Arabic News - http://www.arabicnews.com/ansub/
Asahi Shimbun - http://www.asahi.com/english/
Asia Times (Hong Kong) - http://www.atimes.com/
Bangkok Post - http://www.bangkokpost.net/
Christian Science Monitor - http://www.csmonitor.com/
Crescent International - http://www.muslimedia.com/mainpage.htm
Daily Telegraph (London, England) - http://news.telegraph.co.uk/
Dawn (Karachi, Pakistan) - http://www.dawn.com/
Debka (Israel) - http://www.debka.com
East Africa Daily Nation - www.nationaudio.com/News/DailyNation/Today/
Gulf News (UAE) - http://www.gulf-news.com/
Ha'aretz (Israel) - http://www.haaretzdaily.com/
IFRC Internation Federation of the Red Cross - http://www.ifrc.org/
IRIN Integrated Regional Information Network - http://www.irinnews.org/
Iraq Press News Agency - http://www.iraqpress.org/

-24-

Islamic Republic News Agency (Iran) - http://www.irna.com/en
Jakarta Post - http://www.thejakartapost.com/
Janes - http://www.janes.com/
Jordan Times - http://www.jordantimes.com/
L'Osservatore Romano - www.vatican.va/news_services/or/or_eng/text.html
Lagos (Nigeria) Guardian - http://www.guardiannewsngr.com/
Lahore (Pakistan) Nation - http://www.nation.com.pk/
Lebanon Daily Star (Beirut) - http://www.dailystar.com.lb/
Malaysian Star - http://thestar.com.my/
Manila Bulletin - http://www.mb.com.ph/
Manila Times - http://www.manilatimes.net/
Miami Herald - http://www.miami.com/
Moscow Times - http://www.themoscowtimes.com/
National Post and CP - http://www.canada.com/
New Straits Times (Kuala Lumpur) - http://www.emedia.com.my/Current_News/NST/
PETRA (Jordanian News Agency) - http://www.petra.gov.jo
Pakistan Observer (Islamabad) - http://pakobserver.net/
Palestine Chronicle - http://palestinechronicle.com/
People's Daily (China) - http://english.peopledaily.com.cn/
Philippine Star - http://www.philstar.com/philstar/
Pravda - http://english.pravda.ru/
ProMed - epidemiology mailing list
Russian Information Agency Novosti - http://en.rian.ru/
Russian Issues (Misc. Russian news) - http://www.therussianissues.com/
Russian Observer - http://www.russianobserver.com/
SABA (The News Agency of Yemen) - http://www.sabanews.gov.ye
Saudi Gazette - http://www.saudigazette.com.sa/sgazette/
South African Dispatch - http://www.dispatch.co.za/
Sydney Morning Herald - http://www.smh.com.au
Tehran Times - http://www.tehrantimes.com/
Times of India - http://timesofindia.indiatimes.com/cms.dll
UNHCR UN High Commissioner on Refugees - http://www.unhcr.ch/
Ummah News - http://www.ummahnews.com/
Uzbekistan Report - http://www.uzreport.com/eng/
Washingtion Post - http://www.washingtonpost.com/
XinHua News Service - http://www.xinhuanet.com/english/
Yemen Times (weekly) - http://www.yementimes.com/
Yomiuri Shimbun (Japan) - http://www.yomiuri.co.jp/

3.5.7 Summary of Data Sources

DATASET NAME	DATA SOURCE	TRANSFER METHOD	COMMENTS

-25-

DATASET NAME	DATA SOURCE	TRANSFER METHOD
ACS	FBI Automated Case System (ACS)	FTP
IntelPlus	FBI Intel Plus	FTP
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	FTP
VGTOF	FBI National Crime Information Center (NCIC)	CD-ROM
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Multiple
Open Source News	Translingual Information Detection, Extraction and Summarization (TIDES) Program, Defense Advanced Research Projects Agency (DARPA)	CD-ROM

b2
b7E

Outside the Scope

-26-
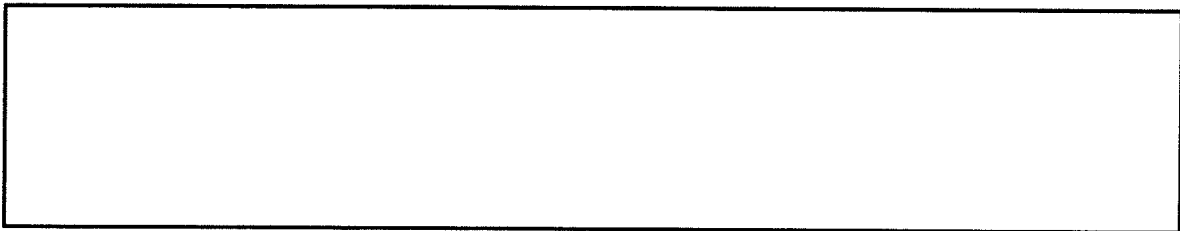
Attachment L

Outside the Scope
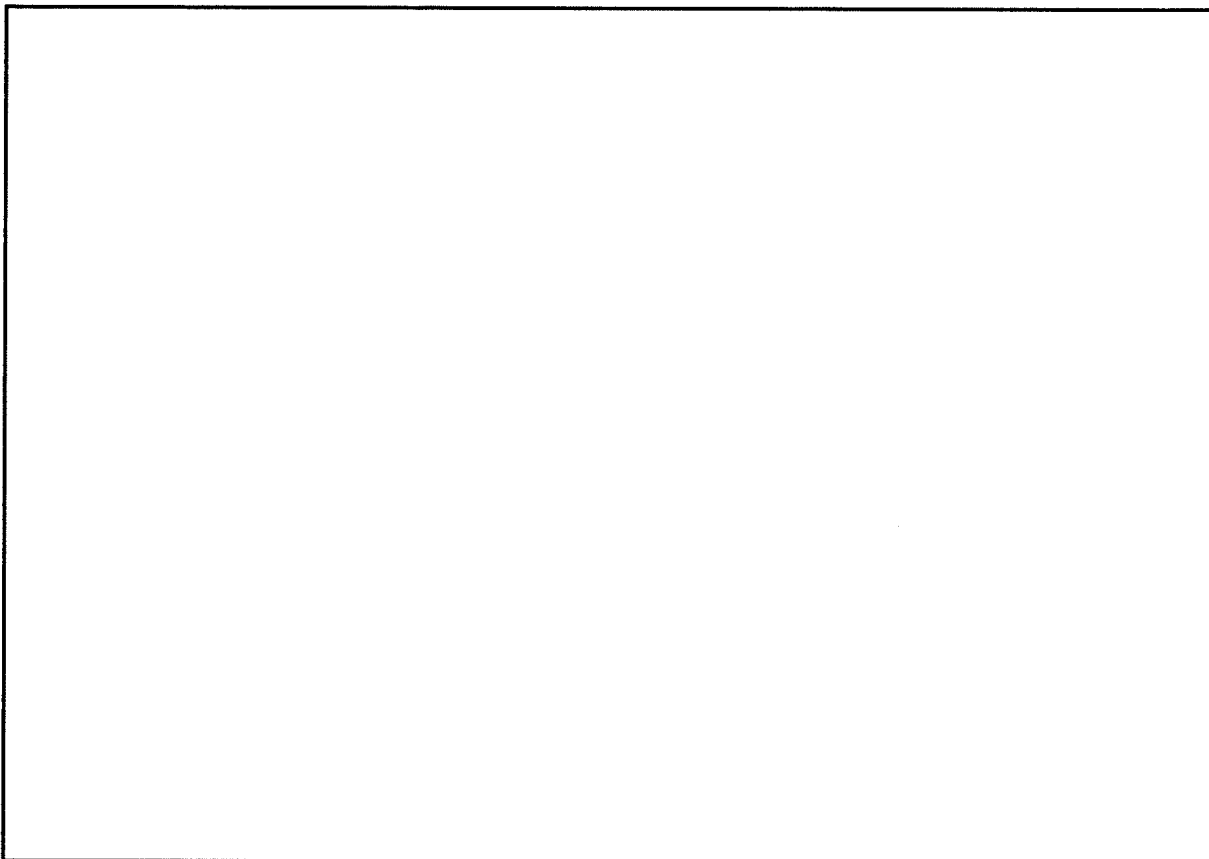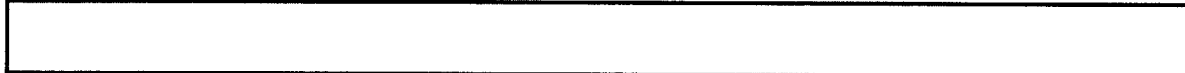
Outside the Scope

Outside the Scope

4 Custom Software Applications

4.1 IDW-S Data Ingest Applications

Figure 4.1.1 is the dataflow diagram for the IDW-S data ingest process.
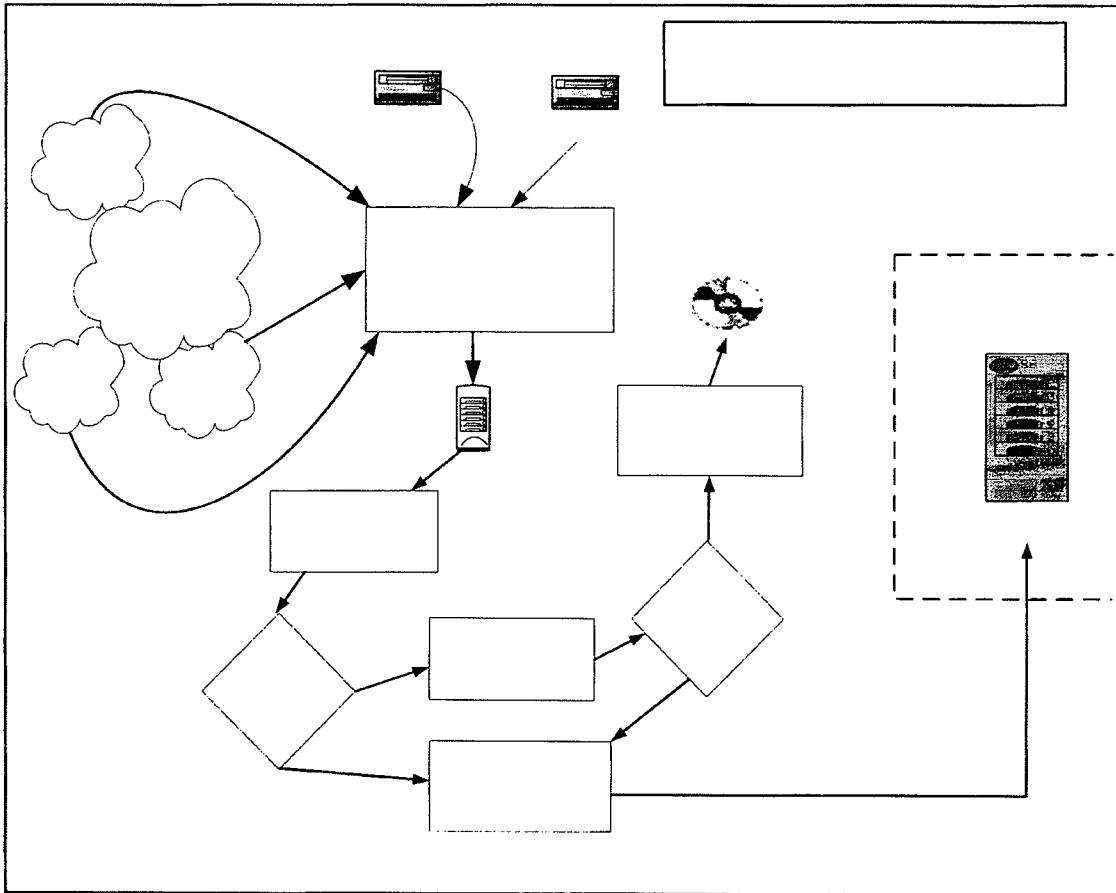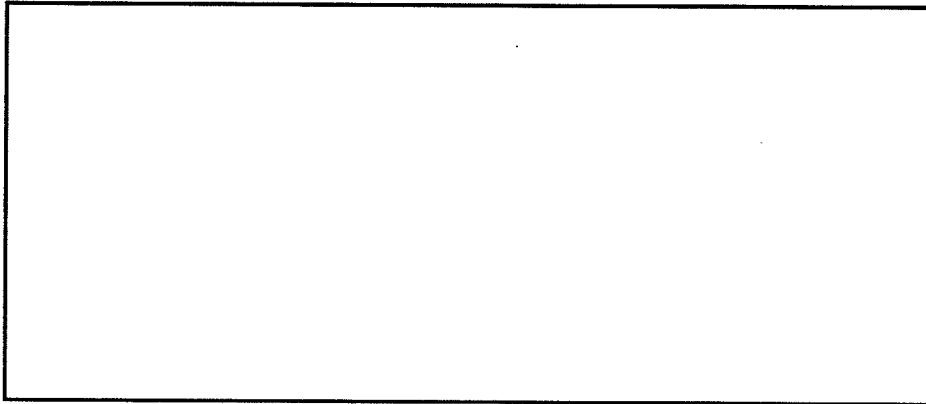
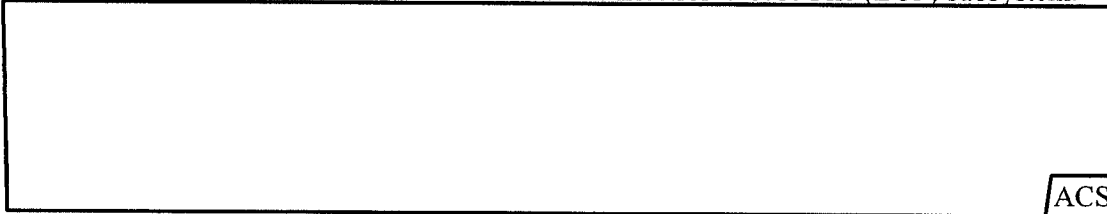**Figure 4.1.1 IDW-S Data Ingest Dataflow**

Outside the Scope

Outside the Scope

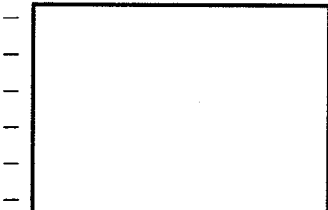Data ingest processing on IDW-S includes the following:

- **ACS Processing:** The ACS data is a subset of the Electronic Case File (ECF) subsystem.
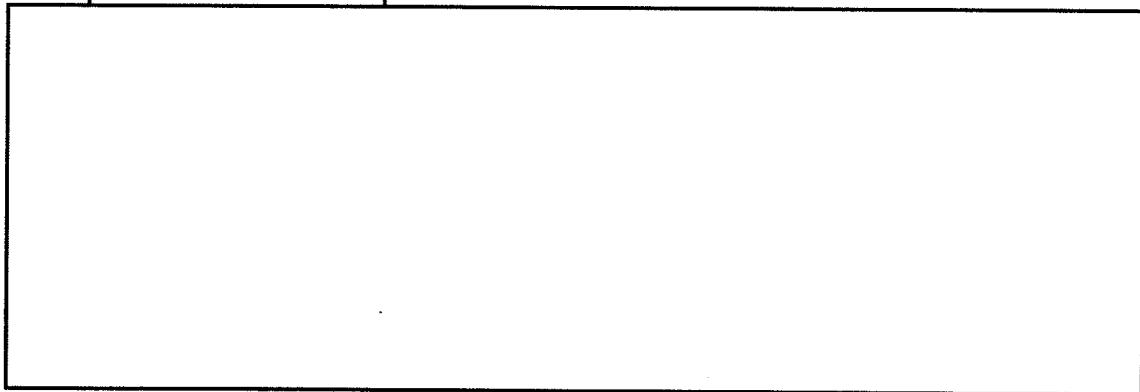
b2
b7E

ACS

provides ADD, MOD, and DELETE record types.

- **IntelPlus Processing:** The IntelPlus data includes of the following CT file rooms:

  -
  -
  -
  -
  -
  -

b2
b7E

- **SAMNet Processing:** The SAMNet data consists of cable traffic messages received by the FBI.

  b2
  b7E

- **JICI Processing:** The JICI data consists of one file room where each case file and serial is represented by a directory. Each directory contains the text and image files associated with the serial. JICI data is provided in entirety.

- **MiTAP Processing:** The MiTAP data consists of file archives of news messages.

  b2
  b7E

- **VGTOF Processing:** VGTOF is a structured data source that is currently available in IDW V1.0 The VGTOF data is composed of an ASCII source file of structured data records and files. The records for each individual are combined into a document. VGTOF data is provided in entirety, replacing the previous data.

  Outside the Scope

Federal Bureau of Investigation
Information Resources Division
Data Management Section

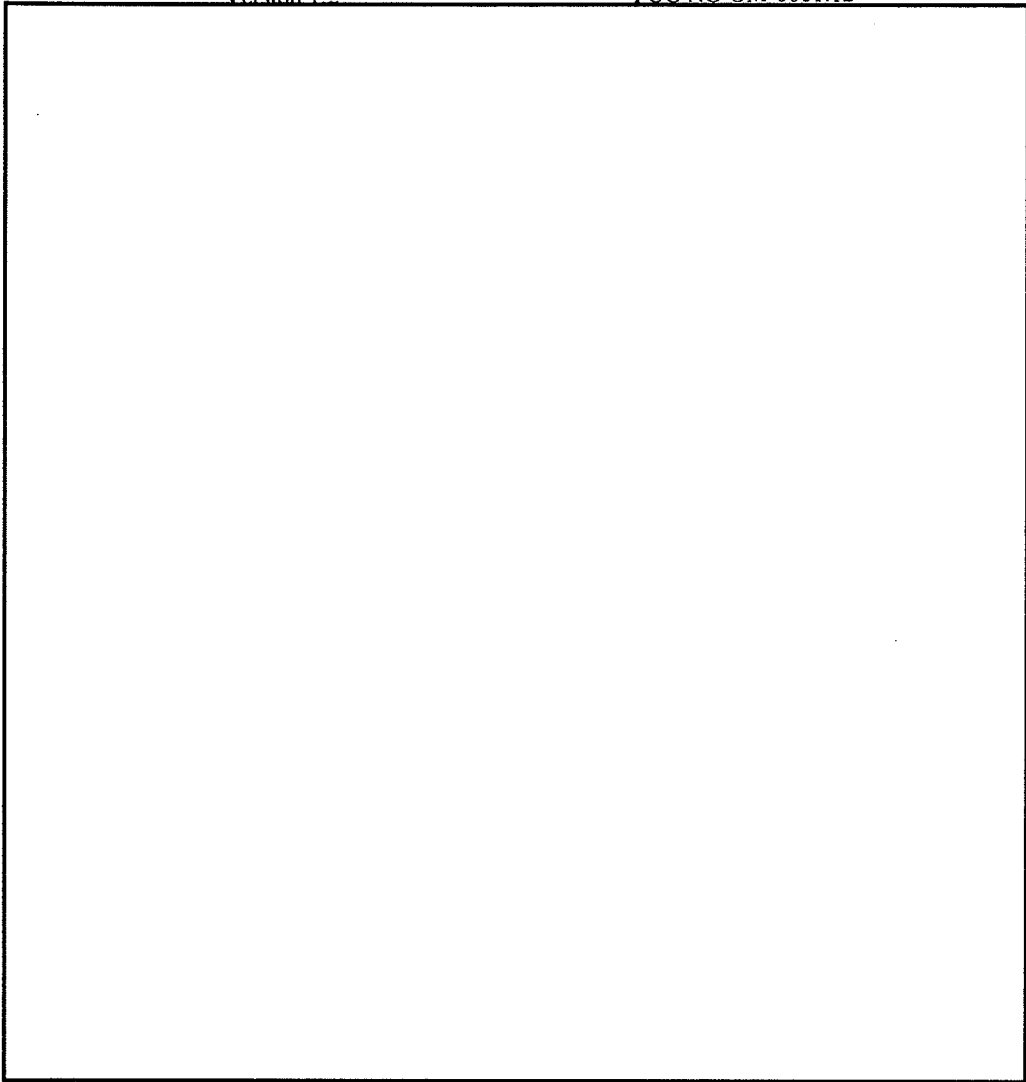Investigative Data Warehouse
Privileged Users Guide
Version 1.2

December 1, 2004

Outside the Scope

4.1 Operations

The IDW system is broken up into three subsystems, each with a different set of responsibilities

DOCLAB System
IDW-S contains data from the following data sources with security classification indicated in the table below:

DATA SOURCE	CLASSIFICATION	DATA TRANSFER MECHANISM TO IDW
FBI Automated Case System (ACS)	Secret and below	
FBI IntelPlus	Secret and below	
FBI Secure Automated Messaging Network (SAMNet)	Secret and below	
FBI National Crime Information Center (NCIC)	SBU	
FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below	
MiTAP	Unclassified	

b2
b7E

Outside the Scope

Outside the Scope

The SPT-specific data sources will include:

- Financial Center (FinCen)
-
- NoFly
- Selectee
-
-
-
-
- Unified Name Index (UNI) extracts
-

b2
b7E

Note: Hardcopy versions of this document must be verified for correct version number with the IDW CM Document Control Library.
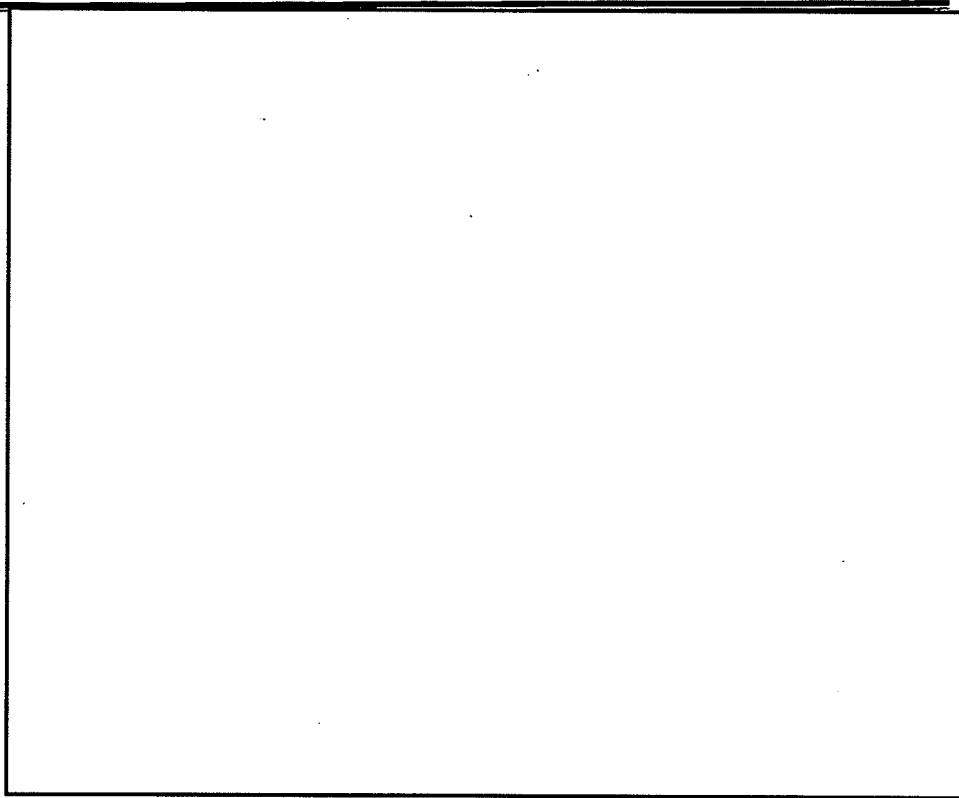
PUG NG-OM-0061.12
FOR OFFICIAL USE ONLY
Page 16

Federal Bureau of Investigation

Information Resources Division

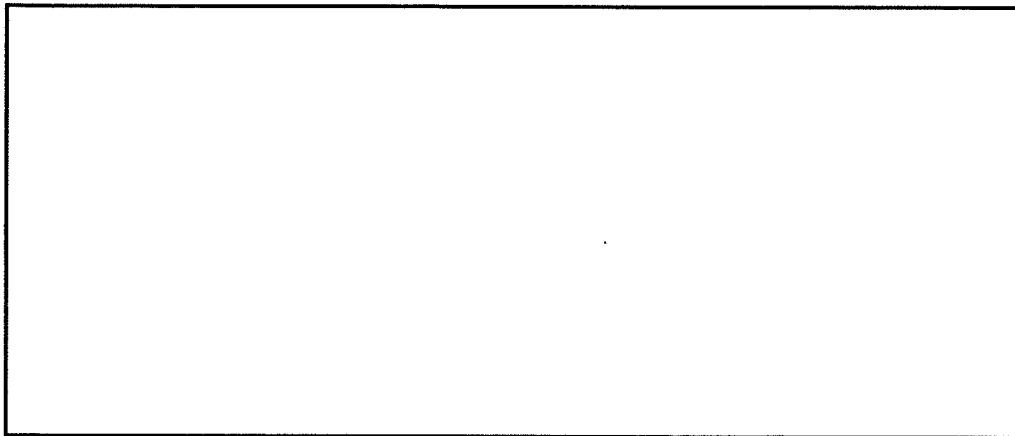## Data and Information Management Section
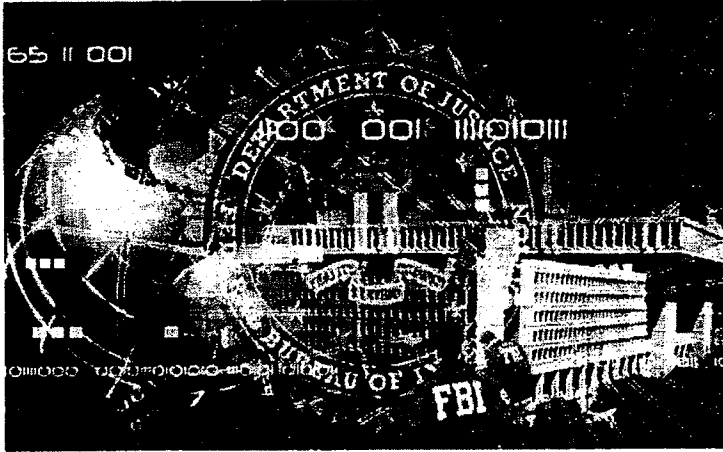
Investigative Data Warehouse – Secret (IDW-S)

System Security Plan

Document Version 1.5

24 January 2005

Outside the Scope

1.2.2 Supported Projects

IDW-S is an FBI enterprise program/system and provides data and data processing/analysis services to FBI agents and analysts as they perform counter-terrorism, counter-intelligence, and law enforcement missions. The initial focus for the IDW-S Core Subsystem has been to support data analysis/data mining for the following FBI groups/activities:

Counter-Terrorism Division (CTD)

Special Event Unit

In addition, scanning/OCR performed in the DOCLAB-S subsystem supports the following FBI projects/programs:

PROJECT NAME	CLASSIFICATION / COMPARTMENTS	PROJECT POC
Joint Intelligence Committee Investigation (JICI)	Secret	Records Management Division Federal Bureau of Investigation J. Edgar Hoover FBI Building 935 Pennsylvania Avenue, NW Washington, DC 20535
IntelPlus	Secret	Information Resources Division Federal Bureau of Investigation J. Edgar Hoover FBI Building 935 Pennsylvania Avenue, NW Washington, DC 20535

b6
b7C

-13-

Outside the Scope

Automated Transfer of Raw Data to IDW-S

Raw data is automatically transferred to the IDW-S system from approved data sources in accordance with an Interconnection Agreement, Memorandum of Understanding, Memorandum of Agreement or Interface Control Document. IDW-S V1 receives update data by the following means:

- ACS update data is transmitted to the IDW-S system

- IntelPlus update data is transmitted to the IDW-S system

- SAMNet update data is transmitted to the IDW-S system

- VGTOF data is transmitted to the IDW-S system
- Open Source News data is transmitted to the IDW-S system
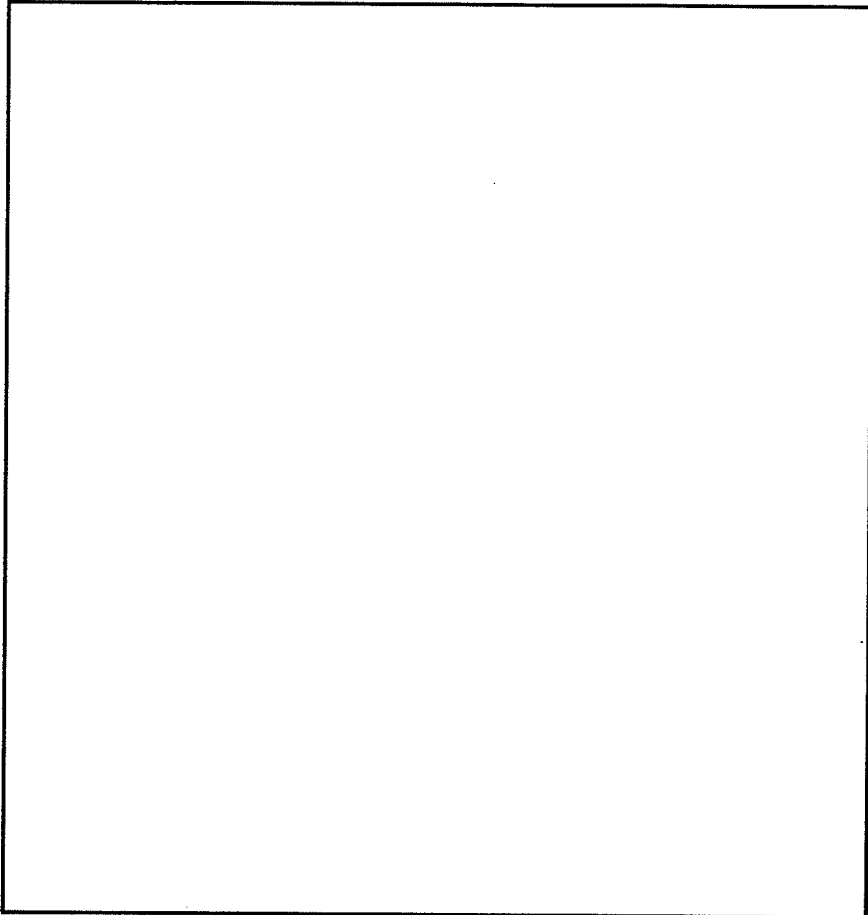- The JICI library is static and is not updated on IDW-S V1.

b2
b7E

Parse and Format (Concatenated) Data to Individual Files (HTML)

- Initial processing of raw data file⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯ data into individual serial records (in the case of ACS ECF), documents (IntelPlus, JICI, Open Source News), messages (SAMNet), or files (VGTOF)

b2
b7E
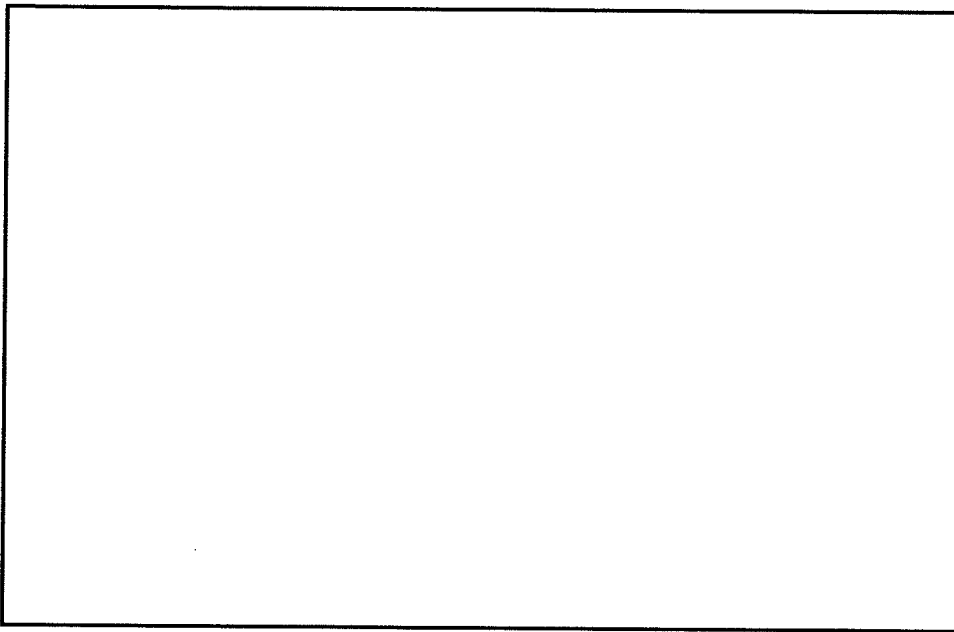
Outside the Scope

Outside the Scope

3.5.1.1 IDW-S Core Subsystem Data Processed

Table 3.5.1.1 below outlines the IDW-S datasets and information about transfer and ingest processing for each source.

DATASET NAME	DATA SOURCE	CLASSIFICATION	DATA TRANSFER MECHANISM TO IDW-S
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below	

b2
b7E

DATASET NAME	DATA SOURCE	CLASSIFICATION	DATA TRANSFER MECHANISM TO IDW-S
IntelPlus Filerooms	FBI IntelPlus	Secret and below	
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below	
VGTOF	FBI National Crime Information Center (NCIC)	SBU	
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below	
Open Source News	MiTAP	Unclassified	

b2
b7E

Table 3.5.1.1 IDW-S Data Sets

Outside the Scope

Outside the Scope

3.9.9 Indirect Connections

3.9.9.1 IDW-S Core Subsystem Indirect Connections

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	COMMENTS
FBI Automated Case System (ACS)	Secret	FBI	FTP	
FBI Intel Plus	Secret	FBI	FTP	
FBI Secure Automated Messaging Network (SAMNet)	Secret	FBI	FTP	
FBI National Crime Information Center (NCIC)	Unclassified/SBU	FBI	CD-ROM	
FBI Document Conversion Laboratory (DocLab), Records Management Division (RMD), FBIHQ	Secret	FBI	CD/DVD	

b2
b7E

| SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	COMMENTS
MiTAP – Open Source News	Unclassified	NA	CD-ROM	

3.9.9.2 SPT Subsystem Indirect Connections
None.

b2
b7E

3.9.9.3 DOCLAB-S Subsystem Indirect Connections

SYSTEM NAME	CLASSIFICATION & COMPARTMENTS	ACCREDITED BY	TRANSFER METHOD	COMMENTS
FBI Investigative Data Warehouse - Secret (IDW-S)	Secret	FBI	CD-ROM & FTP	
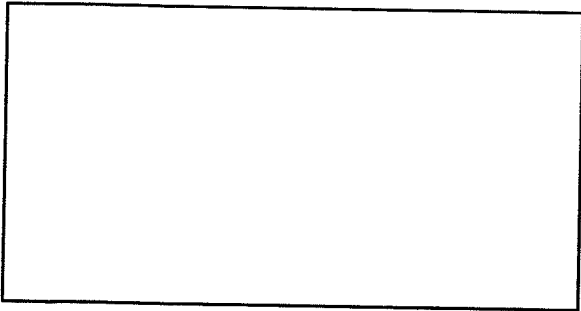
OTHER O/S

        IDW, Version 1.0 is scheduled for release January 2004
and will provide access to six primary data sources:

                    IDW Version 1.0

    o Electronic Case File (ECF)/Automated Case Support (ACS)
       /Virtual Case File - FBI investigative and intelligence
                        information.

    o SAMNET - wire traffic to the FBI from members of the
                intelligence community.

    o JICI - counterterrorism files that were scanned into a
             database to accommodate the Joint Intelligence
             Committee Investigation (JICI) on the September
             11, 2001, terrorist attack on the World Trade
             Center.

                                                    b2
                                                    b7E

    o VGTOF - Violent Crime and Terrorist Offender File
                information that includes biographical data
                pertaining to members of the identified groups.

    o Open Source - Fifty-seven news sources from around the
                    world that are either in English or have
                    been translated into English.