Investigative Data Warehouse (IDW) - Secret System Security Plan 16 January 04 Version 1.0

# **System Security Plan**

# Investigative Data Warehouse-SECRET (IDW-S)

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

> 16 January 2004 Version: 1.0

Federal Bureau of Investigation (FBI), Information Resources Division (IRD) Investigative Data Warehouse (IDW) - Secret System Security Plan 16 January 04 Version 1.0

# Investigative Data Warehouse (IDW) - Secret **System Security Plan**

## TATTOONICTION

INTRODUCTION			
The Federal Bureau of Investigation's (FBI) Investigative Data Warehouse Secret System S) is an initial data warehouse, content management and data mining system that will permit investigative, analytical, administrative and intelligence personnel to access aggregated data previously only available through individual applications. The IDW-S system will be authore to process classified national security data up to, and including, Secret. The IDW-S system successor to the Secure Collaboration Operational Prototype Environment (SCOPE), which originally was named the Secure Counter-Terrorism Operational Prototype Environment.	nit FBI ta norized n is the		
Data processed by the system will include the following data sets:	Outside	the Sco	<b>a</b> ac
<ul> <li>Approved case files from the FBI's Automated Case Support (ACS) case management system;</li> </ul>		che se	)P(
<ul> <li>Electronic versions of the Joint Intelligence Committee Investigation (JIC defined archived documents;</li> </ul>	CI)		

Investigative Data Warehouse (IDW) - Secret System Security Plan 16 January 04 Version 1.0

- 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

<b>Investigative Data</b>	Warehouse (IDW) - Secret
•	System Security Plan
	16 January 04
	Version 1.0

	 	·	

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.

agency) programs.		
PROJECT NAME	CLASSIFICATION/ COMPANIMENUS	
Automated Case System (ACS		
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

Investigative Data Warehouse (IDW) - Secret System Security Plan 16 January 04 Version 1.0

b2 b7E Outside the Scope

Investigative Data Warehouse (IDW) - Secret System Security Plan 16 January 04 Version 1.0

#### 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	DRANSFER MEDIIOD
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

Investigative Data Warehouse (IDW) - Secret System Security Plan 16 January 04 Version 1.0

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

b2 b7E

Data Sources w/Transfer Mechanism

#### **3.5.1 ACS ECF**

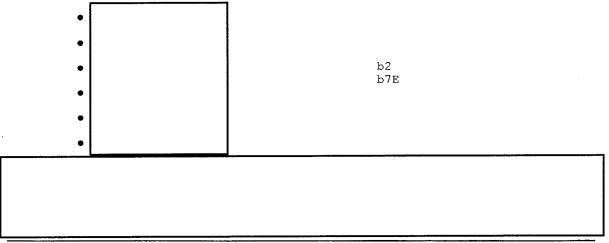
IDW-S contains a subset of the ECF (Electronic Case File) subsystem of the Automated Case System (ACS). This subset consists of serials in those case classifications/sub classifications that have been officially sanctioned for inclusion in IDW-S. For each such serial, the ECF data includes metadata and 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

Investigative Data Warehouse (IDW) - Secret

System Security Plan 16 January 04	
Version 1.0	
	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
	ل
3.5.5 ЛСІ	
	b2
	b7E
	1
TICL is a static collection that is not an I to I	
ЛСІ is a static collection that is not updated.	}
. 25	

Investigative Data Warehouse (IDW) - Secret System Security Plan 16 January 04 Version 1.0

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
once a day. Open Source News data is	
	,
	]

Investigative Data Warehouse (IDW) - Secret

	System Security Plan
•	System Security Plan 16 January 04 Version 1.0
	Version 1.0

#### 3.9.9 Indirect Connections

Outside the Scope

b2 b7E

IDW-S connects to the following sources of data:

SVSTIBM) NAME	CLASSIFICATION & COMPARIMENTS	ACCREDITED BY	URANSFER MEDIOD
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

47

Investigative Data Warehouse (IDW) - Secret System Security Plan 16 January 04 Version 1.0

> b2 b7E

SYSUEM	CLASSIFICATION	A COMPANIES	THE COURTS	COMMENTER
name	CLANDIACAULON &	ACCREDIBLED BAY	TRANSPER	COMMENIS
The state of the s	COMPARTIMENTS	(5)41	MERCOD	
EDI D		 		
FBI Document	Secret	FBI	CD/DVD	
Conversion				
Laboratory		,		
(DocLab),				
Records				
Management			į	
Division				
(RMD),				
FBIHQ				
			•	
Translingual	Unclassified	NA	CD-ROM	
Information	=			
Detection,				
Extraction and	,			
Summarizatio				
n (TIDES)				
Program,				
Defense				
Advanced				
Research				
Projects				
Agency				
(DARPA)		•		
	Unclassified	NA	CD-ROM	
1				

Indirect Connections

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

# 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)

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

## <u>Investigative Data Warehouse (IDW) - Secret</u> <u>System Security Plan</u>

## INTRODUCTION

The Federal Bureau of Investigation's (FBI) Investigative Data Warehouse Secret System (IDVS) is an initial data warehouse, content management and data mining system that will permit Finvestigative, analytical, administrative and intelligence personnel to access aggregated data previously only available through individual applications. The IDW-S system will be authoriz to process classified national security data up to, and including, Secret. The IDW-S system is successor to the Secure Collaboration Operational Prototype Environment (SCOPE), which originally was named the Secure Counter-Terrorism Operational Prototype Environment.	BI ed
Data processed by the system will include the following data sets:	
<ul> <li>Approved case files from the FBI's Automated Case Support (ACS) case management system;</li> </ul>	Outside the Scope
<ul> <li>Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents;</li> </ul>	
-1-	
INCLASSIETED // EOD OBBIGIAL MOD OWN	
UNCLASSIFIED // FOR OFFICIAL USE ONLY	•

Investigative Data Warehouse (IDW) - Secret
System Security Plan

19 December 2003
Version 0.8

- 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

 314
·

Outside the Scope

-2-

Investigative Data Warehouse (IDW) - Sec System Security Pl 19 December 20 Version 0	an O3
Data Sources	
IDW-S contains data from the following data sources with security classification indicated in brackets:	Outside the Scope

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

- 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 analytical tools.	direct the
Data Ingest	
IDW-S receives data from sources by FTP over FBINet (ACS ECF, IntelPlus, and SA	MNet) and
CD-ROM (VGTOF, Open Source News)	
Data is received by the Ingest Subsystem	
•	
<ul> <li>Received data is parsed into individual serial records (in the case o ECF), documents (IntelPlus, JICI, Open Source News), messages ( or files (VGTOF).</li> </ul>	
1	
• 1	

Investigative Data Warehouse (IDW) - Secre System Security Plan	
System Security Plar  19 December 2003  Version 0.8	
Version 0.8	<u>1</u>
	1
	•
	Outside the Scope
	,
	•
	f
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

-21-

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

UNCLASSIFIED // FOR OFFICIAL USE ONLY

-22-

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

> b2 b7E

<u>19</u> December 2003
Version 0 <u>.8</u>
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
The state of the s
3.5.5 ЛСІ
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
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-

Investigative Data Warehouse (IDW) - Secret
System Security Plan

19 December 2003
Version 0.8

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.ve

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/

-24-

Investigative Data Warehouse (IDW) - Secret
System Security Plan

19 December 2003
Version 0.8

			19 December 2003 Version 0.8	
Uzbekistan F Washington XinHua New Yemen Time Yomiuri Shi	vs - http://www.umm Report - http://www.u Post - http://www.wa vs Service - http://ww es (weekly) - http://w mbun (Japan) - http://	zreport.com/er shingtonpost.c w.xinhuanet.co ww.yementime /www.yomiuri	om/ om/english/ ss.com/	
	mary of Data Sou	***************************************		
DATASET NAME	DATASOURCE	MEDITOD		
ACS	FBI Automated Case System (ACS)	FTP		b2 ъ7Е
IntelPlus	FBI Intel Plus	FTP		Outside the Scope
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	FTP		
VGTOF	FBI National Crime Information Center (NCIC)	CD-ROM		
лсі	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Multiple		

-25-

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

DATASET NAME	DAVIA SOURCE Translingual	ORONSTOR MEDICOD		
Open Source News	Translingual Information Detection, Extraction and Summarization (TIDES) Program, Defense Advanced Research Projects Agency (DARPA)	CD-ROM		.b2 .b7E
				•
				Outside the Scope
			ļ	
			ļ	

-26-

	System Security Plan	
	19 December 2003	
	Version 0.8	•
_	1 42101 43	
_		1
١		
ł		
Т		
1		
١		
1		
		•
ı		
ł		•
1		
1		
1		

#### 3.9.9 Indirect Connections

Outside the Scope

IDW-S connects to the following sources of data:

SASSITEM INAME	CLASSIFICATION & COMPARIMENUS	ACC REDITED BY	TRANSPER METHOD
FBI Automated Case System (ACS)	Secret	FBI	FTP
FBI Intel Plus	Secret	FBI	FTP

b2 b7**E** 

-40-

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

	SVSUFM NAME	CLASSIFICATION & COMPARIMIENTS	ACCREDITED BY	TRANSFER METILOD	COMMENTS	
•	FBI Secure Automated Messaging Network (SAMNet)	Secret	FBI	FTP		
	FBI National Crime Information Center (NCIC)	Unclassified/SBU	FBI	CD-ROM		
1	FBI Document Conversion Laboratory (DocLab), Records Management Division (RMD), FBIHQ	Secret	FBI	Multipld	·	b2 b7E Outside the Scope
autorija.	Translingual Information Detection, Extraction and Summarizatio n (TIDES) Program, Defense Advanced Research Projects Agency (DARPA)	Unclassified	NA	CD-ROM		

-41-

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

SVSTJEM NAME	CLASSIFICATION & COMPARTMENUS	ACCREDITED BY	TRANSFER METHOD	Complines
	Unclassified	NA	CD-ROM	
		Indirect Conne	-42	

b2 b7E

-42-

## Maintenance Manual (MM)

Version 1.1 ATO

## **IDW Operational Services**

MM NG-OM-004.11ATO

# 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
Maintenance Manual
Version 1.1 for Authority to Operate
June 11, 2004

Version 1.1 ATO

MM NG-OM-004.11ATO

#### 1 Introduction

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.

# System Administrator Manual (SAM)

Version 1.1 ATO

сору

IDW Operational Services

SAM NG-OM-005.11ATO

# 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

# System Administrator Manual (SAM)

IDW Operational Services

Version	1	1	ATO.
A CISIOII	Ł	٠Ł	AIU

SAM NG-OM-005.11ATO

1.4.1.1Data Sources  The FBI maintains large databases of records. These records are recorded in both standard and vendor/developer unique formats.	the	Scope
	b2 b7E	
<ul> <li>Data processed by the system includes the following sources:</li> <li>Approved case files from the FBI's Automated Case Support (ACS) management system;</li> <li>Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents;</li> <li>Secure Automated Messaging Network (SAMNet) message traffic;</li> <li>IntelPlus (INTEL+) File Rooms;</li> </ul>		
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		

SAM NG-OM-005.11ATO FOR OFFICIAL USE ONLY Page 2

# System Administrator Manual (SAM)

Version 1.1 ATO

Information Systems (CJIS) Division;

## **IDW** Operational Services

**SAM NG-OM-005.11ATO** 

<ul> <li>Defense Advanced Research Projects Agency (DARPA) Translingual Information Detection, Extraction and Summarization (TIDES) Open Source Data.</li> </ul>				
4				
				·

• Violent Gang and Terrorist Organization File (VGTOF) from the Criminal Justice

#### **DRAFT**

UNCLASSIFIED//FOR OFFICIAL USE ONLY

# 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

UNCLASSIFIED//FOR OFFICIAL USE ONLY	
	:*  :
	, i
	·
	Outside the Scop
The table below lists the data and garmens for the Consectional Calculation	Ourside tile scol

# DRAFT

DADASEII		
RANNE	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
нсі	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below
Open Source News	MiTAP[	Unclassified
	(	Operational Subsys
The data	flow begins at the	external data sources
iatabases inc	luding ACS, SAM	NET, Intelplus and

#### DRAFT

UNCLASSIFIED//FOR OFFICIAL USE ONLY				

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

Outside the Scope

# DRAF'T UNCLASSIFIED//FOR OFFICIAL USE ONLY

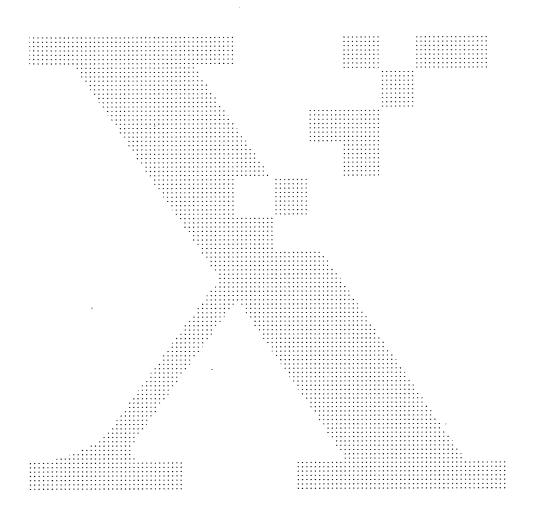
DESCRIPTION OF THE PROPERTY OF	DAVIA SOURCE	AOTOANTEEALIN
FBI Case Data	FBI Automated Case System (ACS)	Secret and below
Financial Center (FinCen) Data		SBU
Various Lists of Data	Various Sources, e.g., Transportation Security Administration (TSA)	SBU
Various CTD Datasets	FBI Counterterrorism Division (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

# Jarmel-sanchez



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

#### UNCLASSIFIED//FOR OFFICIAL USE ONLY

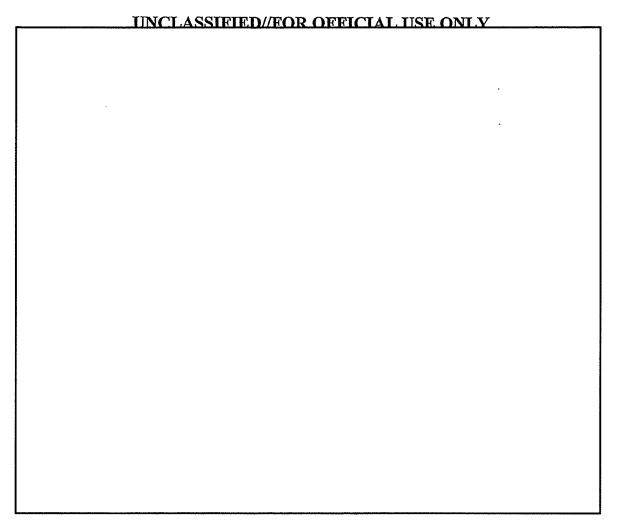
DATASET NAME	DATA SOURCE	CLASSIFICATION
NEW IN	DEVIA SOURCE	OPAPOINT VAINING
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below
IntelPlus Filerooms	FBI IntelPlus	Secret and below
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below
VGTOF	FBI National Crime Information Center (NCIC)	SBU
лсі	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.	1
Γ		1
		1
١		1
١		
1		l

Outside the Scope

b2 b7E



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.

#### 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

August 2005	UNCLASSIFIED // FOR OFFICIAL USE IDW-D System Security Plan	ONLY Version 1.2 Outside the S	Scope
Examp	les of unclassified operational data processed by the	ne IDW-D system include:	
•		ъ2 ъ7Е	
• Violent G	ang and Terrorist Organization File (VGTOF)		

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

Draft

	17 A	nent System ecurity Plan Lugust 2004 Version 0.6
	• Approved case files from the FBI's Automated Case Support (ACS) Case File (ECF) case management system,	Outside the Scope Electronic
	• Secure Automated Messaging Network (SAMNet) message traffic,	
	• IntelPlus File Rooms,	
	•	
		b2 b7E
,	<u> </u>	
	• Universal Name Index (UNI), and	
	<ul> <li>Violent Gang and Terrorist Organization File (VGTOF") from the C Justice Information Systems (CJIS) Division.</li> </ul>	Criminal
		Outside the Scope
	-11-	
	UNCLASSIFIED // FOR OFFICIAL USE ONLY	

Investigative Data Warehouse Secret Development System
System Security Plan
17 August 2004
Draft Version 0.6

		1	
		,	
·			
		-Outside	the Sc
	<ul> <li>Approved case files from the FBI's ACS ECF case management system;</li> </ul>		
	• Electronic versions of the JICI) defined archived documents;		
	SAMNet message traffic;		
	-30-		
	UNCLASSIFIED // FOR OFFICIAL USE ONLY		

Draft

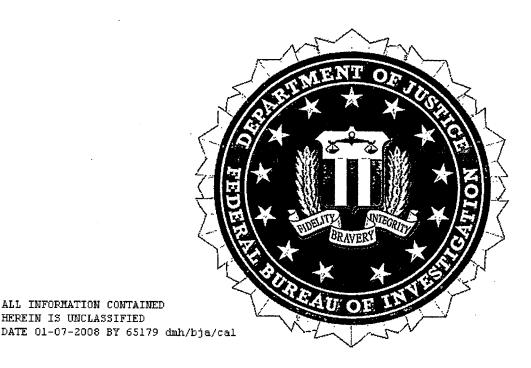
Investigative Data Warehouse Secret Development System
System Security Plan
17 August 2004
Draft Version 0.6

• UNI, and	b2 Ъ7E
VGTOF from CJIS Division.	Outside the Sco
• •	
-31-	

> 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

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

**DOCUMENT VERSION 0.7 25 OCTOBER 2004** 

Investigative Data Warehouse Secret Development System
System Security Plan
25 October 2004
Draft Version 0.7

	Draft Version 0.7	_
	<ul> <li>Approved case files from the FBI's Automated Case Support (ACS) Electronic Case File (ECF) case management system,</li> </ul>	
	Secure Automated Messaging Network (SAMNet) message traffic,	
	• IntelPlus File Rooms,	
	·	
	b2	·
	• b7	
	•	
	Universal Name Index (UNI), and	
	<ul> <li>Violent Gang and Terrorist Organization File (VGTOF") from the Criminal Justice Information Systems (CJIS) Division.</li> </ul>	
<u> </u>		
	Outside the	∋ S
	•	
	-11-	•

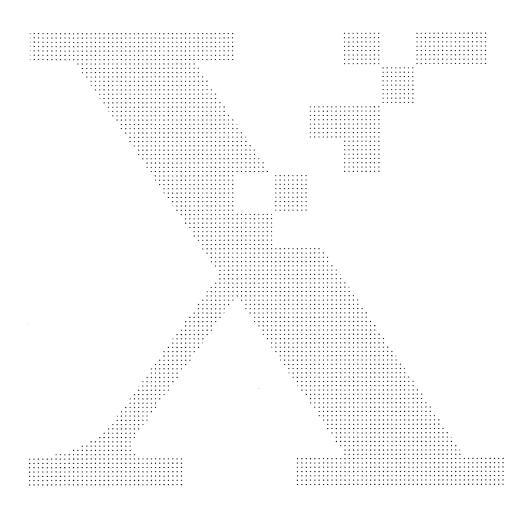
Investigative Data Warehouse Secret Development System
System Security Plan
25 October 2004

	Draft Version 0.7
	1
	·
	ļ
	į
	}
3.5. DATA PROCESSED	Outside the Scop
The IDW-DS system includes the following types of data. Rep	resentative samples of
hese data sets are used. Enough data is available in order to support deve	elopment while
ninimizing the security risk.	and the second s
·	•
<ul> <li>Approved case files from the FBI's ACS ECF case man</li> </ul>	agement system;
<ul> <li>Electronic versions of the JICI) defined archived docum</li> </ul>	ents;
C13 OI	
SAMNet message traffic;	
<b>-30-</b>	
INCLASSIFIED // FOR OFFICIAL USE ON	IT V

Investigative Data Warehouse Secret Development System
System Security Plan
25 October 2004
Draft Version 0.7

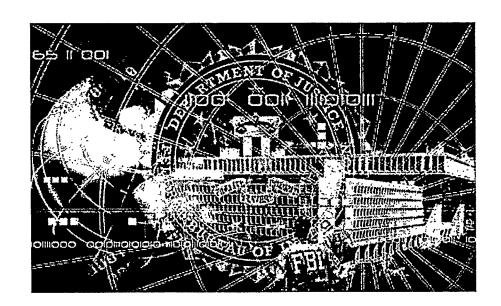
	• IntelPlus File Rooms; • UNI, and	b2 b7E	
	• VGTOF from CJIS Division.		
<u></u>	-31-	Outside th	he Sco
	UNCLASSIFIED // FOR OFFICIAL USE	ONLY	

#### Jarmel-sanchez



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 Investigative Data Warehouse - Secret (IDW-S) System Security Plan

23 June 04 Version 1.3

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

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
23 June 04
Version 1.3

1
·
·
1
i
l l
i
I I
I
l l
l l
i de la companya de
· ·
l l
I I
1

#### 3.9.9 Indirect Connections

Outside the Scope

#### 3.9.9.1 IDW-S Core Subsystem Indirect Connections

SAZIEM VAWIE	GLASSIFICATION & COMPARIMENTS	ACCREDITED BY	TRANSPER MEJUOD
FBI Automated Case System (ACS)	Secret	FBI	FTP

-46-

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Investigative Data Warehouse - Secret (IDW-S) System Security Plan
23 June 04 Version 1.3

SYSTEM NAME	CLASSIFICATION &	ACCREDITED BY	TRANSFER MEDIOD
FBI Intel Plus	COMPARIMENTS Secret	FBI	FTP
1 DI Mici I ius	Beerer	121	1
•			·
FBI Secure Automated	Secret	FBI	FTP
Messaging Network			
(SAMNet)			
FBI Document Conversion	Secret	FBI	CD/DVD
Laboratory			
(DocLab), Records	· Secretaria		
Management Division (RMD),			
FBIHQ			
ı İ			
	<u>-</u>	CD-ROM, Disk,	
FBI National Crime	Unclassified/SBU	FBI	CD-ROM
Information			
Center (NCIC) MiTAP	Unclassified	NA	CD-ROM
			<u> </u>  -
			<u> </u>

-47-

#### FEDERAL BUREAU OF INVESTIGATION

#### OFFICE OF THE PROGRAM MANAGEMENT EXECUTIVE

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED



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.

DATIASET 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
лсі	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below
Open Source News	MiTAP	Unclassified

Operational Subsystem Data Sources

Outside the Scope

b2

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

Outside the Scope

50 A 50 A 50 T 50		<u> </u>
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

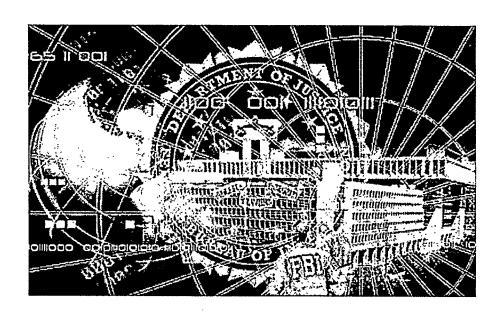
#### **SPT Data Sets**

İ		
1		

Outside the Scope

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

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
15 January 2005
Version 2.0

Automated Transfer of Raw Data to IDW-S	he Scope:
Raw data is automatically transferred to the IDW-S system from approved data sources accordance with an Interconnection Agreement, Memorandum of Understanding, Memorandum of Agreement or Interface Control Document. IDW-S V1 receives updated 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	b2 b7E

-30-

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

VGTOF data is transmitted to the IDW-S system

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
15 January 2005
Version 2.0

l		
İ		
l		
l		
İ		
l		
1		
l		
		ľ
351	Data Processed	
J.J.1	Data I Tucesseu	Outside the

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		CLASSIFICATION
ACS Electronic Case Files (ECF)	I Caca Stretam	Secret and below

-44-

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
15 January 2005
Version 2.0

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
ЛСІ	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below
Open Source News	МіТАР	Unclassified
		Table 3.5.1.1 IDW-

-45-

Outside the Scope

UNCLASSIFIED // FOR OFFICIAL USE ONLY

b2 b7E

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
15 January 2005
Version 2.0

#### 3.9.9 Indirect Connections

#### 3.9.9.1 IDW-S Core Subsystem Indirect Connections

GOVERNO DIAMES LOS ACCORDOS LACOSTOS LA			
Sysiem name	CLASSIFICATION & COMPARIMENTS	ACCREDITED BY	FRANSFER MAJUOOD
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

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
15 January 2005
Version 2.0

SYSTEM MAME	CLASSIFICATION & COMPARIMENTS	ACCREDITED BY	Transfer Method	
MiTAP – Open · Source News	Unclassified	NA	CD-ROM	b2 b7E
	·			

Outside the Scope

-53-

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

Privileged Users Guide Version 1.1 ATO	PUG NG-OM-0061.11ATO	
		Outside the Scope
	•	
IDW-S contains data from the follobrackets:	owing data sources with security classification indicated in	
Note: Hardcopy versions of this document mu	ust be verified for correct version number with the IDW CM Document Control Library. PUG NG-OM-0061.11ATO FOR OFFICIAL USE ONLY Page 14	·

#### Privileged Users Guide (PUG)

Version 1.1 ATO

IDW Operational Services PUG NG-OM-0061.11ATO

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.

PUG NG-OM-0061.11ATO

FOR OFFICIAL USE ONLY

Page 15

#### Security Operations Manual (SECOM)

Version 1.1 ATO

IDW Operational Services

SECOM NG-OM-006.11ATO

#### 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

#### Security Operations Manual (SECOM)

**IDW Operational Services** 

Version 1.1 ATO

SECOM NG-OM-006.11ATO

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.

Financial Center (FinCen)      Financial Center (FinCen)	<b>7</b> ·			
•				
• NoFly	b2			
• Selectee	b7E			
•				
•				
Unified Name Index (UNI) extracts				
•	2	. 1	~	
	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

#### Security Operations Manual (SECOM)

**IDW** Operational Services

Version 1.1 ATO

SECOM NG-OM-006.11ATO

2 System Security Overview	
	Outside the S
Data processed by the system will include the following data sets:	
<ul> <li>Approved case files from the FBI's Automated Case Support (AC</li> </ul>	S) case management

ope

- 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 Page 0

## Security Operations Manual (SECOM)

IDW Operational Services

Version 1.1 ATO

SECOM NG-OM-006.11ATO

•	Information Systems (СЛS) Division;				

Outside the Scope

## Security Operations Manual (SECOM)

IDW Operational Services

Version 1.1 ATO

SECOM NG-OM-006.11ATO

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

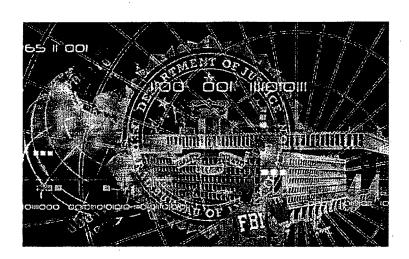
- Automated Case Support (ACS) System, Electronic Case File (ECF) Subsystem [Secret and below]
- IntelPlus [Secret and below]
- Secure Automated Message Network Secret (SAMNet-S) [Secret and below]
- NCIC Violent Gang and Terrorist Offender File (VGTOF) [Sensitive But Unclassified]
- Joint Intelligence Committee Investigation (JICI) [Secret and below]

	•	DARPA/TIDES Open Source News [Unclassified]	Outside	the	Scope
Í					
I					
	<u> </u>				

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 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

### Investigative Data Warehouse - Secret (IDW-S) System Security Plan 20 December 2004 Version 1.4 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 b7E data by the following means: ACS update data is IntelPlus update data SAMNet update data VGTOF data

UNCLASSIFIED // FOR OFFICIAL USE ONLY

-29-

Outside the Scope

Open Source News data

The JICI library is static and is not updated

# UNCLASSIFIED // FOR OFFICIAL USE ONLY Investigative Data Warehouse - Secret (IDW-S) System Security Plan 20 December 2004 Version 1.4 3.5.1.1 IDW-S Core Subsystem Data Processed processing for each source.

Outside the Scope

Table 3.5.1.1 below outlines the IDW-S datasets and information about transfer and ingest

DATASETE NAME	EES SEES E DAUA SOURCES	<b>CEASSIDE ELION</b>
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below

b2 b7E

-43-

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

DATASET : SAME	DATA SOURCE	ŒLASSITICATION
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-

Table 3.5.1.1 IDW-S Data Sets b2

b7E

b2 b7E

-44-

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

#### 3.9.9 Indirect Connections

3.9.9.1 IDW-S Core Subsystem Indirect Connections

	Core Subsystem		
STEMNAME	FCLASSIPICATION	A ACONEDITED	TRANSFERS
	COMPARTMENTS	100	
FBI Automated	Secret	FBI	FTP
Case System			
(ACS)			
			FORD
FBI Intel Plus	Secret	FBI	FTP
	,		
	•		
FBI Secure	Secret	FBI	FTP
Automated			
Messaging			
Network (SAMNet)	]		
(Britistice)			
FBI National Crime	Unclassified/SBU	FBI	CD-ROM
Information			ļ
Center (NCIC)			
FBI Document	Secret	FBI	CD/DVD
Conversion Laboratory			
(DocLab),			
Records			
Management			1
Division (RMD), FBIHQ			
Thirty			
		1	
	<del></del>	·	<del></del>

Outside the Scope

b2 b7E

-51-

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

Version 1.4

Outside the Scope

b2 b7E

-52-

# 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

2.3.1 IDW	-S Operational Subsys	<u>stem</u>		Outside the
The table be	ow lists the data and so	ources for the Opera	ional Subsystem.	
The table be	low lists the data and so	ources for the Opera	ional Subsystem.	
The table be	ow lists the data and so	ources for the Opera	ional Subsystem.	
The table be	ow lists the data and so	ources for the Opera	ional Subsystem.	
The table be	·		cional Subsystem.	

DATTASEST NAME	DATA SOURCE	<u>GLASSIFICATION</u>
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
IICI	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.

UNCLASSIFIED//FOR OFFICIAL USE ON	LY
,	
3.2 Special Projects Team (SPT) Subsystem	Outside the Scope
he table below lists the data and sources for the SPT Subsystem.	
	•

DATASET		
DAGE	DATA SOURCE	GLASSIFICATION
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

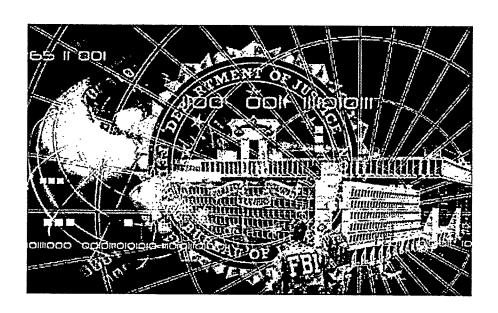
#### SPT Data Sets

		ļ
		!

Outside the Scope

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

	Investigative Data Warehouse - Secret (IDW-S) System Security Plan
	25 January 2005
	Version 1.6
İ	
Automate	d Transfer of Raw Data to IDW-S
Raw data is autom	natically transferred to the IDW-S system from approved data sources in
accordance with a	n Interconnection Agreement, Memorandum of Understanding, Memorandum
of Agreement or I	nterface Control Document. IDW-S V1 receives update data by the following
	ACS update data is transmitted to the IDW-S system
	ACS update data is transmitted to the ID w-5 system
•	IntelPlus update data is transmitted to the IDW-S system
_	CANDI-Auralia da da da da da MONIG
• 1	SAMNet update data is transmitted to the IDW-S system
•	VGTOF data is transmitted to the IDW-S system  Onen Source News data is transmitted to the IDW S
•	open source news data is transmitted to the in w-5 system by the bare
	The JICI library is static and is not updated on IDW-S V1.
	-23-
	-23-
	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

(VGTOF)	nto individual seria Open Source New	ioj, modsagos (o	HVII (OL), OI II	103
			Oi	atside the S
		•		

				25 Ja	ecurity Plan anuary 2005 Version 1.6	
		W	**************************************			
		•				
.5.1 Data	a Processed					
					0 : 11	
.5.1.1 IDV	W-S Core Subsyste	em Data Processed			Outside	the S
Table 3.5.1.1	l below outlines the	em Data Processed e IDW-S datasets and	l information abou	t transfer and ir		the S
Table 3.5.1.1 processing for DATESET	l below outlines the or each source.	e IDW-S datasets and	information abou	t transfer and in		the S
Table 3.5.1.1 processing for	l below outlines the		l information abou	t transfer and in		the S
Table 3.5.1.1 processing for DATEASET NAME	DATASOURCE  FBI Automated	e IDW-S datasets and	l information abou	t transfer and in		b2
Cable 3.5.1.1  DATASET  NAME  ACS  Electronic  Case Files	below outlines the or each source.  DATASOURCE	e IDW-S datasets and	information abou	t transfer and in		b2
Table 3.5.1.1 processing for DATASET NAME  ACS Electronic	DATEASOURCE  FBI Automated Case System	e IDW-S datasets and	information abou	t transfer and in		b2
Cable 3.5.1.1  DATASET  NAME  ACS  Electronic  Case Files	DATEASOURCE  FBI Automated Case System	e IDW-S datasets and	l information abou	t transfer and in		b2
DATEST  ACS Electronic Case Files	DATEASOURCE  FBI Automated Case System	e IDW-S datasets and	information abou	t transfer and in		b2
Cable 3.5.1.1  DATASET  NAME  ACS  Electronic  Case Files	DATEASOURCE  FBI Automated Case System	e IDW-S datasets and	information abou	t transfer and in		b2
Cable 3.5.1.1  DATASET  NAME  ACS  Electronic  Case Files	DATEASOURCE  FBI Automated Case System	e IDW-S datasets and	information abou	t transfer and in		b2

Investigative Data Warehouse - Secret (IDW-S) System Security Plan 25 January 2005 Version 1.6

DATASET		
NAME	DATIA 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
лсі	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 -38-

Outside the Scope

UNCLASSIFIED // FOR OFFICIAL USE ONLY

b2 b7E

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
25 January 2005
Version 1.6

#### 3.9.9 Indirect Connections

#### 3.9.9.1 IDW-S Core Subsystem Indirect Connections

	Core oursystem		
SYSUEM NAME	CLASSIFICATION & COMPARIMENTS	ACCREDITED BY	TRANSPER METEOD
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

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
25 January 2005
Version 1.6

SYSTEM NAME	COMPARIMENTS	ACCREDITED BY	URANSFER MEUROD	
MiTAP – Open Source News	Unclassified	NA	CD-ROM	b2 b7E
				· ]

Outside the Scope

-46-

#### INVESTIGATIVE DATA WAREHOUSE

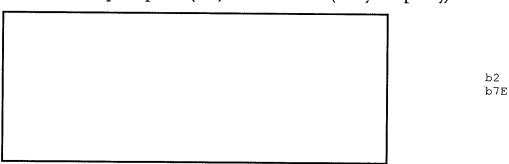
# User Reference for IDW Version 1.1 Applications

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).



- 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. ORGON:** 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 17 October 2003 Version 0.2

# 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
DW-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-

Investigative Data Warehouse (IDW) - Secret System Security Plan 17 October 2003 Version 0.2

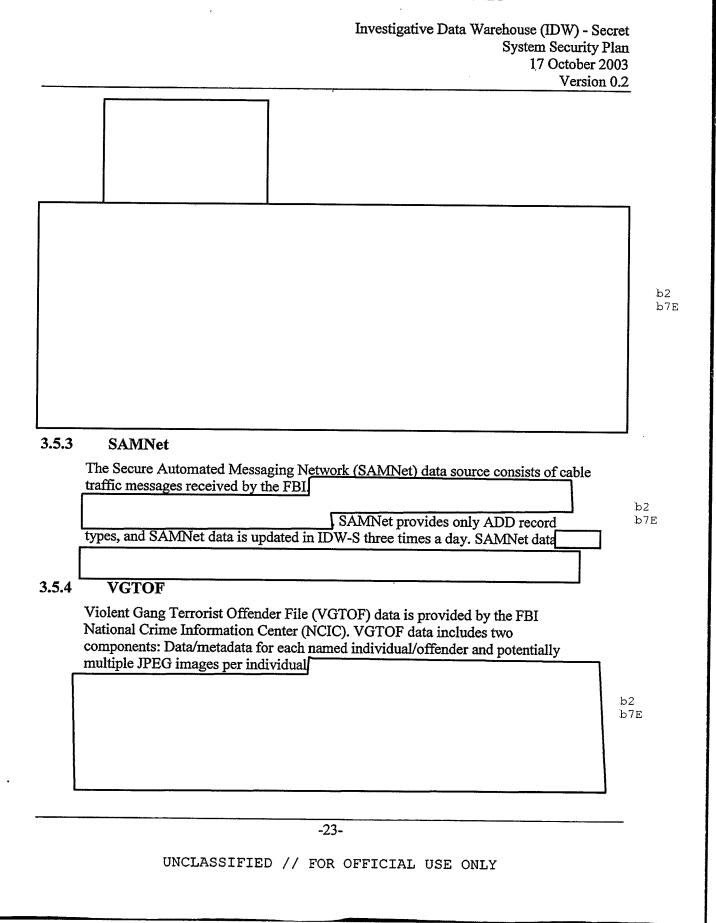
- Secure Automated Messaging Network (SAMNet) message traffic;
- IntelPlus File Rooms; and
- Violent Gang and Terrorist Organization File (VGTOF") from the Criminal Justice Information Systems (CJIS) Division;
- Defense Advanced Research Projects Agency (DARPA) Translingual Information Detection, Extraction and Summarization (TIDES) Open Source Data

Outside the Scope

Investigative Data Warehouse (IDW) - Secret System Security Plan 17 October 2003 Version 0.2

Data Source:	S Outside	the S	Scope
DW-S contain brackets:	ins data from the following data sources with security classification indicated		
•	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]		
ata Ingest			
OW-S receiv	res data from sources (ACS ECF, IntelPlus, SAMNet)		
nq	(VGTOF, Open Source News).		b2 b7E
• [ • [	(VGTOF, Open Source News).		
• [	- Received data into individual serial records (in the case of ACS ECF), documents (IntelPlus, JICI, Open Source News), messages (SAMNet), or files (VGTOF).		
• [	- Received data into individual serial records (in the case of ACS ECF), documents (IntelPlus, JICI, Open Source News), messages		
• [	- Received data into individual serial records (in the case of ACS ECF), documents (IntelPlus, JICI, Open Source News), messages		
• [	- Received data into individual serial records (in the case of ACS ECF), documents (IntelPlus, JICI, Open Source News), messages		

Investigative Data Warehouse (ID		
	ecurity Pl	
	October 200 Version 0	
	v cision o	<u>'.2</u>
3.5. DATA PROCESSED		
DW-S processes the following data:	utside tl	ne Scop
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 inclus	.•	
in IDW. For each such serial, the ECF data includes metadata and text. IDW-S	ion is	
synchronized against the ECF system once a day, a process which consists of	10	
receiving and processing the previous day's increment of ADD, MOD, and		
DELETE records		
	ĵ.	
		b2
.5.2 IntelPlus		b7E
IDW-S currently contains several IntelPlus counter-terrorism (CT) Filerooms:		
The Country Country (C1) I herooms.		
•		
		_
-22-		
UNCLASSIFIED // FOR OFFICIAL USE ONLY		



Investigative Data Warehouse (IDW) - Secret System Security Plan 17 October 2003 Version 0.2

3.5.5 ЛСІ
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
is not updated.  ICI is a static collection that
is not appared.
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/
All A frice come 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/

Investigative Data Warehouse (IDW) - Secret System Security Plan 17 October 2003 Version 0.2

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

DATIASET TRANSFER NAME DATA SOURCE METHOD COMMENTS					 
Separation (Separation)	DATACET		18:2/48/25/25/25		
NAME DATA SOURCE METHOD COMMENTS	the contract of the contract o			1	
	MANAGE	DATA CAMERTE	METHOD	COMMENTE	 1
ALEXE   CHARLES   CAMPILLANDS					

Investigative Data Warehouse (IDW) - Secret System Security Plan 17 October 2003 Version 0.2

DATASET	Charles Grandwith	TRANSFER
NAME	DATA SOURCE	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
лсі	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

Outside

-26-

Investigative Data Warehouse – Secret (IDW-S)
System Security Plan
11 June 2004
Version 1.3

### **Attachment L**

 	**	 	 		
			i		
			 O	_1_	<b>G</b>
			Outside	tne	Scope

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED DATE 05-20-2008 BY 65179/DMH/HKG/VTA

Investigative Data Warehouse – Secret (IDW-S)
System Security Plan
11 June 2004
Version 1.3

4.1.1 Data Ingest Common Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.2       ACS Files         4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.3       SAMNet Files         4.1.4       IntelPlus Files         4.1.5       JICI Files         4.1.6       MiTAP Files         4.1.7       VGTOF Files	
4.1.4       IntelPlus Files.         4.1.5       JICI Files.         4.1.6       MiTAP Files.         4.1.7       VGTOF Files.	
4.1.5 JICI Files	
4.1.6 MiTAP Files	
4.1.7 VGTOF Files	
•	

Outside the Scope

Investigative Data Warehouse – Secret (IDW-S)
System Security Plan
11 June 2004
Version 1.3

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.

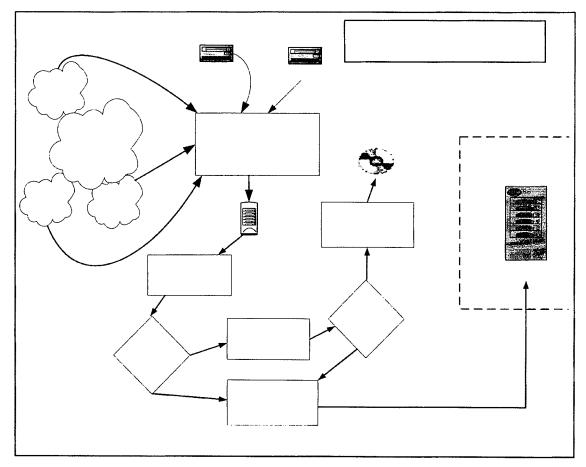
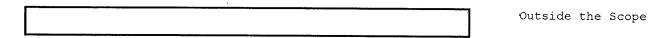


Figure 4.1.1 IDW-S Data Ingest Dataflow



Investigative Data Warehouse – Secret (IDW-S)
System Security Plan
11 June 2004
Version 1.3

		Outside	the S	Scop
Da	ta ingest processing on IDW-S includes the following:			
•	ACS Processing: The ACS data is a subset of the Electronic Case File (ECF) subsy	/stem.		
		}		b2 b7E
	provides ADD, MOD, and DELETE record types.	ACS		
•	IntelPlus Processing: The IntelPlus data includes of the following CT file rooms:			
	_			
	-			
		<del></del>	b2 b7	

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Page 109

Investigative Data Warehouse – Secret (IDW-S)
System Security Plan
11 June 2004
Version 1.3

•	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.  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	b2 b7E
	files. The records for each individual are combined into a document.  VGTOF data is provided in entirety, replacing	
	the previous data	the Scope

Version 1.2

PUG NG-OM-0061.12

### Federal Bureau of Investigation Information Resources Division Data Management Section



Investigative Data Warehouse Privileged Users Guide Version 1.2

ALL INFORMATION CONTAINED December 1, 2004 HEREIN IS UNCLASSIFIED DATE 05-20-2008 BY 67159/DMH/HKG/VTA

Privileged Users Guide (PUG)	IDW Operational Services	
Version 1.2	PUG NG-OM-0061.12	
		Outside the Scop
4.1 Operations		
TI IDW 4 1 1 1 1 1 4 down out out to		

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:

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 12

Version 1.2

DATASOURCE.	CLASSIFIC TION	DATA TRANSFER MECHANISM TO IDV S.
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

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

PUG NG-0M-0061.12

FOR OFFICIAL USE ONLY

Page 13

Privileged Users Guide (PUG)	IDW Operational Services	
Version 1.2	PUG NG-OM-0061.12	7
	.•	
·		
		Outside the Scope
The SPT-specific data sources will include:  Financial Center (FinCen		
Norly     Selectee	_	.b2
•		Ъ7Е
<ul> <li>Unified Name Index (UNI) extracts</li> </ul>		

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

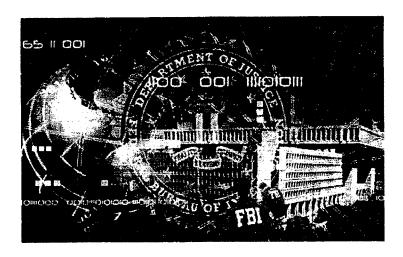
PUG NG-OM-0061.12

FOR OFFICIAL USE ONLY

Page 16

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
24 January 2005
Version 1.5

# 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

UNCLASSIFIED // FOR OFFICIAL USE ONLY

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED DATE 05-20-2008 BY 67159/DMH/HKG/VTA

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
24 January 2005
Version 1.5

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 FB1 projects/programs:

PROJECT NAME	CLASSIFICATION/ COMPARIMENTS	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-

# UNCLASSIFIED // FOR OFFICIAL USE ONLY Investigative Data Warehouse - Secret (IDW-S) System Security Plan 24 January 2005 Version 1.5 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

-29-

UNCLASSIFIED // FOR OFFICIAL USE ONLY
Investigative Data Warehouse - Secret (IDW-S) System Security Plan
24 January 2005
Version 1.5

Initial processing of raw data file	
data into individual serial records (i	n the case of ACS ECF),
documents (IntelPlus, JICI, Open Source News), message	es (SAMNet), or files
(VGTOF)	.b2
	b7E
	.576
	·
•	
	Outside the Scope
	•

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
24 January 2005
Version 1.5

	Outside the Same
	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	DATA SOURCE	CLASSIFICATION	DATA TRANSFER MECHANISM TO 18W 8
ACS Electronic Case Files (ECF)	FBI Automated Case System (ACS)	Secret and below	·
(-51)			

b2 b7E

-43-

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
24 January 2005
Version 1.5

DATASET NAME	DATASOURCE	CLASSIFICATION	DATA TRANSFER MECHANISM TO TOWS	
IntelPlus Filerooms	FBI IntelPlus	Secret and below		
SAMNet	FBI Secure Automated Messaging Network (SAMNet)	Secret and below		b2 b7E
VGTOF	FBI National Crime Information Center (NCIC)	 SBÚ		
JICI	FBI Records Management Division (RMD), Document Laboratory (DocLab), FBIHQ	Secret and below		
Open Source News	MiTAP	Unclassified		
		Table 3.5.1.1 IDW-5	Data Sets	_
				Outside the Sco
				Outside the Scop

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
24 January 2005
Version 1.5

### 3.9.9 Indirect Connections

### 3.9.9.1 IDW-S Core Subsystem Indirect Connections

	o Core oubsystem		
SYSTEM NAME	CPASSIFICATION  COMPARIMENTS	A) CREDII BY	ED TRANSFER MLTIOD
FBI Automated Case System (ACS)	Secret	FBI	FTP
FBI Intel Plus	Secret	FBI	FTP
FBI Secure Automated Mcssaging 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

-51-

Investigative Data Warehouse - Secret (IDW-S)
System Security Plan
24 January 2005
Version 1.5

SYSTEM NAME	PCLASSIFICATION & 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 & COMPARIMENTS:	ACCREDITED BY	TRANSFER METHOD	COMMENTS
FBI Investigative Data Warehouse - Secret (IDW-S)	Sccret	FBI	CD-ROM & FTP	

-52-

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.

- 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.

b2 b7Е