
Federal Bureau of Investigation
Information Resources Division
Data Management Section

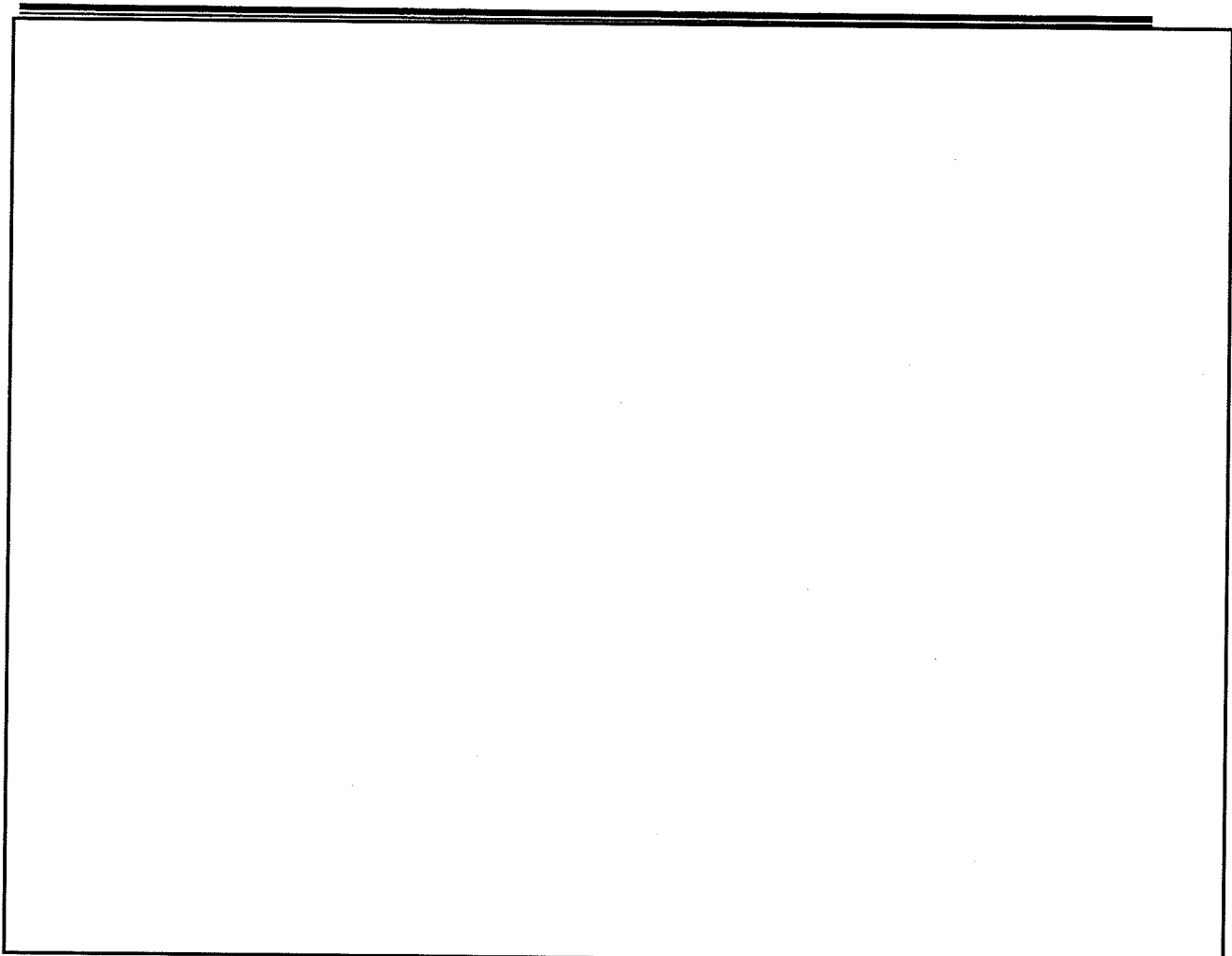


ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-07-2008 BY 65179 DMH/BJA/CAL

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**



1.4.1.1 Data Sources

Outside the Scope

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



b2
b7E

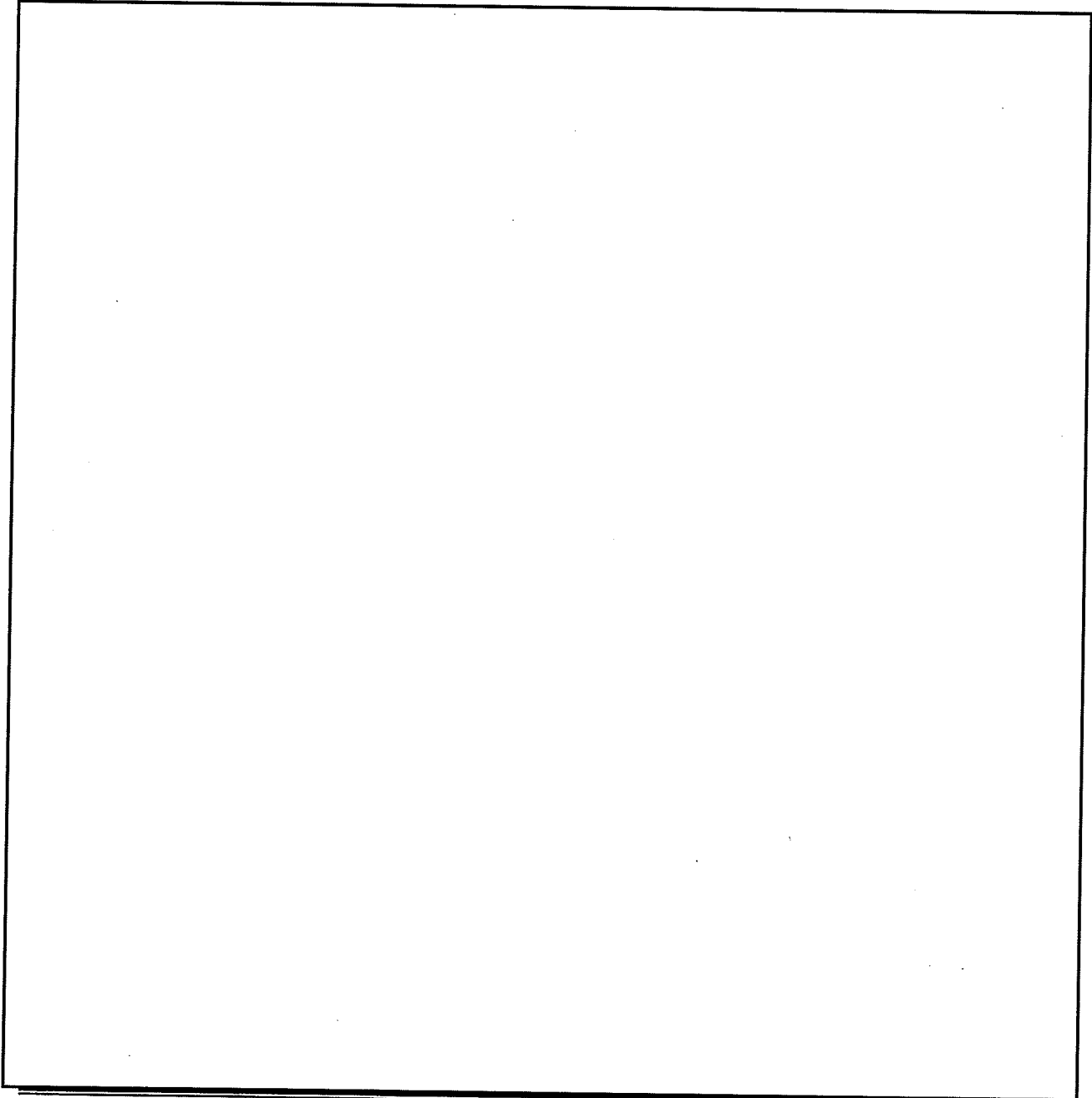
Data processed by the system includes the following sources:

- 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;

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

-
- 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

Outside the Scope

DRAFT

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FEDERAL BUREAU OF INVESTIGATION

OFFICE OF THE PROGRAM MANAGEMENT EXECUTIVE



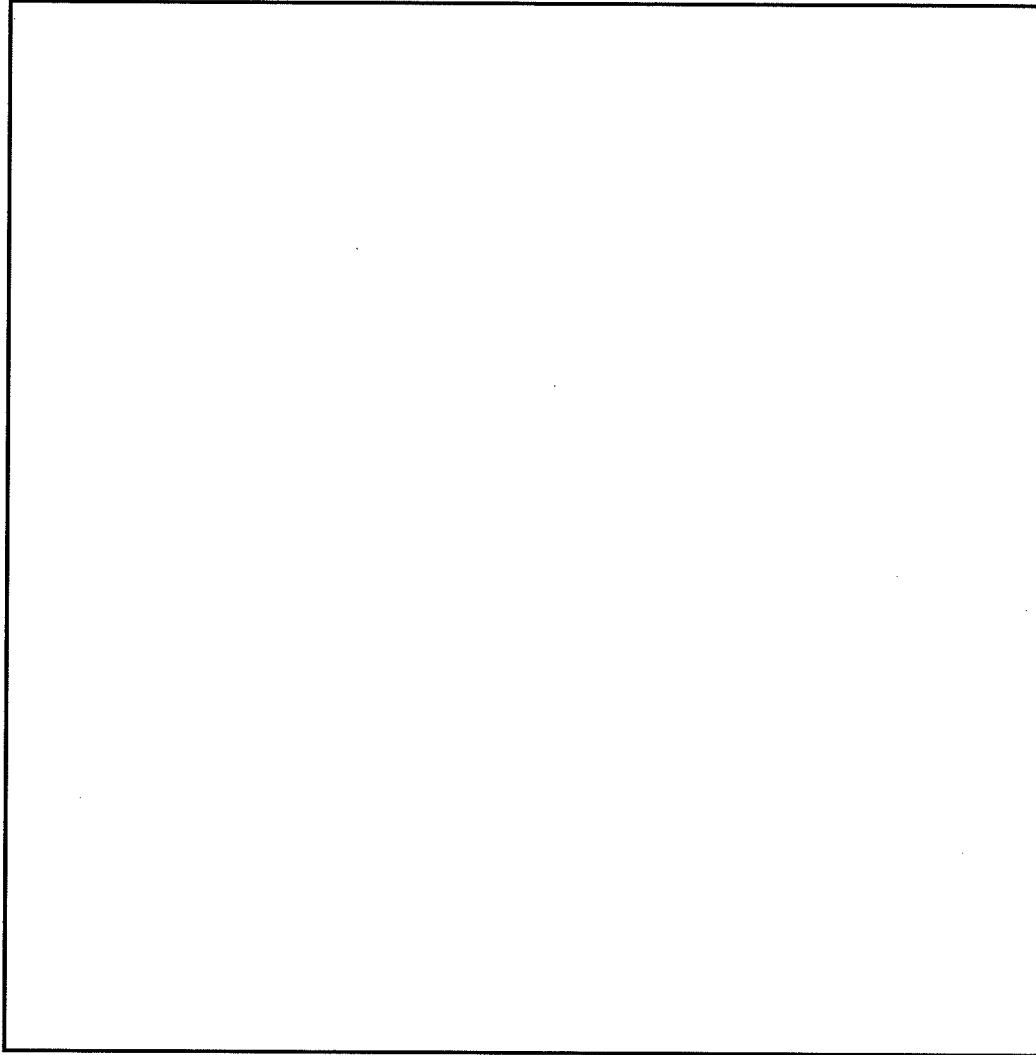
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-07-2008 BY 65179 DMH/BJA/CAL

***Security Concept of Operations (S-CONOPS)
Investigative Data Warehouse (IDW)
Document Version 1.1***

June 18, 2004

DRAFT

UNCLASSIFIED//FOR OFFICIAL USE ONLY



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

Outside the Scope

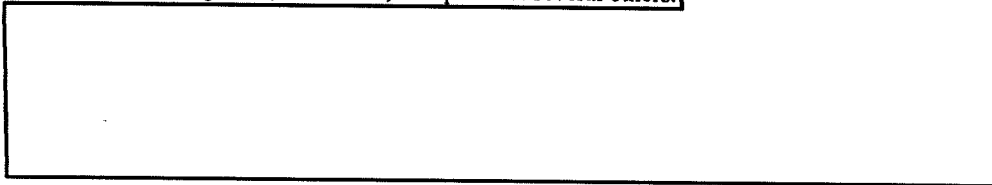
DRAFT

UNCLASSIFIED//FOR OFFICIAL USE ONLY

DATABASE NAME	DATASOURCE	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

Operational Subsystem Data Sources

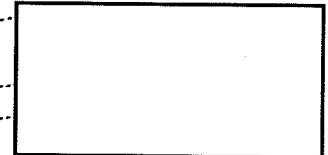
The data flow begins at the external data sources. These sources include various FBI databases including ACS, SAMNET, Intelplus and several others.



Comment: ACS = Automated Case Support

b2
b7E

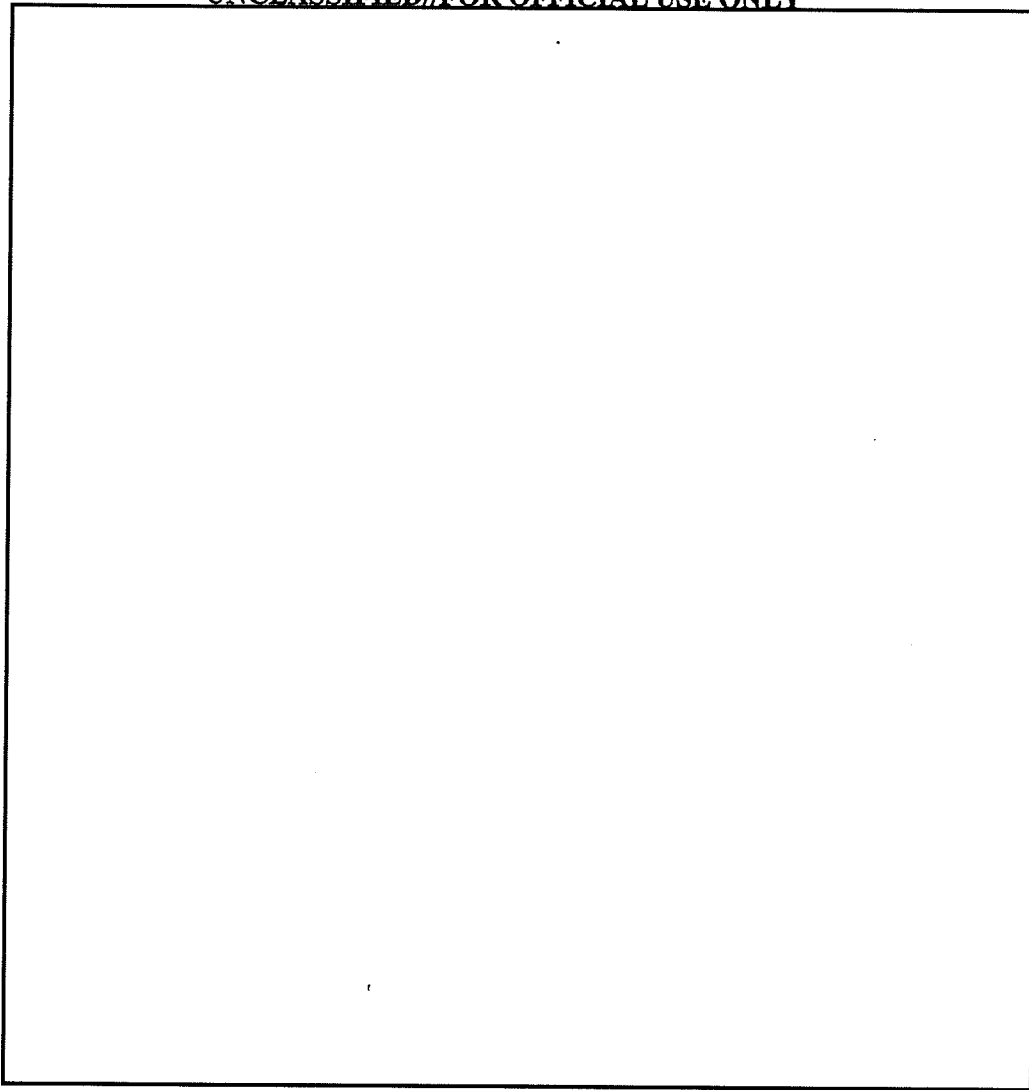
Outside the Scope



Outside the Scope

DRAFT

UNCLASSIFIED//FOR OFFICIAL USE ONLY



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

Outside the Scope

DRAFT

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

DRAFT

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FEDERAL BUREAU OF INVESTIGATION

OFFICE OF THE PROGRAM MANAGEMENT EXECUTIVE



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-07-2008 BY 65179 dmh/bja/cal

***Security Concept of Operations (S-CONOPS)
Investigative Data Warehouse (IDW)
(IDW-S, IDW-I, SPT Subsystem, & DocLab)
Document Version 1.1***

June 18, 2004

DRAFT

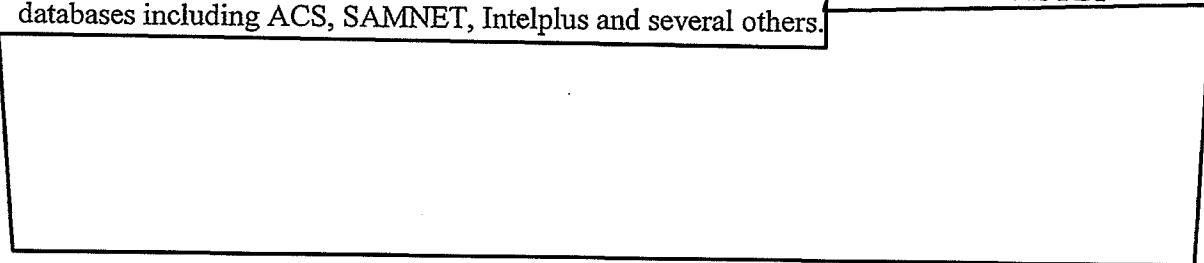
UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

b2
b7E

Operational Subsystem Data Sources

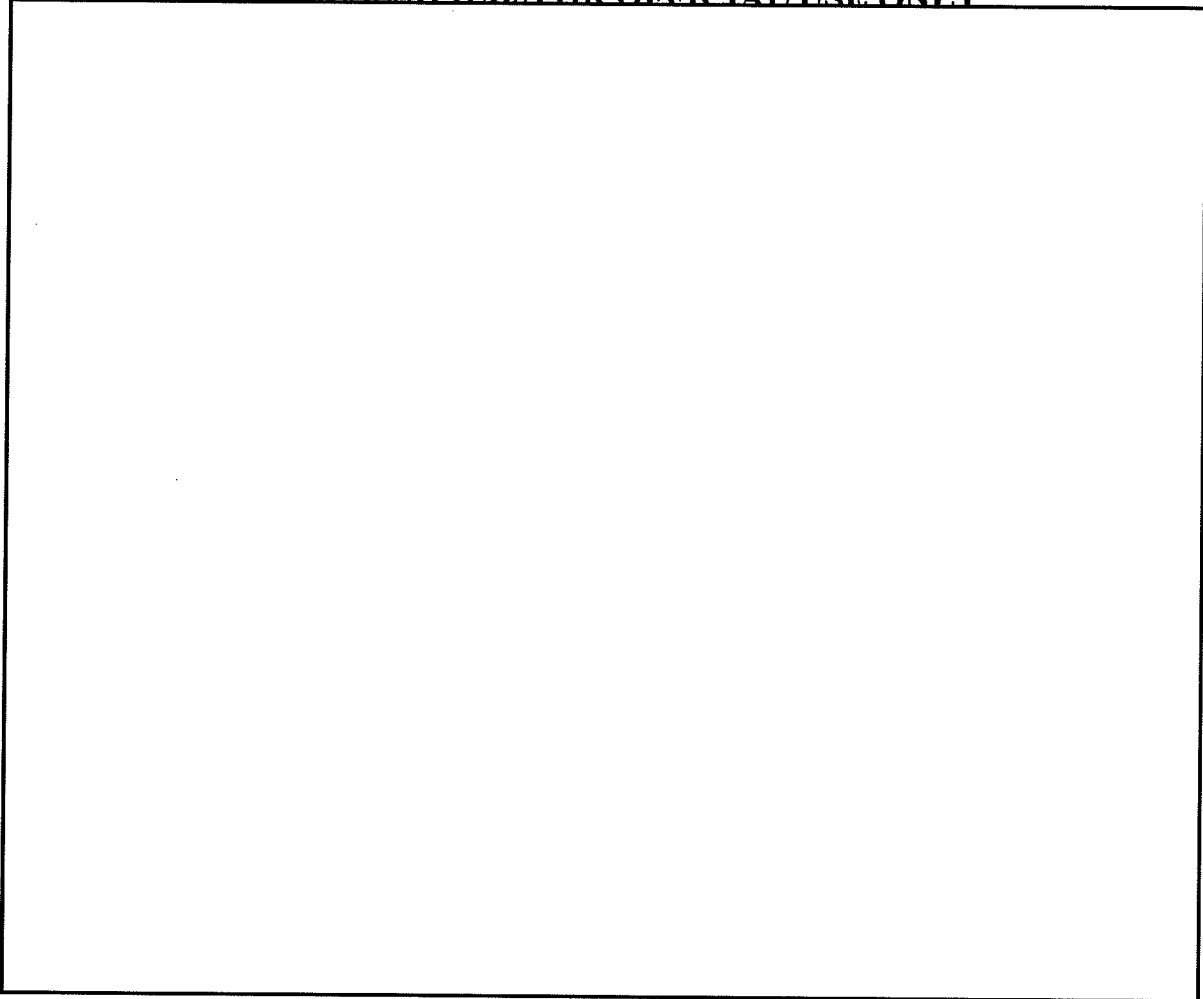
The data flow begins at the external data sources. These sources include various FBI databases including ACS, SAMNET, Intelplus and several others.



Outside the Scope

DRAFT

UNCLASSIFIED//FOR OFFICIAL USE ONLY



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.

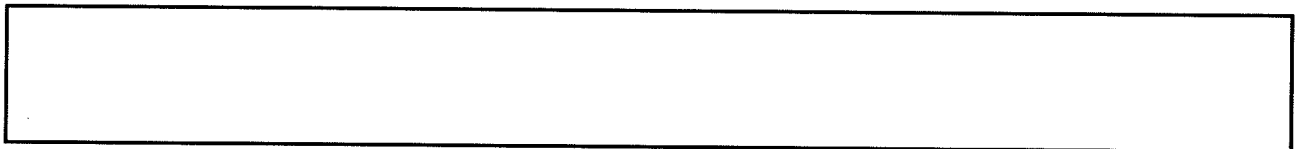
DRAFT

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-07-2008 BY 65179 dmh/bja/cal

INVESTIGATIVE DATA WAREHOUSE
DEVELOPMENT SYSTEM (IDW-D)
SYSTEM SECURITY PLAN

DOCUMENT VERSION 1.2

AUGUST 2005

[Redacted]

[Redacted]

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

- [Redacted]
- Violent Gang and Terrorist Organization File (VGTOF)

b2
b7E

[Redacted]

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



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-07-2008 BY 65179 dmh/bja/cal

INVESTIGATIVE DATA WAREHOUSE
CLASSIFIED DEVELOPMENT SYSTEM (IDW-DS)
SYSTEM SECURITY PLAN

DOCUMENT VERSION 0.6

17 AUGUST 2004

UNCLASSIFIED // FOR OFFICIAL USE ONLY

[Redacted]

[Redacted]

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,
- [Redacted]
- [Redacted]
- [Redacted]
- Universal Name Index (UNI), and
- Violent Gang and Terrorist Organization File (VGTOFTM) from the Criminal Justice Information Systems (CJIS) Division.

b2
b7E

[Redacted]

Outside the Scope

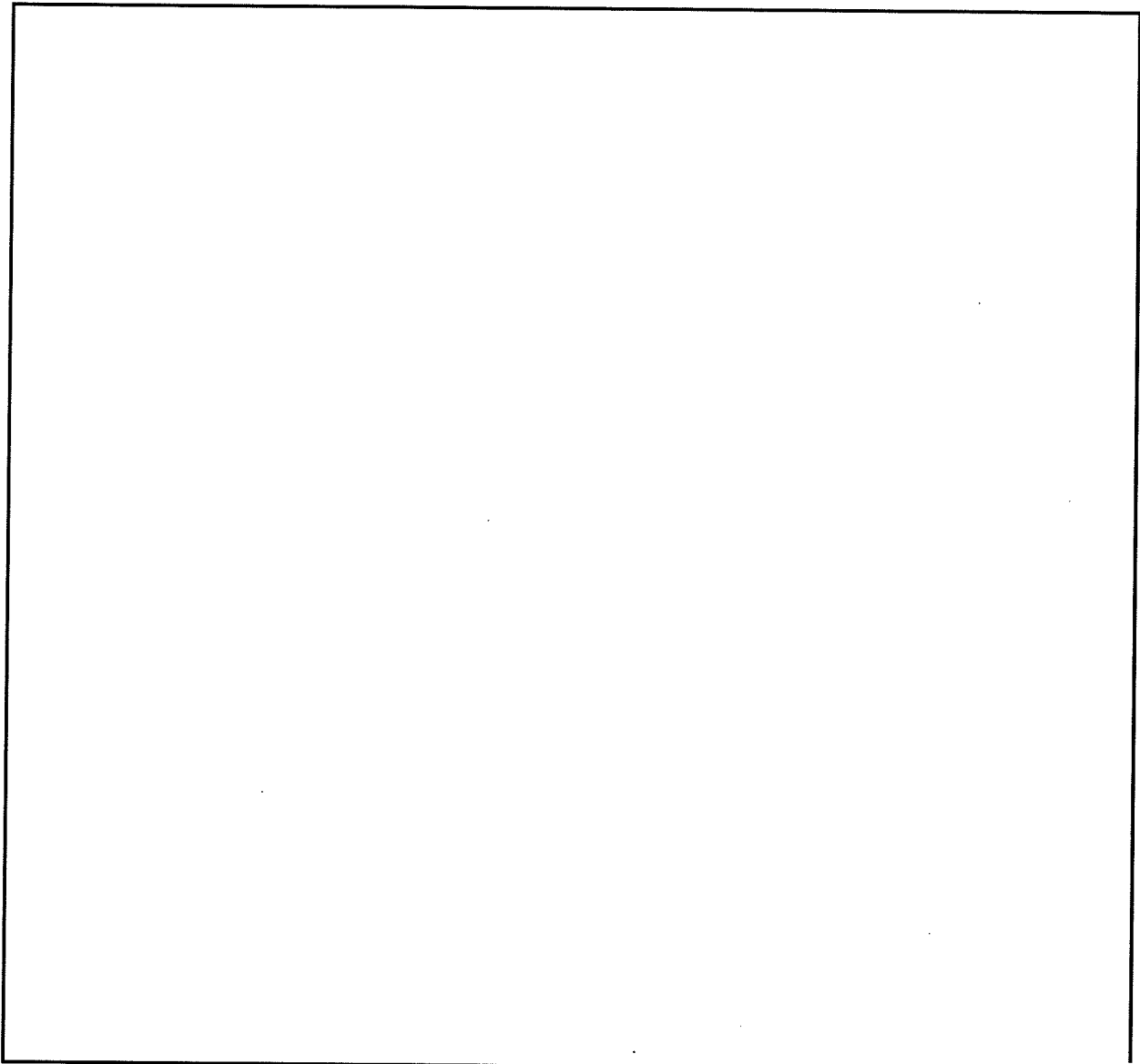
UNCLASSIFIED // FOR OFFICIAL USE ONLY

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;
-

-30-

UNCLASSIFIED // FOR OFFICIAL USE ONLY

- IntelPlus File Rooms;

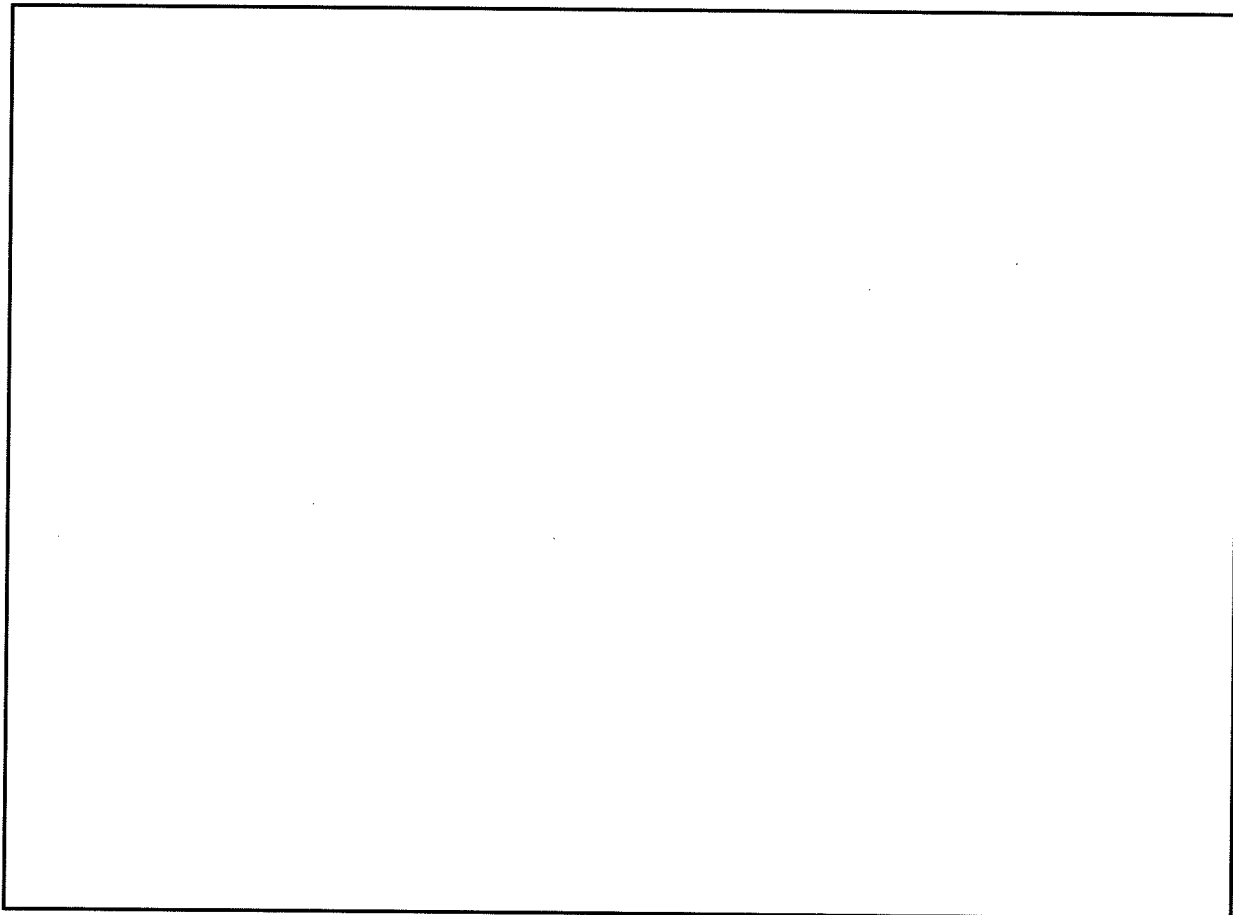


b2
b7E

- UNI, and

- VGTOF from 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

FEDERAL BUREAU OF INVESTIGATION
Office of IT Program Management



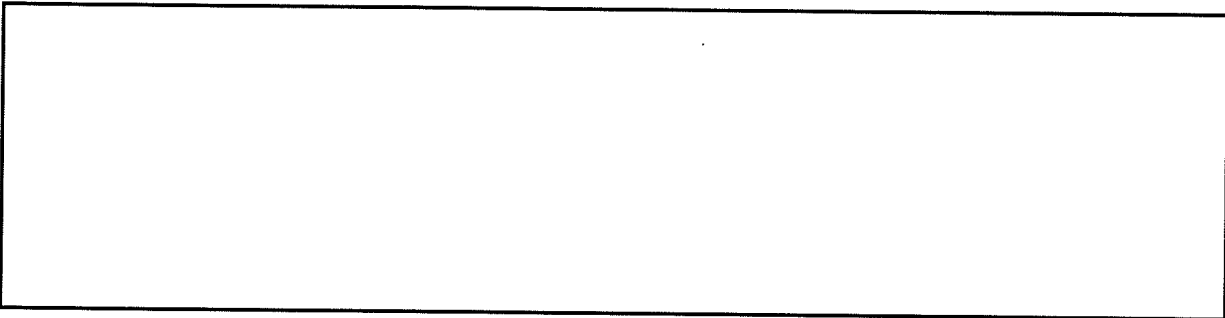
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-07-2008 BY 65179 dmh/bja/cal

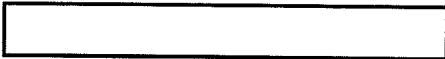


INVESTIGATIVE DATA WAREHOUSE
CLASSIFIED DEVELOPMENT SYSTEM (IDW-DS)
SYSTEM SECURITY PLAN

DOCUMENT VERSION 0.7

25 OCTOBER 2004

UNCLASSIFIED // FOR OFFICIAL USE ONLY

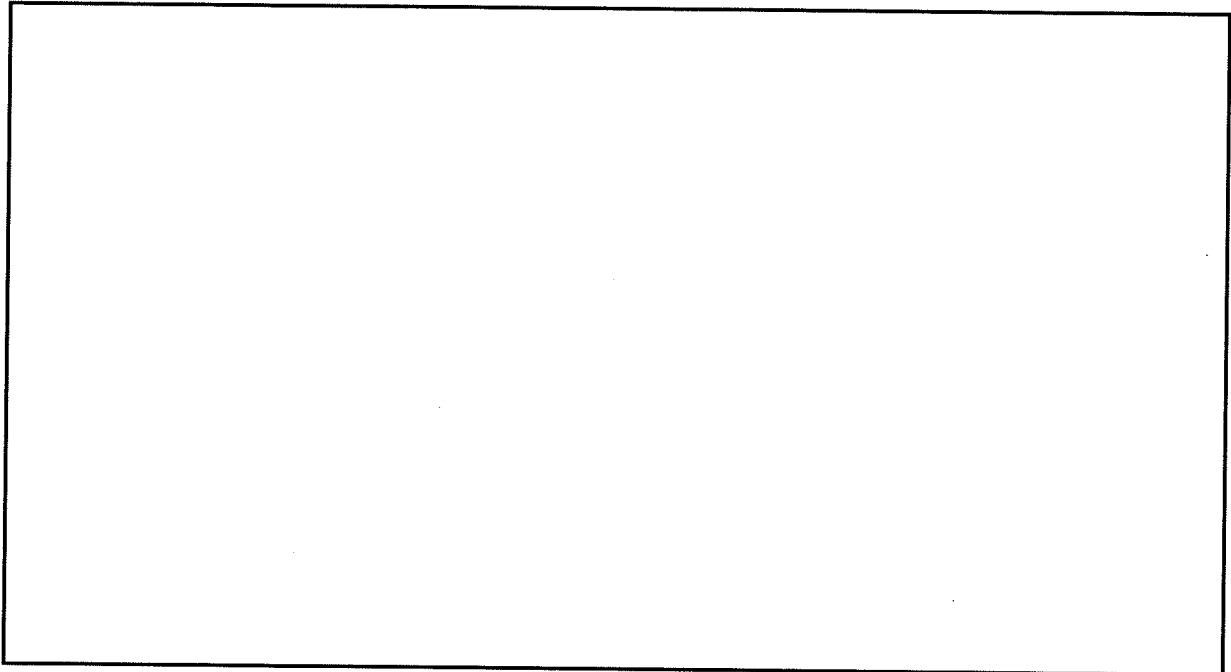


- Approved case files from the FBI's Automated Case Support (ACS) Electronic Case File (ECF) case management system,
- Secure Automated Messaging Network (SAMNet) message traffic,
- IntelPlus File Rooms,
- 
- 
- 
- Universal Name Index (UNI), and
- Violent Gang and Terrorist Organization File (VGTOF") from the Criminal Justice Information Systems (CJIS) Division.

b2
b7E

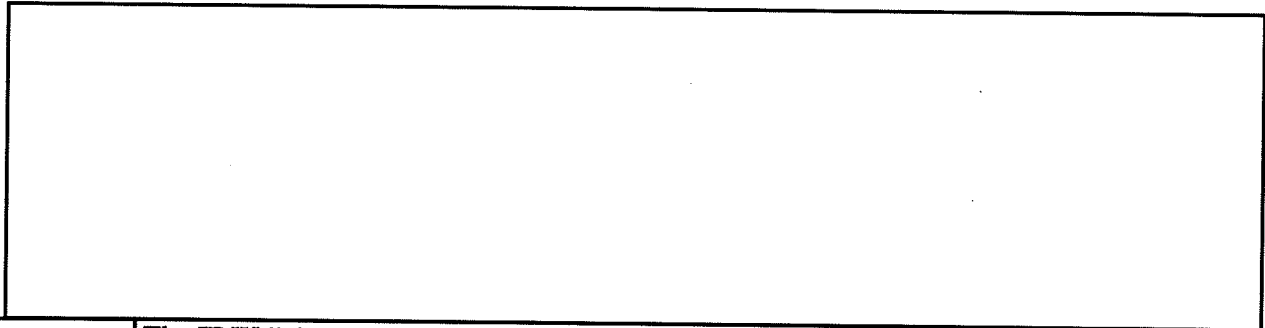


Outside the Scope



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;

- IntelPlus File Rooms;

•

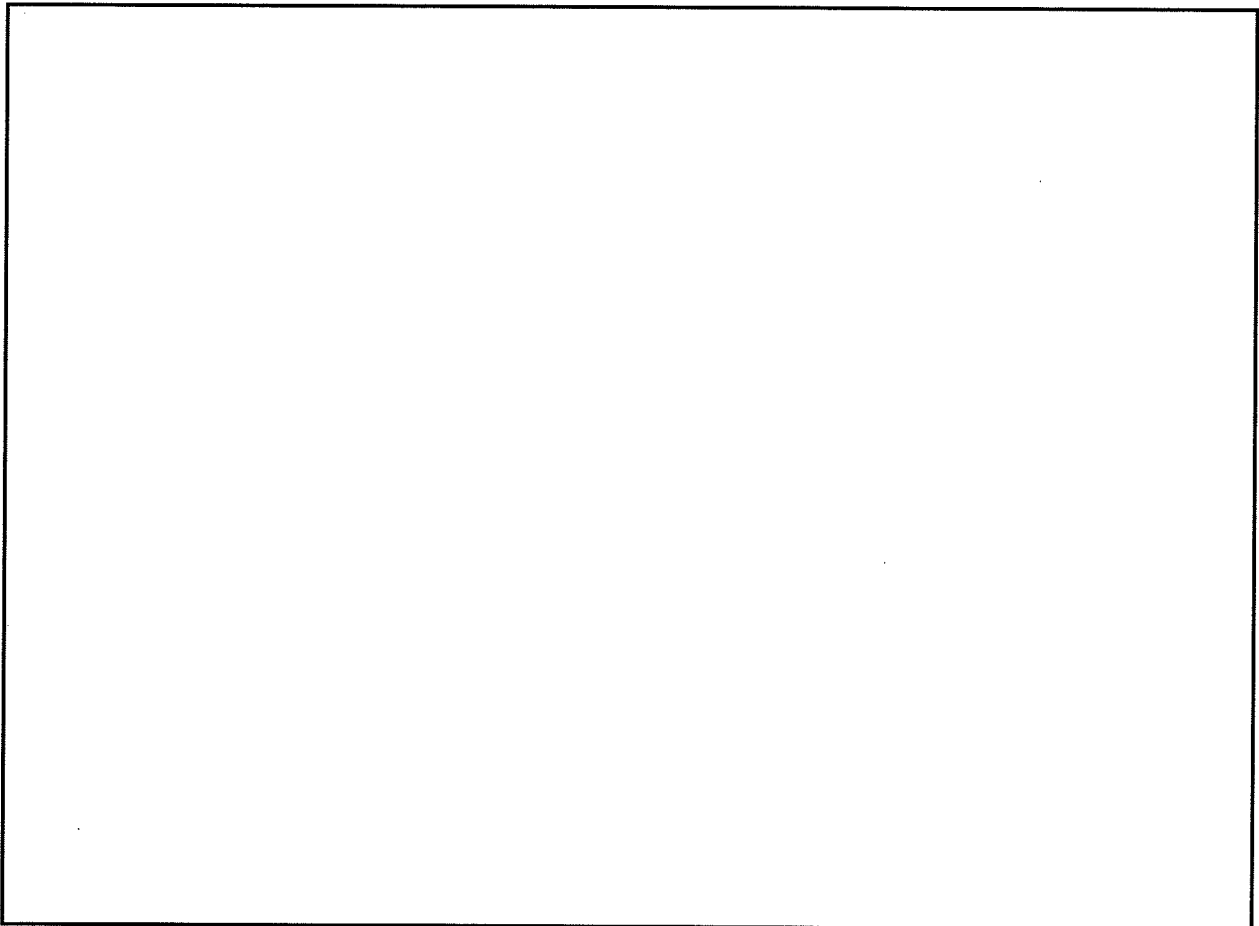
•

•

b2
b7E

- UNI, and

- VGTOF from CJIS Division.



UNCLASSIFIED // FOR OFFICIAL USE ONLY

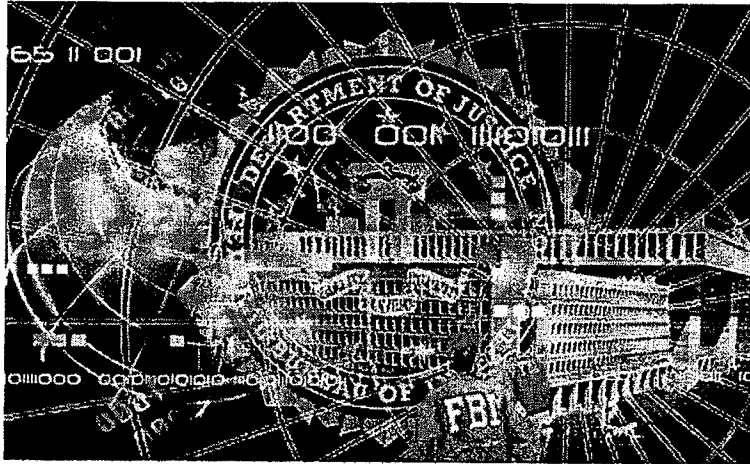
Investigative Data Warehouse - Secret (IDW-S)

System Security Plan

20 December 2004

Version 1.4

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



**INVESTIGATIVE DATA WAREHOUSE – SECRET
(IDW-S)**

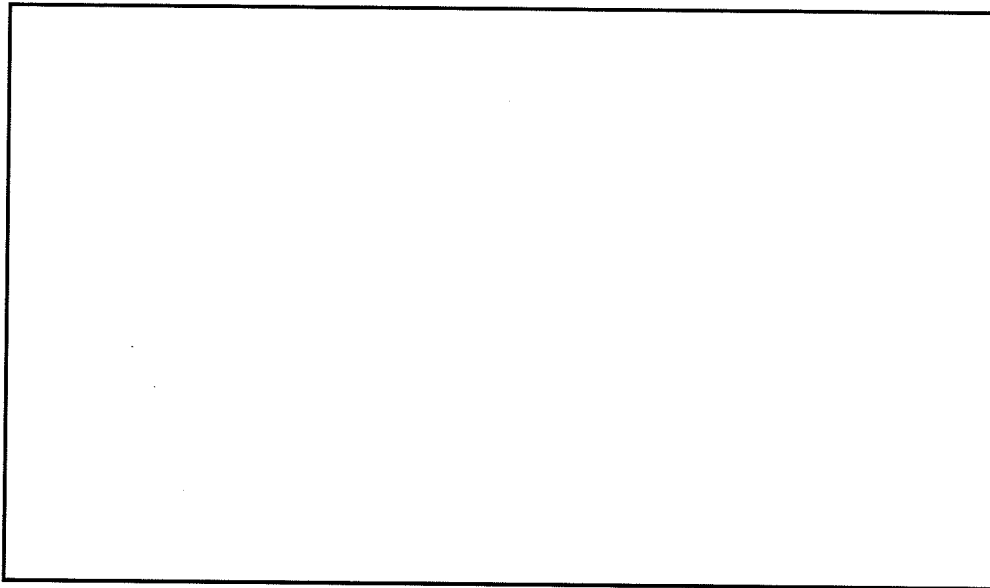
SYSTEM SECURITY PLAN

DOCUMENT VERSION 1.4

20 DECEMBER 2004

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

UNCLASSIFIED // FOR OFFICIAL USE ONLY



Automated Transfer of Raw Data to IDW-S

Outside the Scope

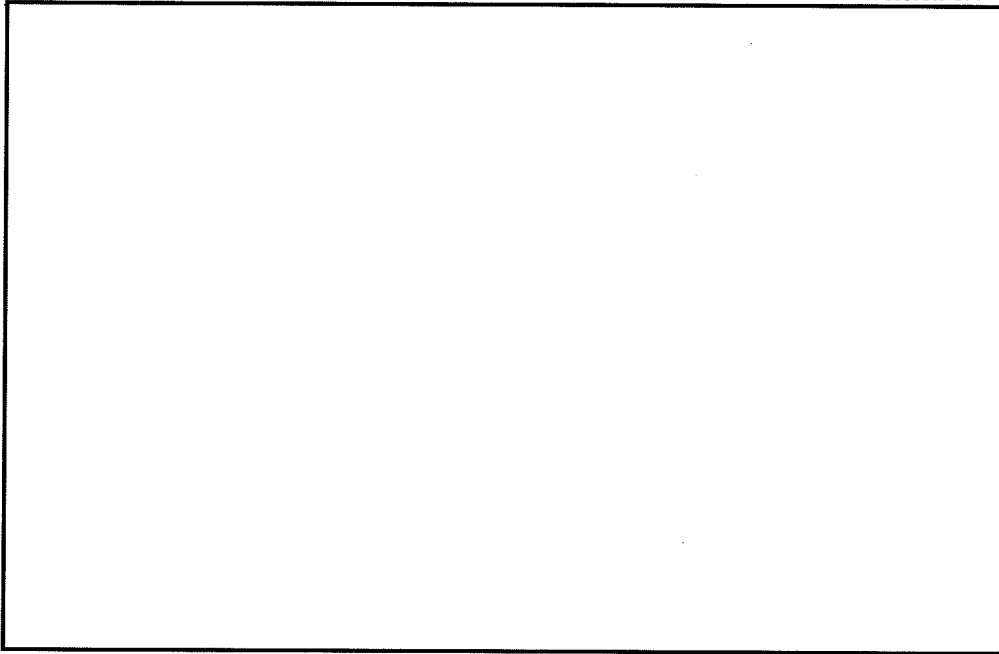
Raw data is automatically transferred to the IDW-S system from approved data sources in accordance with an Interconnection Agreement, Memorandum of Understanding, Memorandum of Agreement [redacted] receives update data by the following means:

b2
b7E

- ACS update data is [redacted]
- IntelPlus update data [redacted]
- SAMNet update data [redacted]
- VGTOF data [redacted]
- Open Source News data [redacted]
- The JICI library is static and is not updated [redacted]



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.

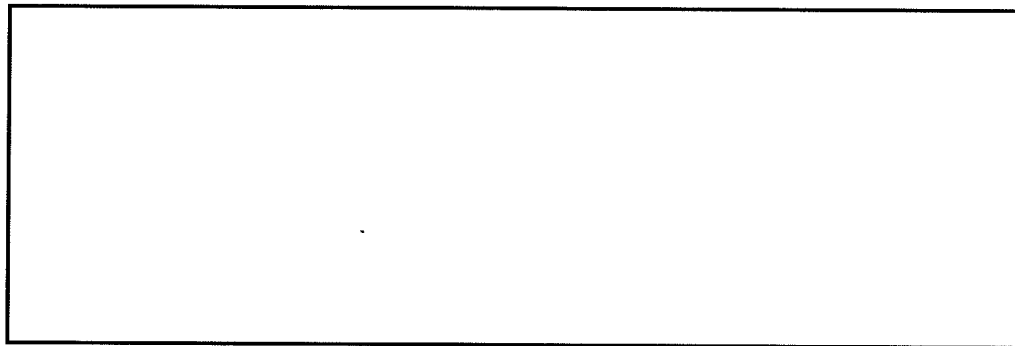
DATASET NAME	DATA SOURCE	CLASSIFICATION	
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below	

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

3.9.9 Indirect Connections

3.9.9.1 IDW-S Core Subsystem Indirect Connections

SYSTEM NAME	CLASSIFICATION COMPARTMENTS	ACCREDITED	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



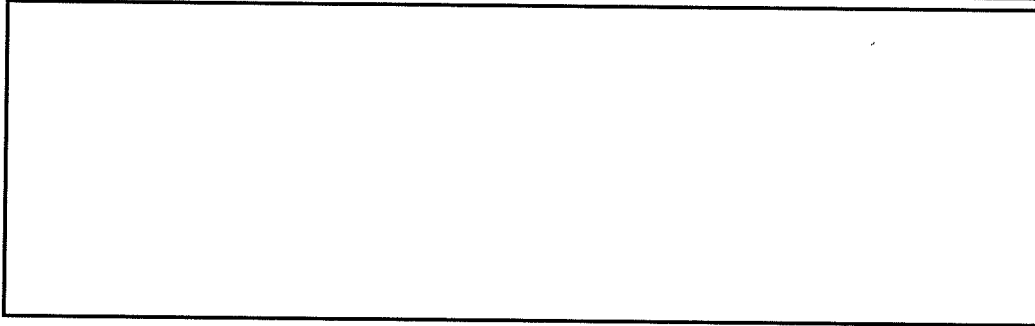
Outside the Scope

b2
b7E



SYSTEM NAME	CLASSIFICATION (COMPARTEMENTS)	ACCREDITED SYSTEM	TRANSFER METHOD	
MiTAP - Open Source News	Unclassified	NA	CD-ROM	

b2
b7E



Outside the Scope

UNCLASSIFIED // FOR OFFICIAL USE ONLY

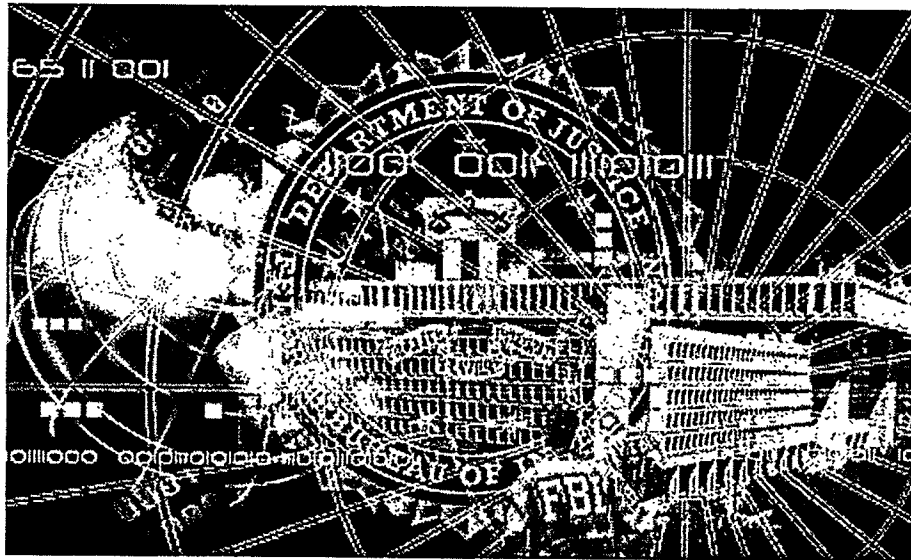
Investigative Data Warehouse - Secret (IDW-S)

System Security Plan

23 June 04

Version 1.3

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



**INVESTIGATIVE DATA WAREHOUSE – SECRET
(IDW-S)**

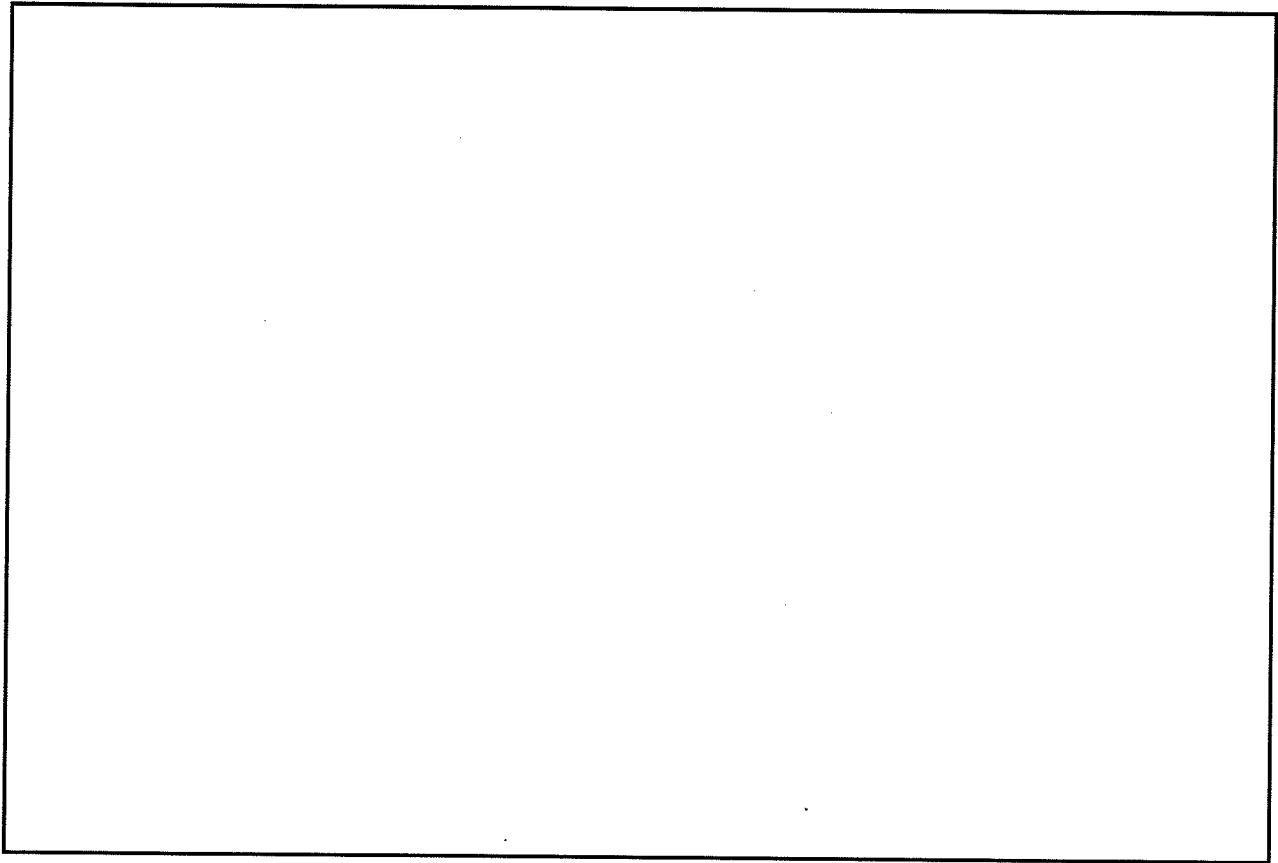
SYSTEM SECURITY PLAN

DOCUMENT VERSION 1.3

23 JUNE 2004

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-08-2008 BY 65179 dmh/bja/cal

UNCLASSIFIED // FOR OFFICIAL USE ONLY

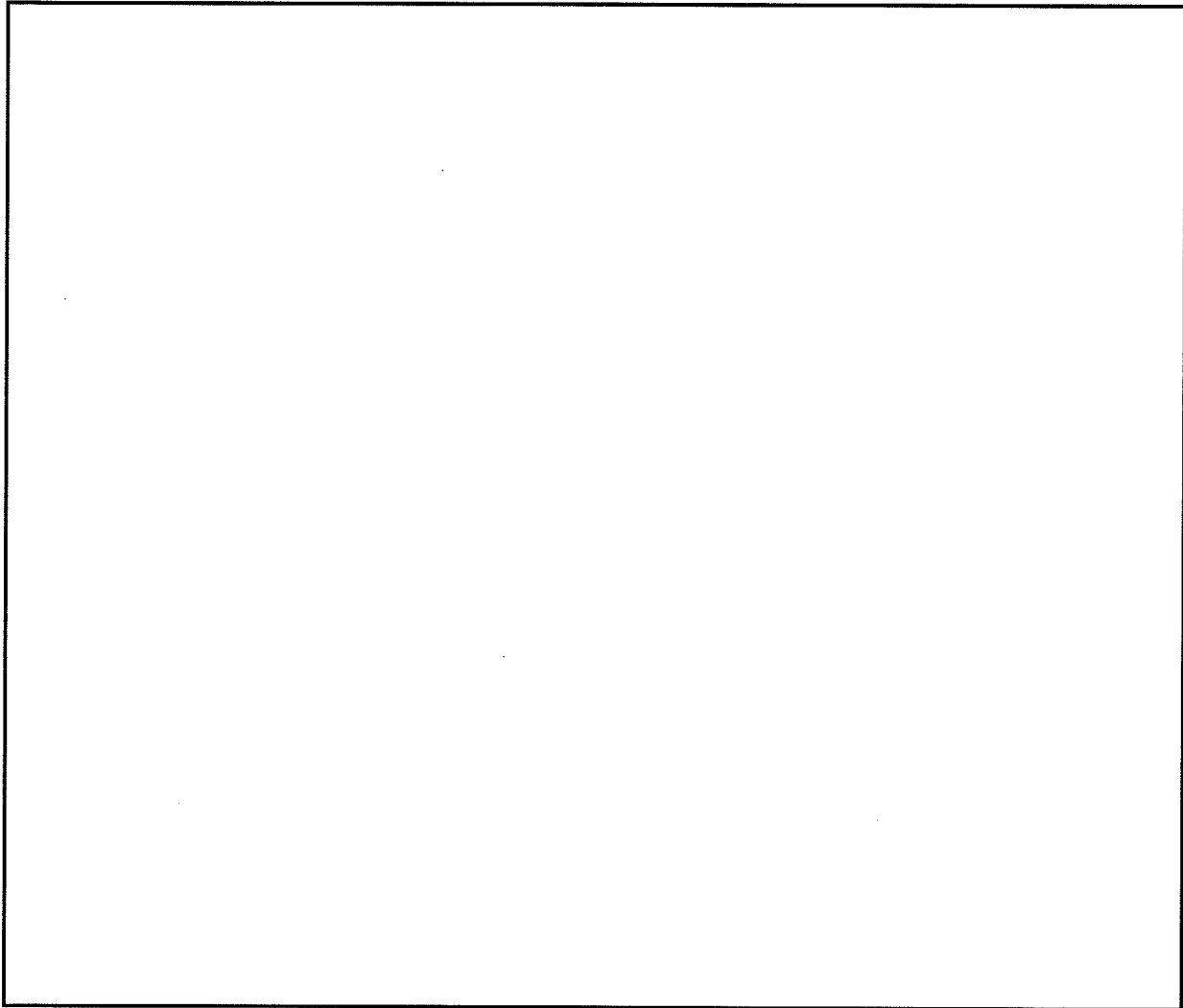


3.1.3.1 IDW-S Core Subsystem Data and Data Processing

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





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

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FEDERAL BUREAU OF INVESTIGATION

OFFICE OF THE PROGRAM MANAGEMENT EXECUTIVE

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-18-2008 BY 65179 dmh/bja/cal

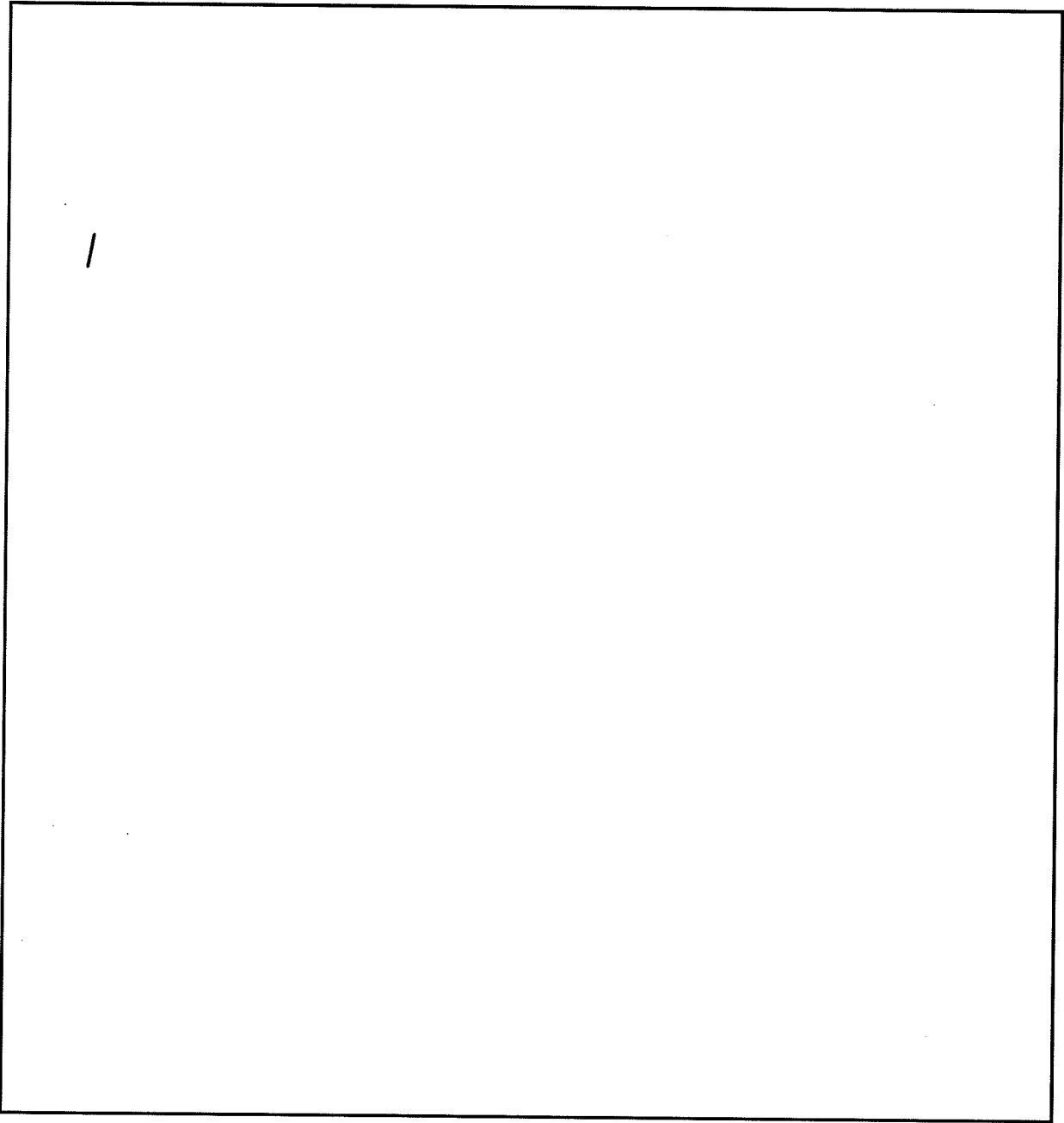


Security Concept of Operations (S-CONOPS) Investigative Data Warehouse (IDW)

Document Version 1.2.2

December 22, 2004

UNCLASSIFIED//FOR OFFICIAL USE ONLY



Outside the Scope

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

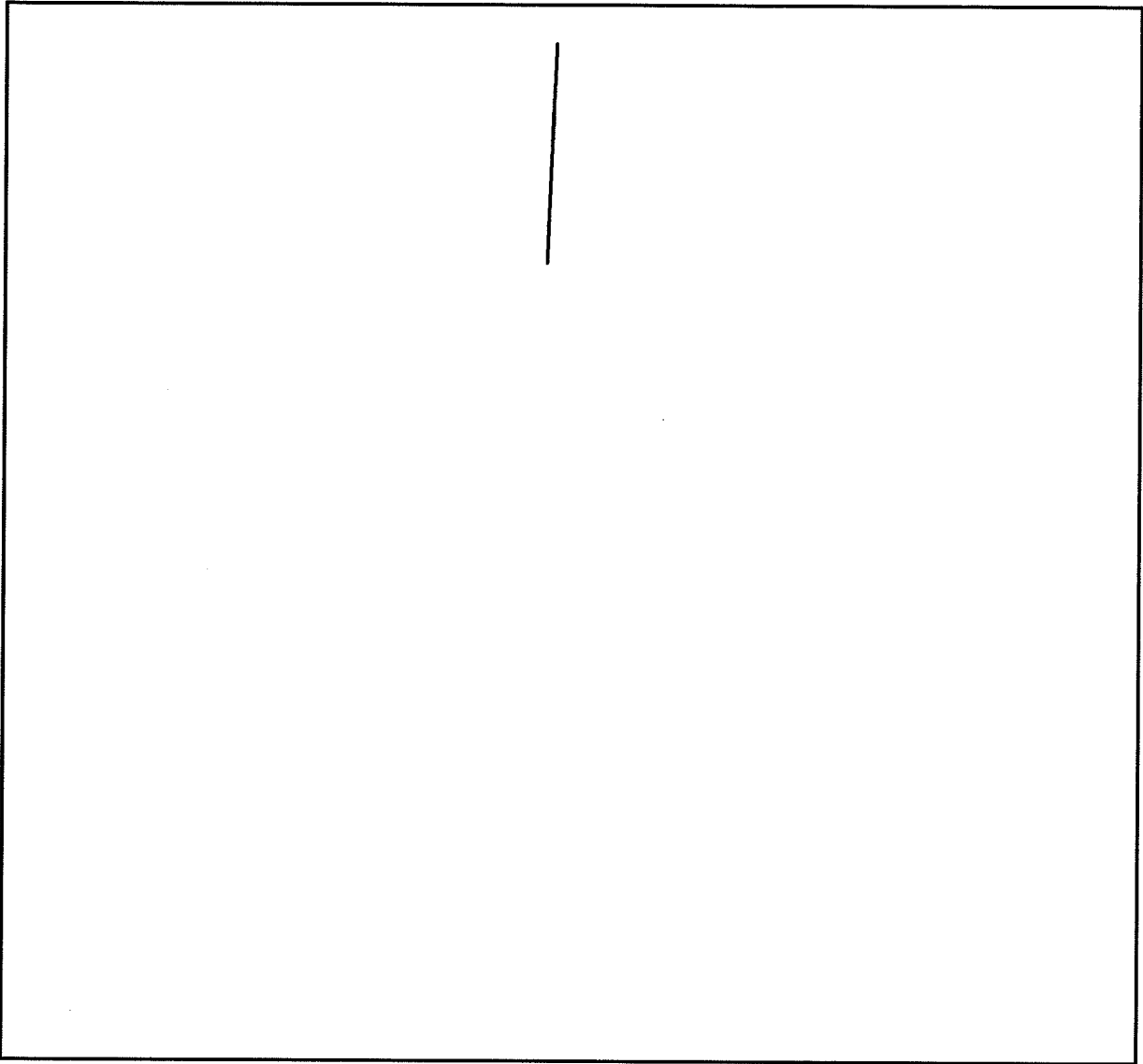
b2
b7E

Operational Subsystem Data Sources

--

Outside the Scope

UNCLASSIFIED//FOR OFFICIAL USE ONLY



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

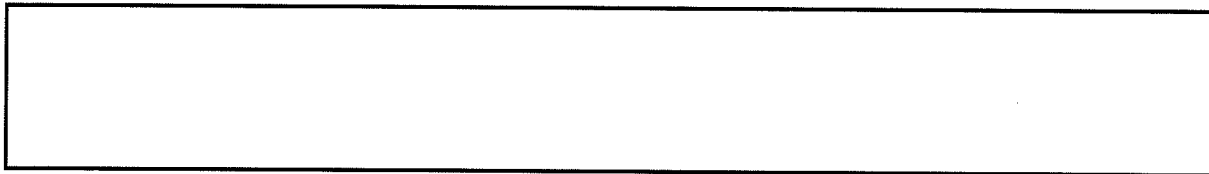
Outside the Scope

UNCLASSIFIED//FOR OFFICIAL USE ONLY

DATASET TYPE	DATA SOURCE	CLASSIFICATION
FBI Case Data	FBI Automated Case System (ACS)	Secret and below
Financial Center (FinCen) Data	<div style="border: 1px solid black; width: 100px; height: 30px;"></div>	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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

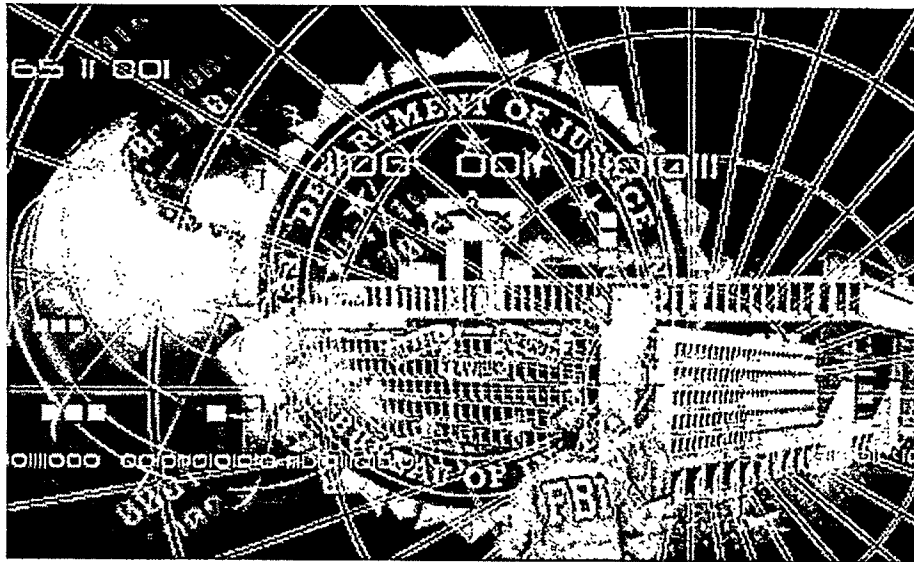
Investigative Data Warehouse - Secret (IDW-S)

System Security Plan

15 January 2005

Version 2.0

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



**INVESTIGATIVE DATA WAREHOUSE – SECRET
(IDW-S)**

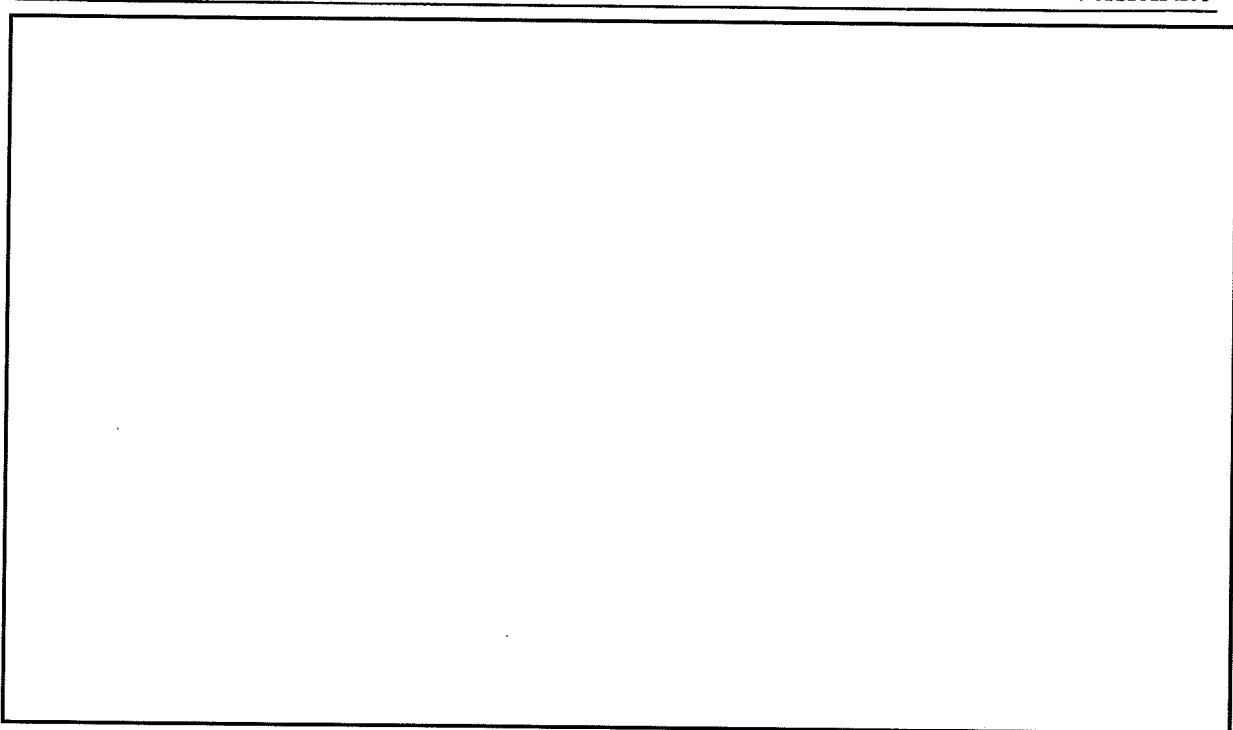
SYSTEM SECURITY PLAN

DOCUMENT VERSION 1.4

15 JANUARY 2005

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

UNCLASSIFIED // FOR OFFICIAL USE ONLY



Automated Transfer of Raw Data to IDW-S

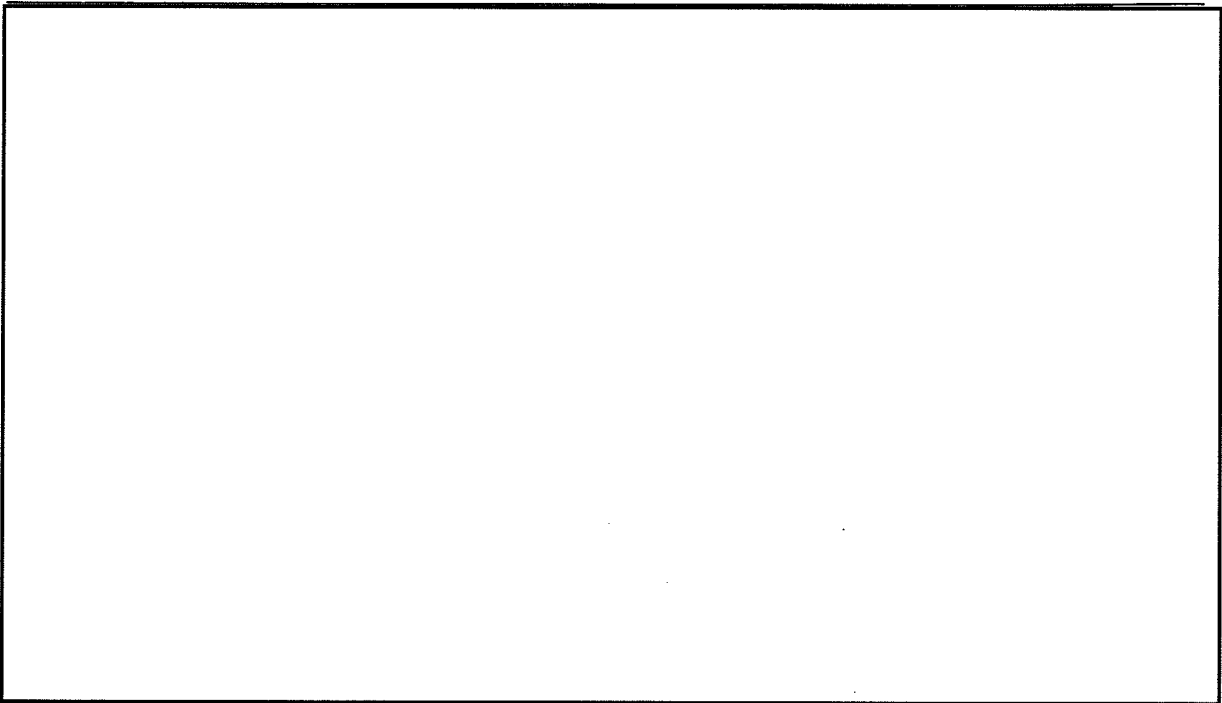
Outside the Scope

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

b2
b7E





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.

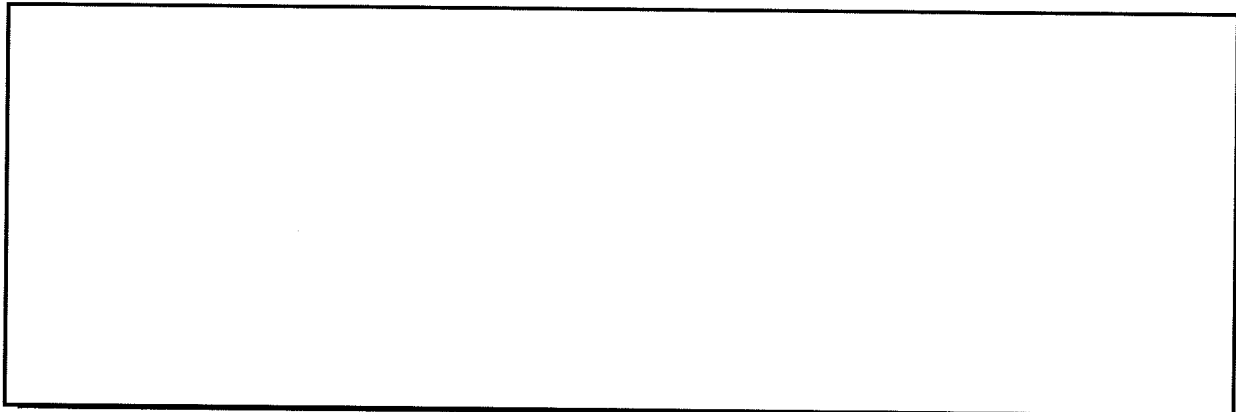
DATASET NAME	DATA SOURCE	CLASSIFICATION	
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below	

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

b2
b7E

Table 3.5.1.1 IDW-S Data Sets



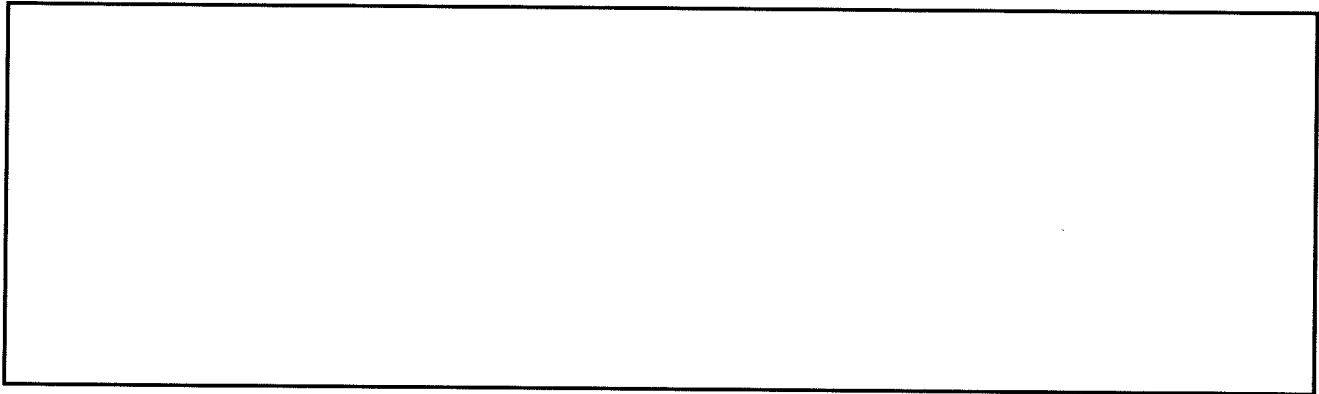
3.9.9 Indirect Connections**3.9.9.1 IDW-S Core Subsystem Indirect Connections**

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

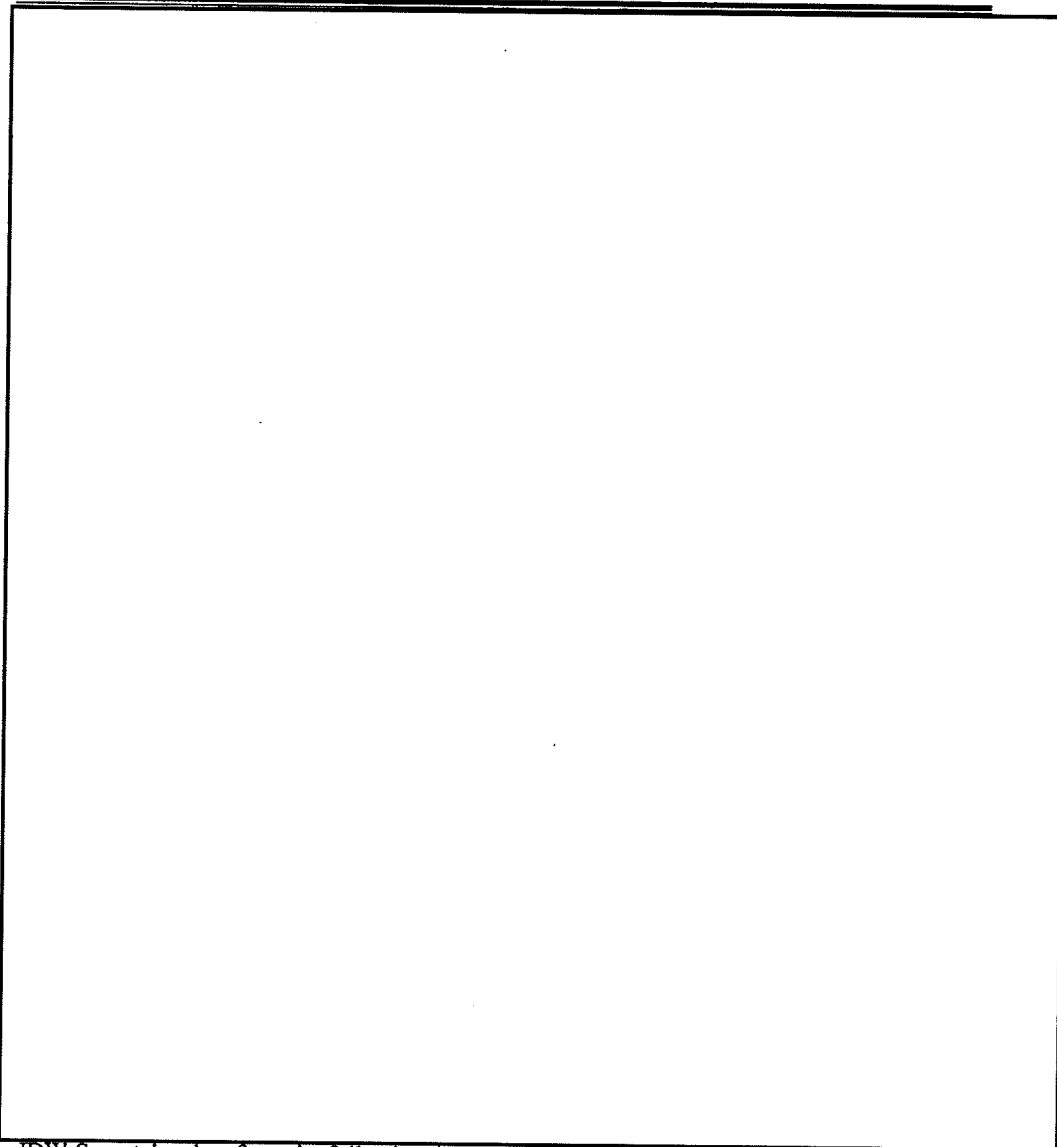
Federal Bureau of Investigation
Information Resources Division
Data Management Section



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

Note: Hardcopy versions of this document must be verified for correct version number with the IDW CM Document Control Library.
PUG NG-OM-0061.11ATO
FOR OFFICIAL USE ONLY



Outside the Scope

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

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

PUG NG-OM-0061.11ATO
FOR OFFICIAL USE ONLY
Page 14

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.

[Redacted]

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

[Redacted]

[Redacted]

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.

Federal Bureau of Investigation
Information Resources Division
Data Management Section



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

Investigative Data Warehouse
Security Operations 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.

**SECOM NG-OM-006.11ATO
FOR OFFICIAL USE ONLY**

Data used in the SES subsystem comes from

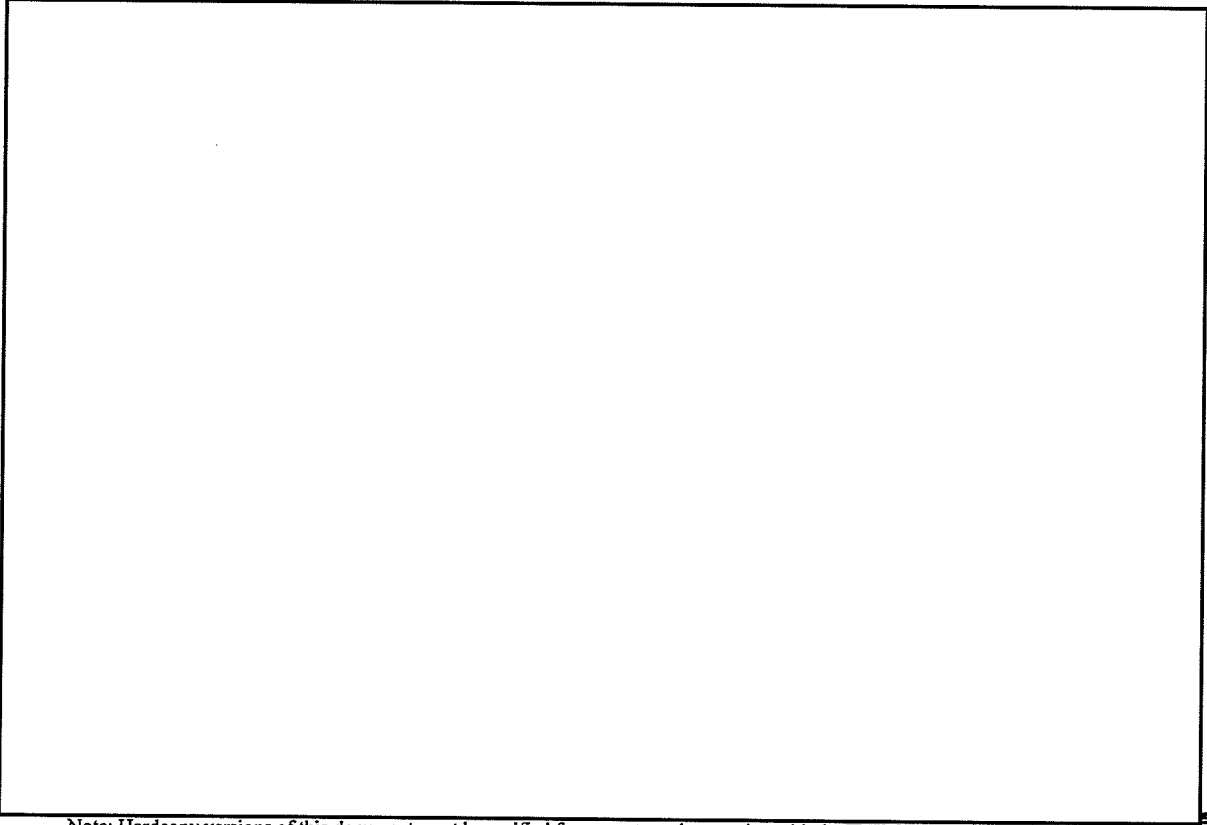
- The standard, customary, data sources for the IDW
- Several SES-unique data sources which are provided for use by a subset of the IDW users.

The SES-specific data sources will include

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

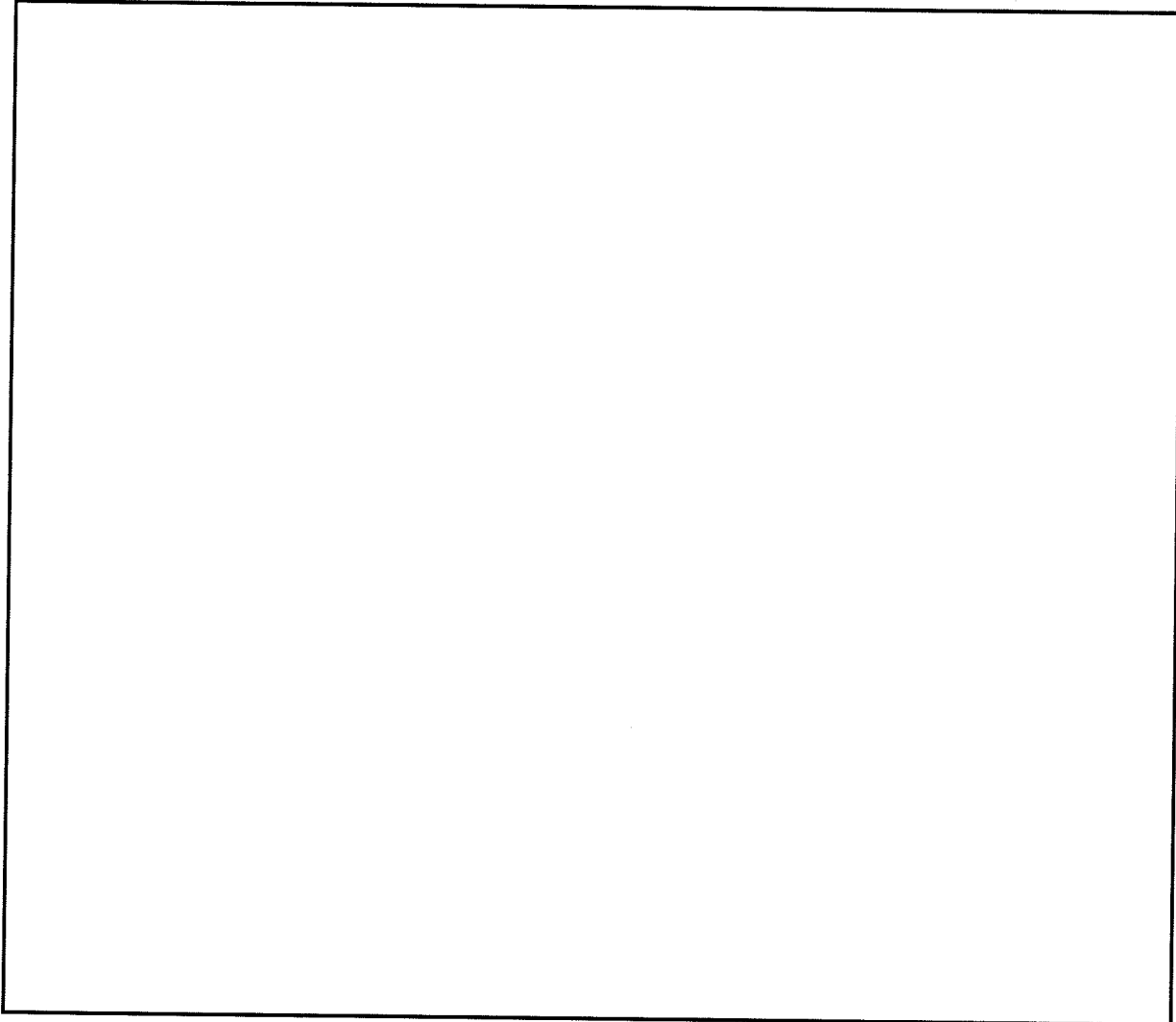
b2
b7E

Outside the Scope



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

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

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

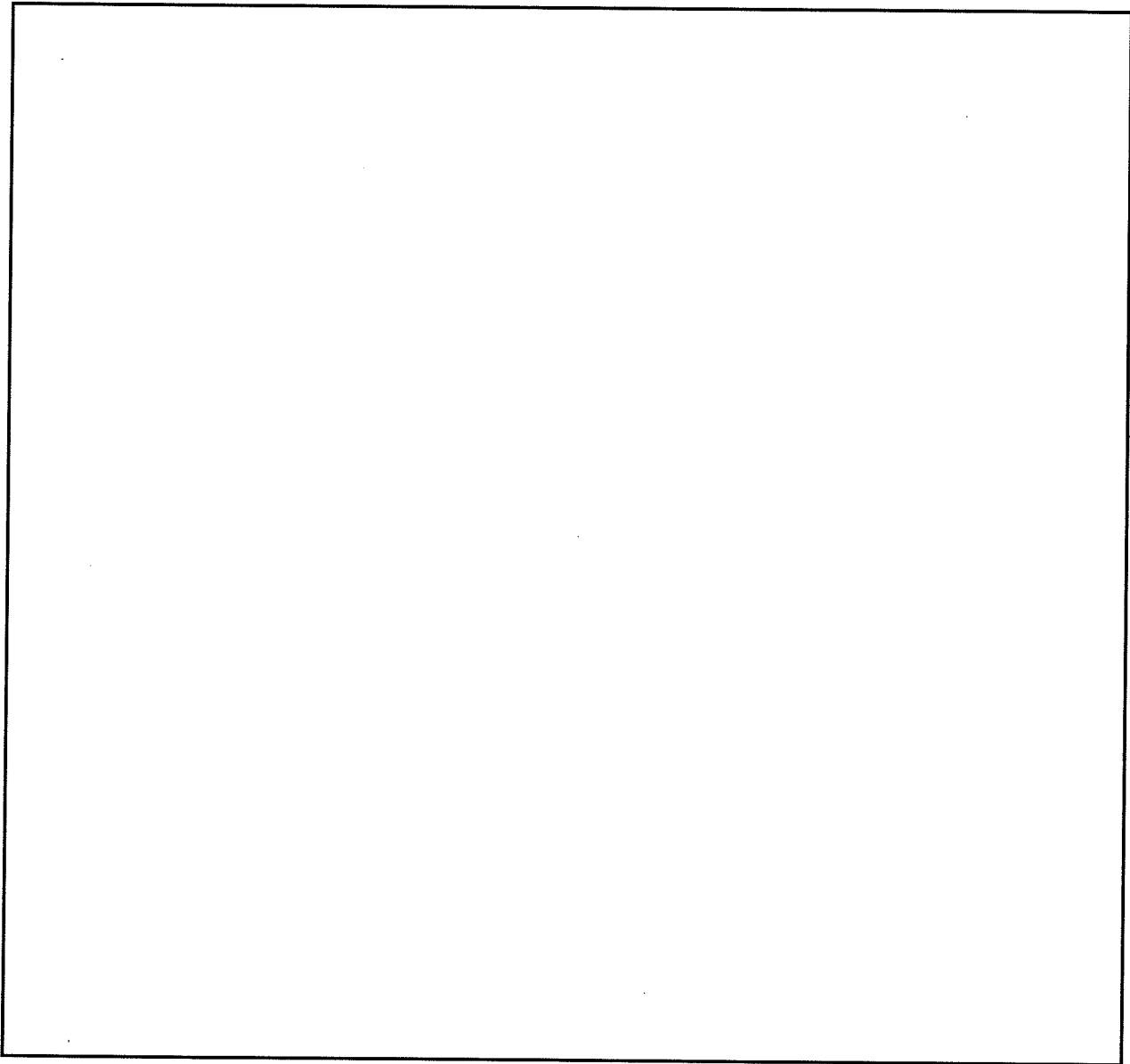
Security Operations Manual
(SECOM)

IDW Operational Services

Version 1.1 ATO

SECOM NG-OM-006.11ATO

-
- 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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

FEDERAL BUREAU OF INVESTIGATION

OFFICE OF THE PROGRAM MANAGEMENT EXECUTIVE



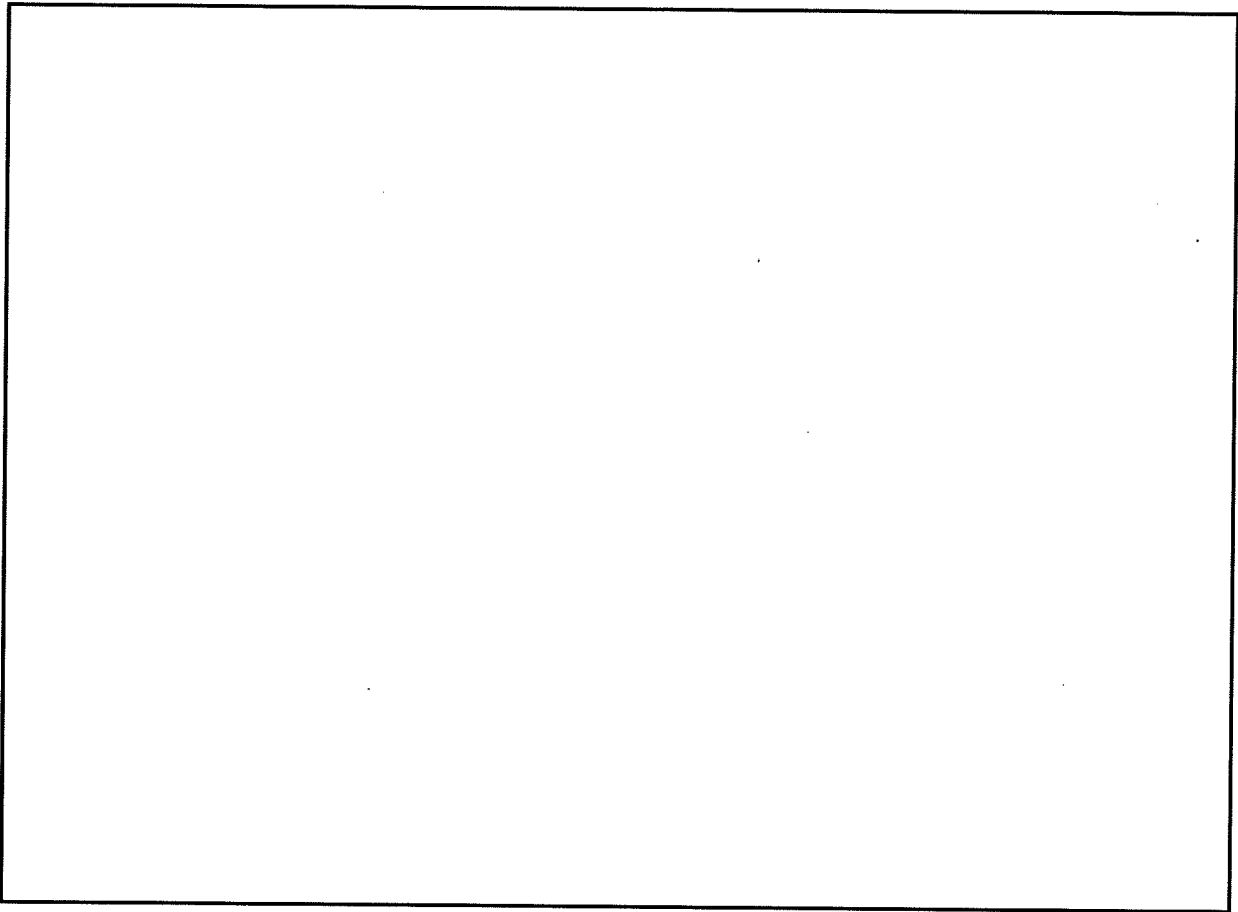
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-28-2008 BY 65179 dmh/bja/cal

1058805

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

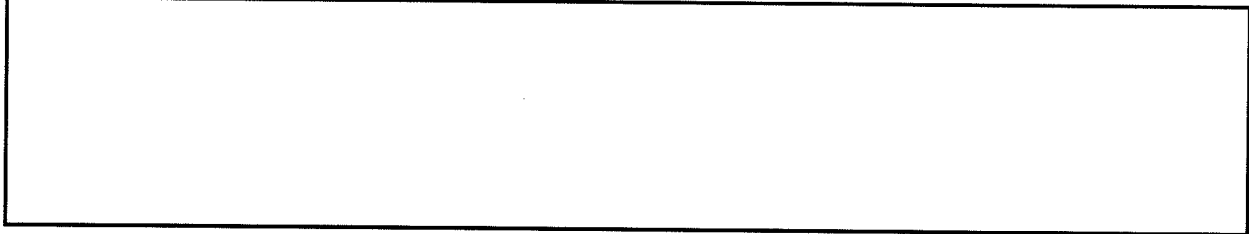
February 7, 2004

UNCLASSIFIED//FOR OFFICIAL USE ONLY



Outside the Scope

2.3.1 IDW-S Operational Subsystem



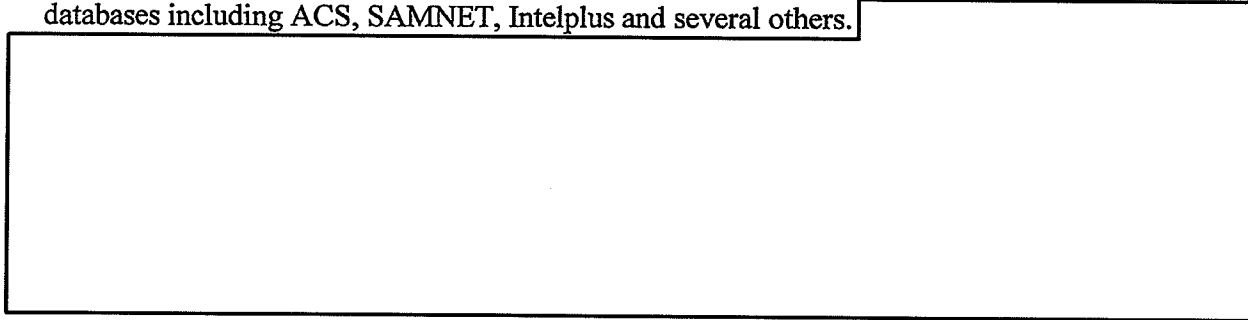
The table below lists the data and sources for the Operational Subsystem.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

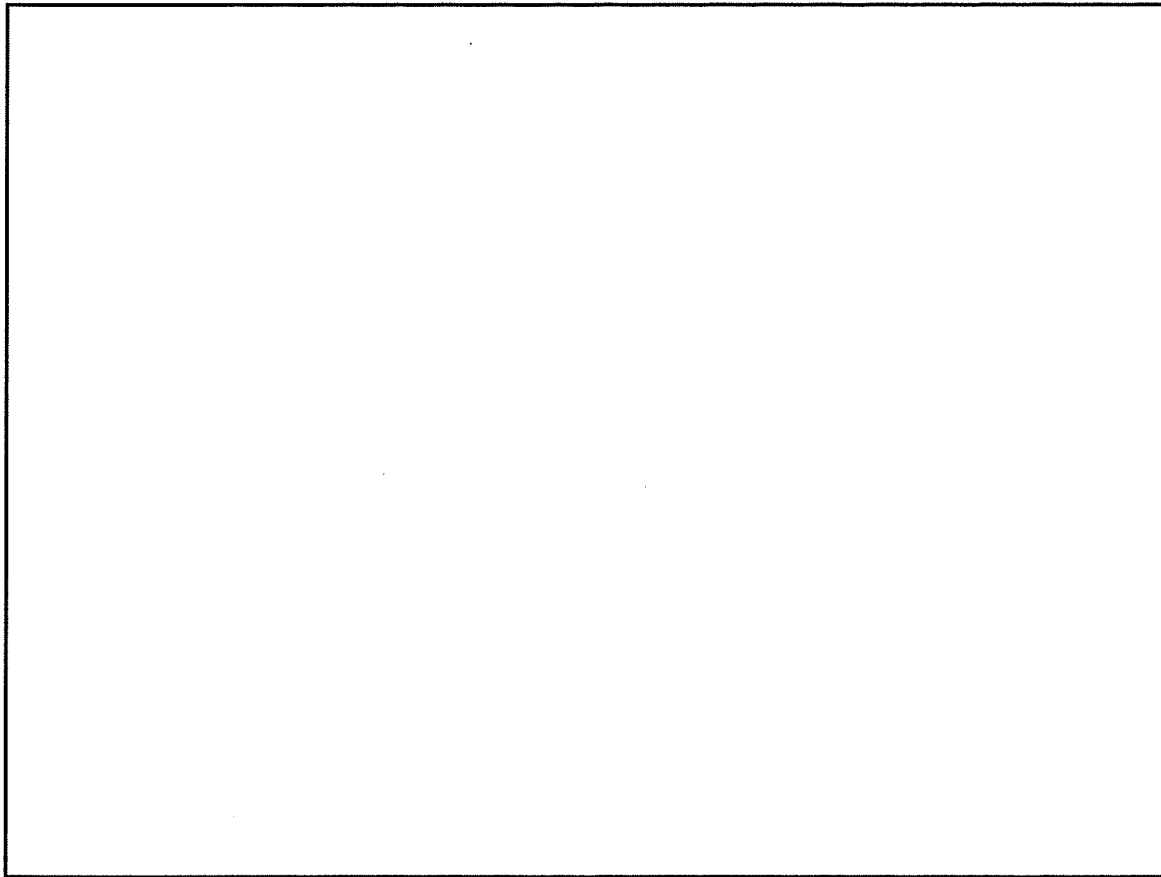
Operational Subsystem Data Sources

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



b2
b7E

UNCLASSIFIED//FOR OFFICIAL USE ONLY



Outside the Scope

2.3.2 Special Projects Team (SPT) Subsystem



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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

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

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED // FOR OFFICIAL USE ONLY

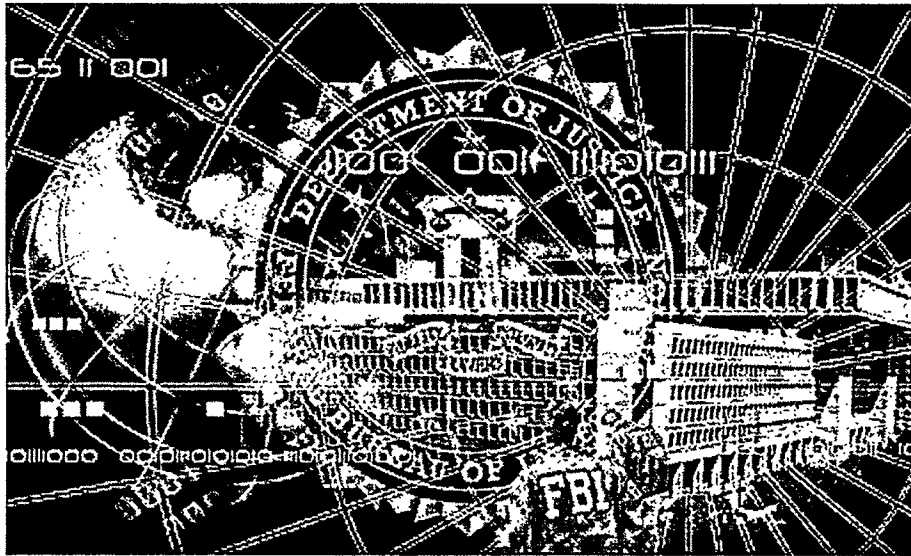
Investigative Data Warehouse - Secret (IDW-S)

System Security Plan

25 January 2005

Version 1.6

**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

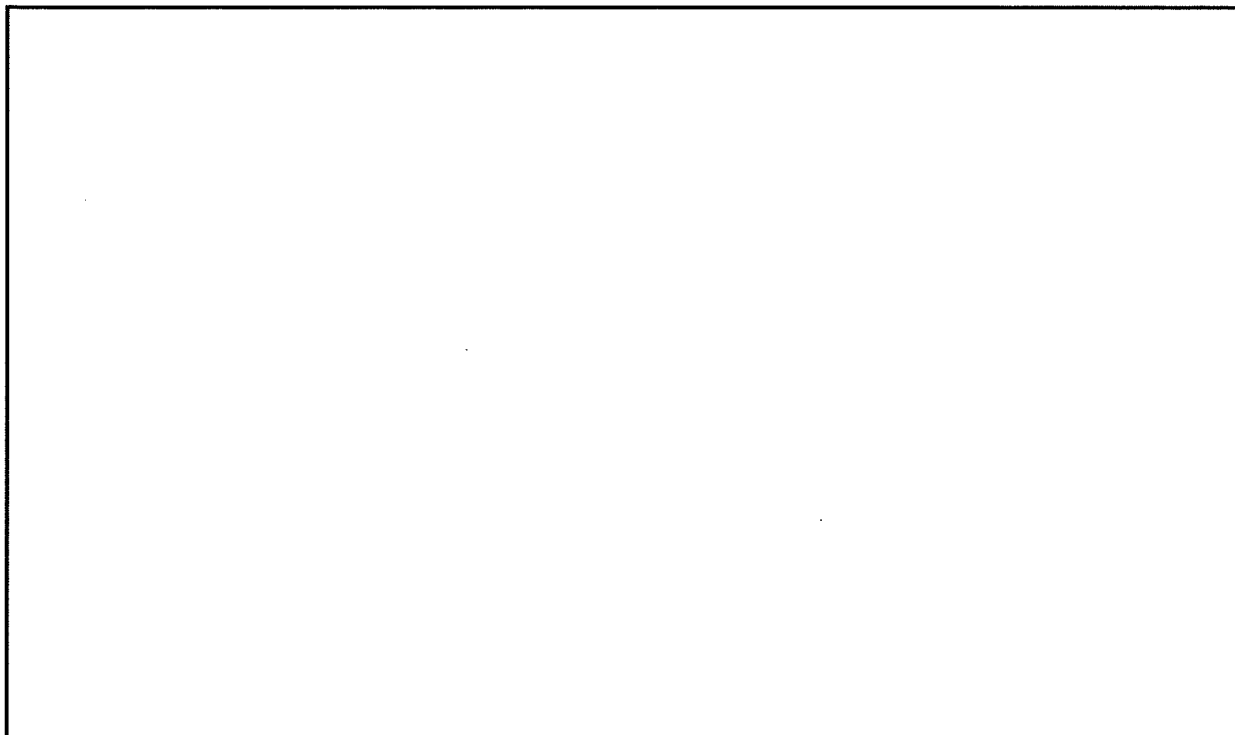
ALL INFORMATION CONTAINED

HEREIN IS UNCLASSIFIED

DATE 01-29-2008 BY 65179 dmh/bja/cal

1058805

UNCLASSIFIED // FOR OFFICIAL USE ONLY



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

b2
b7E



[Redacted]

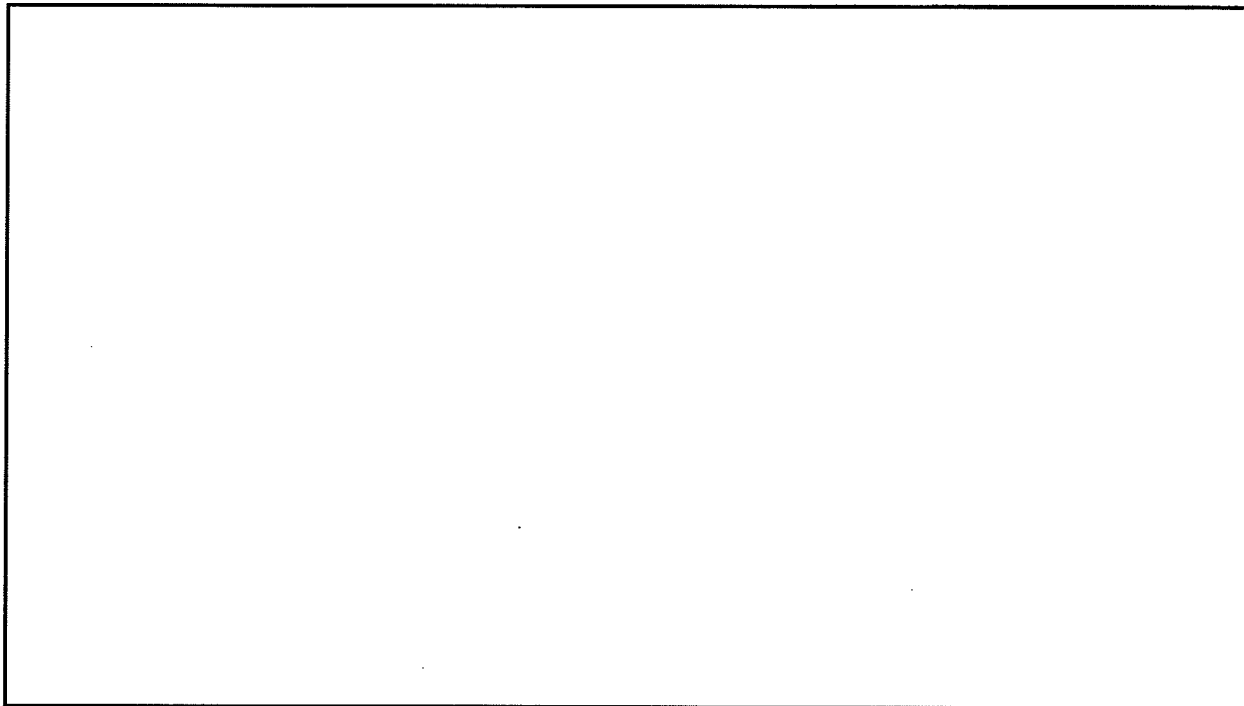
- [Redacted]

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

[Redacted]

Outside the Scope

[Large Redacted Area]



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.

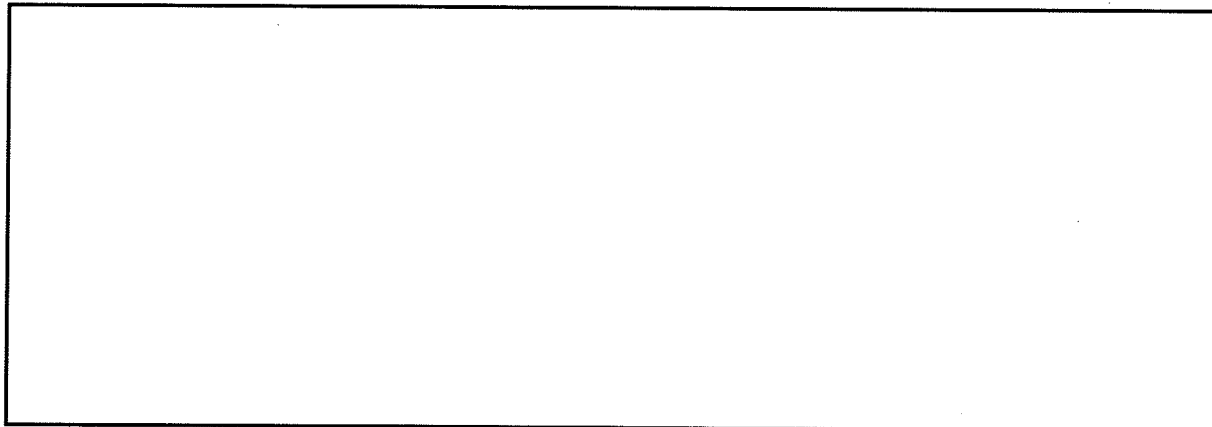
DATASET NAME	DATA SOURCE	CLASSIFICATION	
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below	

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

b2
b7E

Table 3.5.1.1 IDW-S Data Sets



3.9.9 Indirect Connections

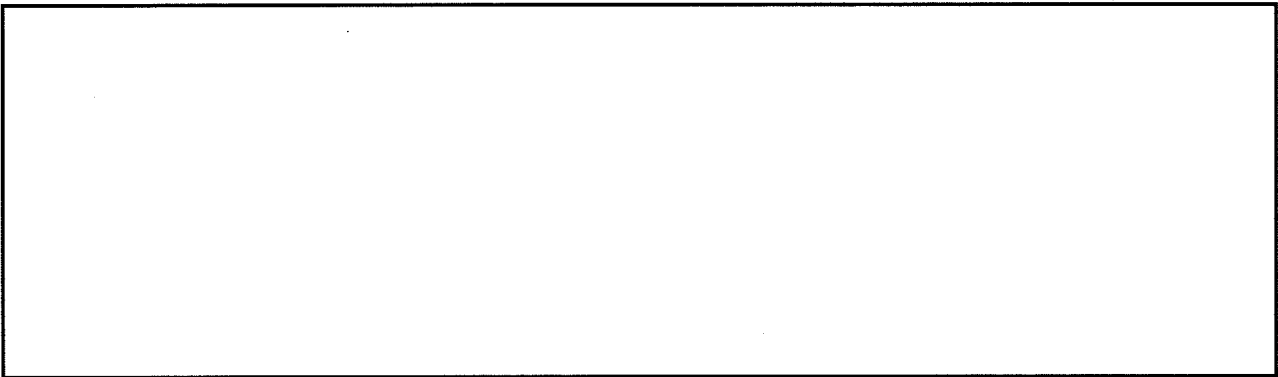
3.9.9.1 IDW-S Core Subsystem Indirect Connections

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

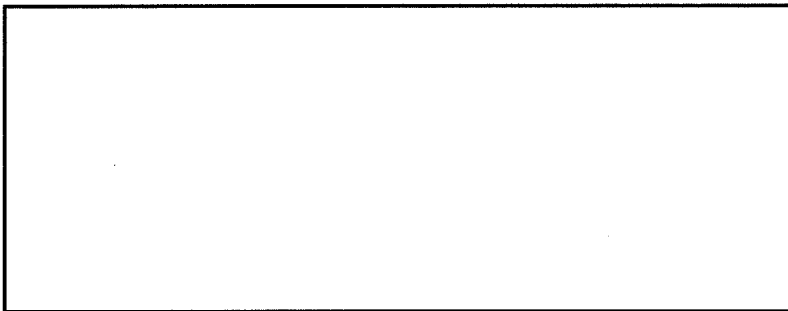
**User Reference for
IDW Version 1.1
Applications**

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

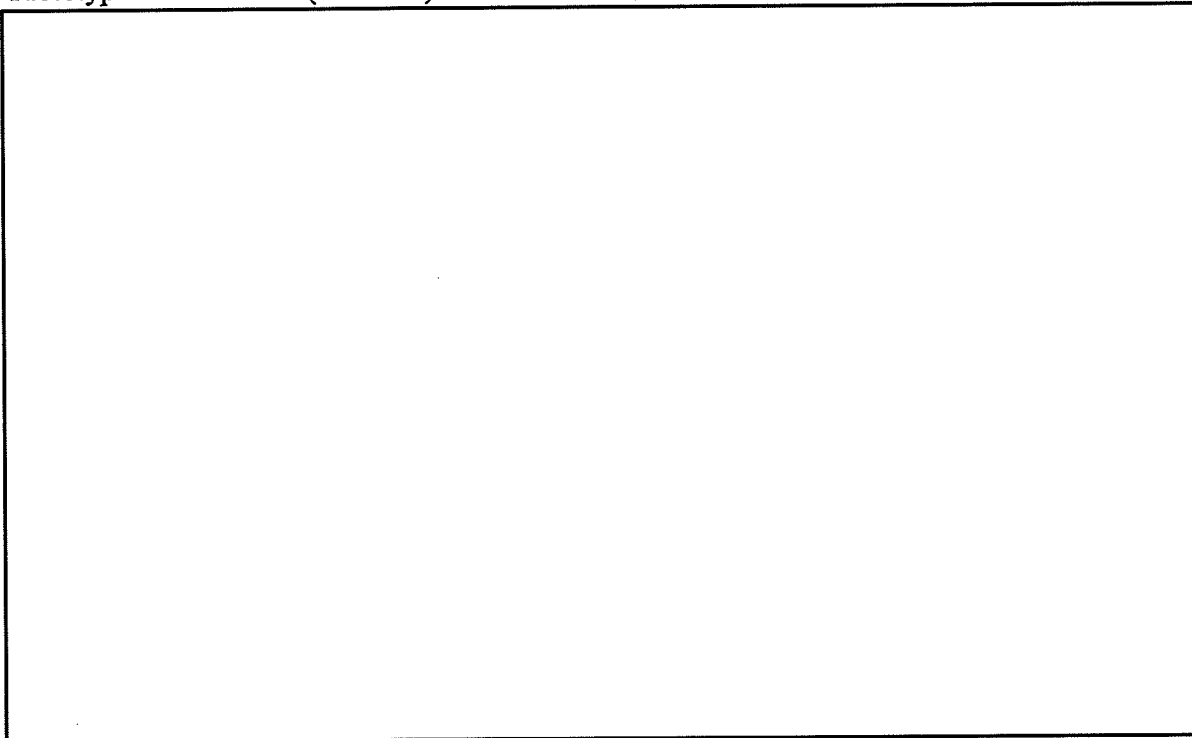
**FEDERAL BUREAU OF INVESTIGATION (FBI),
INFORMATION RESOURCES DIVISION (IRD)**

INVESTIGATIVE DATA WAREHOUSE (IDW) - SECRET

SYSTEM SECURITY PLAN

INTRODUCTION

The Federal Bureau of Investigation's (FBI) Investigative Data Warehouse (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").

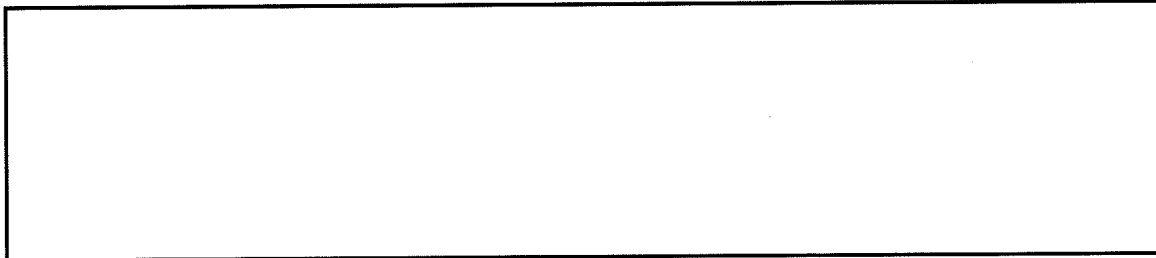


Data processed by the system will include the following data sets:

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;

- 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

[Redacted]

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]

[Redacted]

Data Ingest

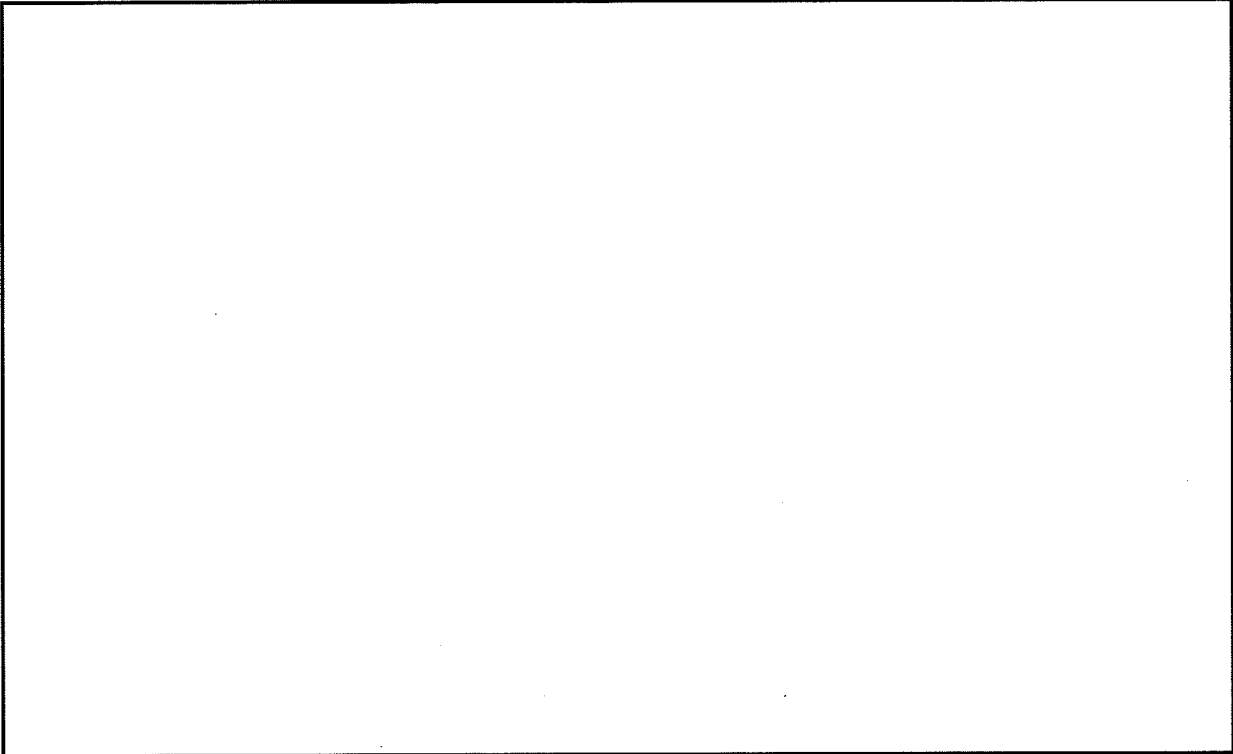
IDW-S receives data from sources [Redacted] (ACS ECF, IntelPlus, SAMNet) and [Redacted] (VGTOF, Open Source News).

[Redacted]

b2
b7E

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

[Redacted]



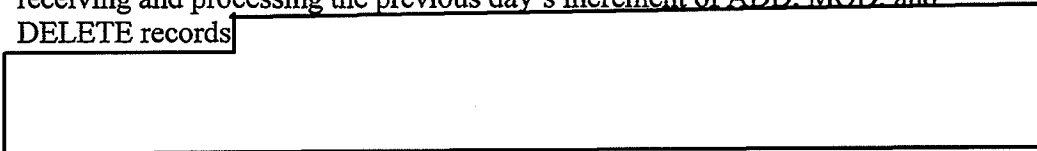
3.5. DATA PROCESSED

Outside the Scope

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

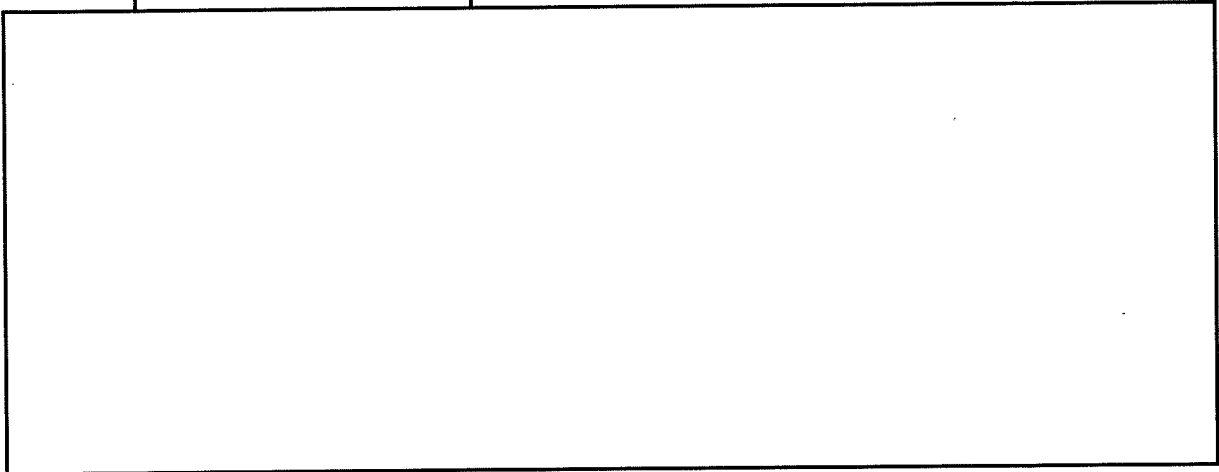
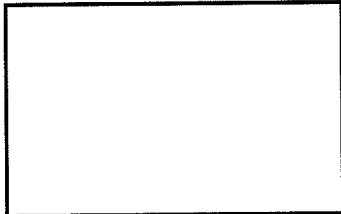


b2
b7E

3.5.2 IntelPlus

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

- 
- 



b2
b7E

3.5.3 SAMNet

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



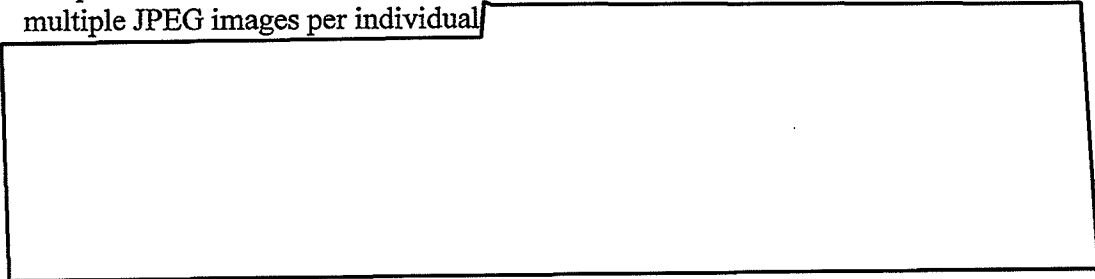
SAMNet provides only ADD record types, and SAMNet data is updated in IDW-S three times a day. SAMNet data



b2
b7E

3.5.4 VGTOF

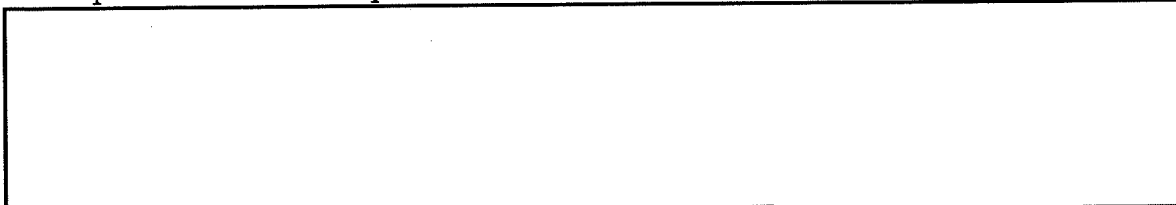
Violent Gang Terrorist Offender File (VGTOF) data is provided by the FBI National Crime Information Center (NCIC). VGTOF data includes two components: Data/metadata for each named individual/offender and potentially multiple JPEG images per individual



b2
b7E

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 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.ina.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.amedia.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	COMMENTS
-----------------	-------------	--------------------	----------

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

