Style Definition: Body Text

System Security Plan

Investigative Data Warehouse-SECRET (IDW-S)

3 DECEMBER 2003

Version: 0.6

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

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").

Outside the Scope

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

- Approved case files from the FBI's Automated Case Support (ACS) case management system;
- Electronic versions of the Joint Intelligence Committee Investigation (JICI) defined archived documents;

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

[redacted]

Outside the Scope

Data Sources

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

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

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

Data Ingest

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

Deleted: SAMNet

- Data is received by the Ingest Subsystem
- [redacted]
  - Received data is parsed into individual serial records (in the case of ACS ECF), documents (IntelPlus, JICI, Open Source News), messages (SAMNet), or files (VGTOF).
- [redacted]

Outside the Scope

[redacted]

Outside the Scope

3.5. Data Processed

IDW-S processes the following data:

3.5.1 ACS ECF

IDW-S contains a subset of the ECF (Electronic Case File) subsystem of the Automated Case System (ACS). This subset consists of serials in those case classifications/sub classifications that have been officially sanctioned for inclusion in IDW. 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. [redacted]

Outside the Scope

3.5.2 IntelPlus

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

- [redacted]
-

b2
b7E

- [redacted]

b2
b7E

[redacted]

b2
b7E

3.5.3 SAMNet

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

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. [redacted]

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 [redacted] JICI is a static collection that is not updated. [redacted]

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) and [redacted] The Open Source News data goes into IDW-S once a day. Open Source News data [redacted]

b2
b7E

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/

Deleted: Internation

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

3.5.7 Summary of Data Sources

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

b2
b7E

[redacted]

3.9.9 Indirect Connections

Outside the Scope

IDW-S connects to the following sources of data:

				[redacted]
FBI Automated Case System (ACS)	Secret	FBI	FTP	[redacted]
FBI Intel Plus	Secret	FBI	FTP	

b2
b7E

FBI Secure Automated Messaging Network (SAMNet)	Secret	FBI	FTP	[redacted]
FBI National Crime Information Center (NCIC)	Unclassified/SBU	FBI	CD-ROM	[redacted]
FBI Document Conversion Laboratory (DocLab), Records Management Division (RMD), FBIHQ	Secret	FBI	Multiple	[redacted]
Translingual Information Detection Extraction and Summarization (TIDES) Program, Defense Advanced Research Projects Agency (DARPA)	Unclassified	NA	CD-ROM	[redacted]

b2
b7E

[redacted]	Unclassified	NA	[redacted]	[redacted]

b2
b7E

Indirect Connections

Formatted: Font: Not Italic

Formatted: Centered