



MARCIA HOFMANN ESQ  
ELECTRONIC FRONTIER FOUNDATION  
454 SHOTWELL STREET  
SAN FRANCISCO, CA 94110

April 8, 2008

Subject: INVESTIGATIVE DATA WAREHOUSE

FOIPA No. 1058805- 000

Dear Ms. Hofmann:

The enclosed documents were reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a. Deletions have been made to protect information which is exempt from disclosure, with the appropriate exemptions noted on the page next to the excision. In addition, a deleted page information sheet was inserted in the file to indicate where pages were withheld entirely. The exemptions used to withhold information are marked below and explained on the enclosed Form OPCA-16a:

**Section 552**

**Section 552a**

- |  |   |                                 |
|--|---|---------------------------------|
| <input type="checkbox"/> (b)(1)            | <input type="checkbox"/> (b)(7)(A)            | <input type="checkbox"/> (d)(5) |
| <input checked="" type="checkbox"/> (b)(2) | <input type="checkbox"/> (b)(7)(B)            | <input type="checkbox"/> (j)(2) |
| <input type="checkbox"/> (b)(3) _____      | <input checked="" type="checkbox"/> (b)(7)(C) | <input type="checkbox"/> (k)(1) |
| _____                                      | <input type="checkbox"/> (b)(7)(D)            | <input type="checkbox"/> (k)(2) |
| _____                                      | <input checked="" type="checkbox"/> (b)(7)(E) | <input type="checkbox"/> (k)(3) |
| _____                                      | <input type="checkbox"/> (b)(7)(F)            | <input type="checkbox"/> (k)(4) |
| <input type="checkbox"/> (b)(4)            | <input type="checkbox"/> (b)(8)               | <input type="checkbox"/> (k)(5) |
| <input checked="" type="checkbox"/> (b)(5) | <input type="checkbox"/> (b)(9)               | <input type="checkbox"/> (k)(6) |
| <input checked="" type="checkbox"/> (b)(6) |   | <input type="checkbox"/> (k)(7) |

184 page(s) were reviewed and 173 page(s) are being released.

- Document(s) were located which originated with, or contained information concerning other Government agency(ies) [OGA]. This information has been:
  - referred to the OGA for review and direct response to you.
  - referred to the OGA for consultation. The FBI will correspond with you regarding this information when the consultation is finished.

You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information and Privacy, U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001 within sixty days from the date of this letter. The envelope and the letter should be clearly marked "Freedom of Information Appeal" or "Information Appeal." Please cite the FOIPA number assigned to your request so that it may be easily identified.

The enclosed material is from the main investigative file(s) in which the subject(s) of your request was the focus of the investigation. Our search located additional references, in files relating to other individuals, or matters, which may or may not be about your subject(s). Our experience has shown, when ident, references usually contain information similar to the information processed in the main file(s). Because of our significant backlog, we have given priority to processing only the main investigative file(s).

If you want the references, you must submit a separate request for them in writing, and they will be reviewed at a later date, as time and resources permit.

See additional information which follows.

Sincerely yours,



David M. Hardy  
Section Chief  
Record/Information  
Dissemination Section  
Records Management Division

Enclosure(s)

The enclosed documents represent the fourth of a series of interim releases that will be made with regard to your request pertaining to the Investigative Data Warehouse.

For your information, some of the enclosed pages contain information about other subject matters. We consider this information "outside the scope" of your request, and have redacted the information and marked it as "Outside the Scope".

The first page of this correspondence reflects that 184 pages were reviewed for this release. There were actually 1076 pages reviewed, however a further review determined that 888 pages of this material are not responsive to this request.

## EXPLANATION OF EXEMPTIONS

### SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information ( A ) could be reasonably be expected to interfere with enforcement proceedings, ( B ) would deprive a person of a right to a fair trial or an impartial adjudication, ( C ) could be reasonably expected to constitute an unwarranted invasion of personal privacy, ( D ) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, ( E ) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or ( F ) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

### SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

FINAL

FOR OFFICIAL USE ONLY

---

**FEDERAL BUREAU OF INVESTIGATION**  
***PROJECT MANAGEMENT OFFICE***

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 08-01-2007 BY 65179 DMH/BJA/CAL

1058805



**SYSTEM**

**CONCEPT OF OPERATIONS (CONOPS)**

**INVESTIGATIVE DATA WAREHOUSE (IDW)**

---

FOR OFFICIAL USE ONLY

26 March 2004  
Version 3

**EXECUTIVE SUMMARY**

The Investigative Data Warehouse (IDW) provides FBI users with the capability to view, query, search, retrieve, correlate, integrate, synthesize, share, and protect information from multiple data sources in support of intelligence and investigative activities. As a single point of entry for accessing both FBI data and non-FBI data, IDW provides FBI users with information needed to successfully accomplish the FBI's counter-crime, counter-intelligence, and counter-terrorism missions.

This Concept of Operations (CONOPS) documents IDW as an evolving family of systems that will provide near- and long-term operational and developmental capabilities to the FBI. When fully deployed, IDW will include four (4) systems:

- The IDW Secret-level operational system (IDW-S) consists of those builds which have undergone appropriate security and operational testing and have been approved by the responsible FBI authorities for operational use. IDW-S V1.0 received Interim Authority to Operate (IATO) on January 23, 2004 and began operations for approved users over FBI Net on January 25, 2004. IDW-S V2 is currently being developed.
- The IDW Integration system (IDW-I) is a Secret-level representation of IDW-S that serves as an environment in which maintenance fixes and proposed new capabilities can be realistically tested before being released into IDW-S.
- IDW-TS/SCI is a version of IDW-S that, when built, will be approved for data that is classified as Top Secret and/or Sensitive Compartmented Information (TS/SCI). It should be noted that because the IDW Program has given high priority to IDW-S, the IDW-TS/SCI system is currently in the definition stage.
- The IDW Development system (IDW-D) is an Unclassified prototyping environment used to facilitate experimentation with proposed new IDW technologies.

This initial IDW CONOPS is focused on IDW-S and IDW-I, the two IDW systems currently developed. As noted above, IDW-S operates under an IATO, whereas IDW-I will operate under an Interim Authority to Test (IATT). This is appropriate to the role of IDW-S as an operational system with a general user base and to the intended role of IDW-I as a test environment. This CONOPS identifies all major IDW system processes and internal and external interfaces. It provides an overview of the IDW-S conceptual design and a high-level description of IDW system requirements. This IDW CONOPS is intended to complement other IDW Program documentation, in particular the IDW Program Management Plan, the IDW-S System Security Plan, and the Target IDW/Virtual Case File (VCF) Business Architecture.

SECTION 3

DESCRIPTION OF THE IDW PROJECT

Pertinent details regarding the IDW project are:

**Project Name:** Investigative Data Warehouse (IDW)

**Account Identification Code:** 15-0200-0-1-999,

**Project Initiation Date:** March 2003,

**Project Planned Completion Date:** December 2006 (As the Master Data Warehouse<sup>1</sup>).

As a single point of entry for accessing investigative data sources, IDW provides FBI users with the capability to readily acquire, store, share, use, disseminate, and protect the information needed to successfully accomplish their assignments and the FBI's overlapping missions in intelligence, counter-terrorism, and criminal investigations.

The IDW system environment consists of a collection of UNIX and NT servers that provide secure access to a family of very large-scale storage devices. The servers provide application, web servers, relational database servers, and security filtering servers. User desktop units that have access to FBINet can access the IDW web application. This provides browser-based access to the central databases and their access control units. The environment is configured so that the FBI analytic and investigative users can access any of the data sources and analytic capabilities of the system for which they are authorized. The entire configuration is scalable to enable expansion as more data sources and capabilities are added.

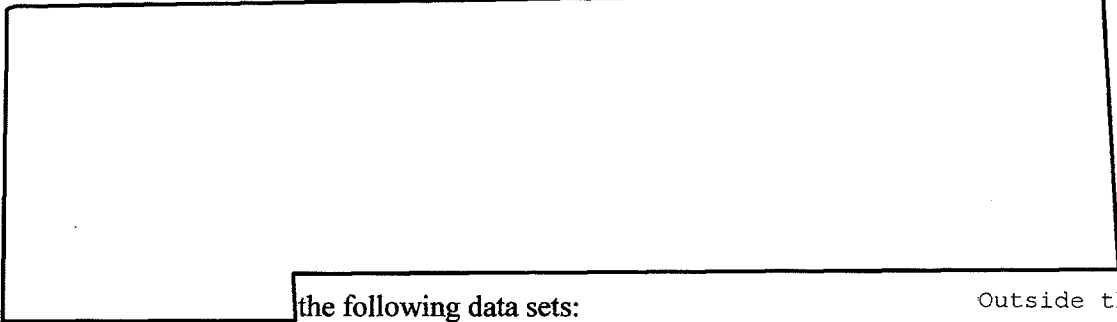
The FBI currently owns or has access to over 30 information technology systems and well over 100 enterprise level applications that support investigative functions. At the user level, the number of databases containing case-centric intelligence is estimated to be in the thousands, a number that has increased largely due to the lack of an enterprise-wide application for data analysis. The IDW project initiative will ultimately integrate many of the underlying system data sources into a single Investigative Data Warehouse that will support data mining and target searching of both FBI data and data from external sources. The project will also support the selective sharing of data with other Federal agencies as part of the Department of Homeland Security's (DHS) Horizontal Information Sharing Initiative and the Joint Terrorism Task Forces (JTTFs). The data warehouse capability will permit the abundance of this investigative data to be shared on an FBI-wide basis, providing a complete data picture to analysts and agents.

---

<sup>1</sup> The Master Data Warehouse is the next generation investigative warehouse which expands the analytical tool capabilities and includes administrative data sets so that the FBI can adequately evaluate return on investment in applying resources to investigative programs.

FINAL

FOR OFFICIAL USE ONLY



the following data sets:

Outside the Scope

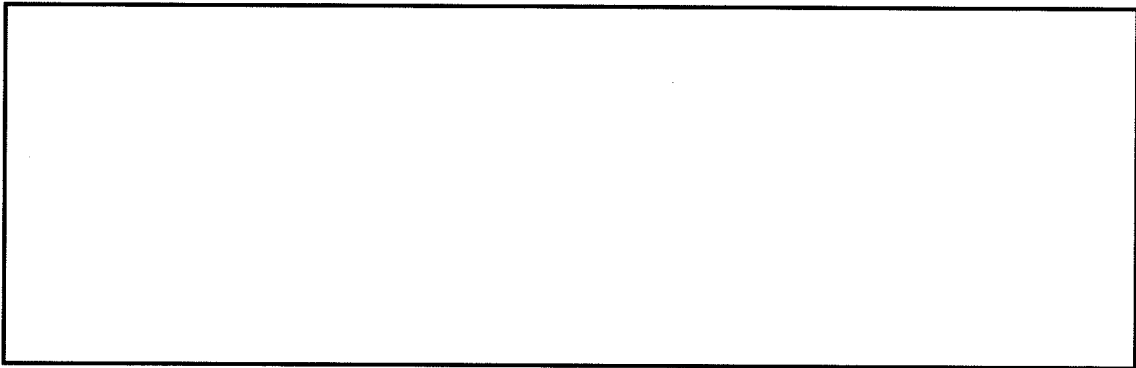
- Approved case files from the FBI's Automated Case Support (ACS) case management system,
- Electronic versions of the Joint Intelligence Committee Inquiry (JICI) archived documents,
- Secure Automated Messaging Network (SAMNet) message traffic;
- IntelPlus File Rooms (IDW V1.0 does not currently update this information),
- Violent Gang and Terrorist Organization File (VGTOF) data from the Criminal Justice Information Systems (CJIS) Division (IDW V1.0 does not currently update this information).



following additional databases and/or data sources:

- [Redacted] - Data provided from FINCEN system
- [Redacted]
- [Redacted]
- Virtual Case File (VCF)
- [Redacted]

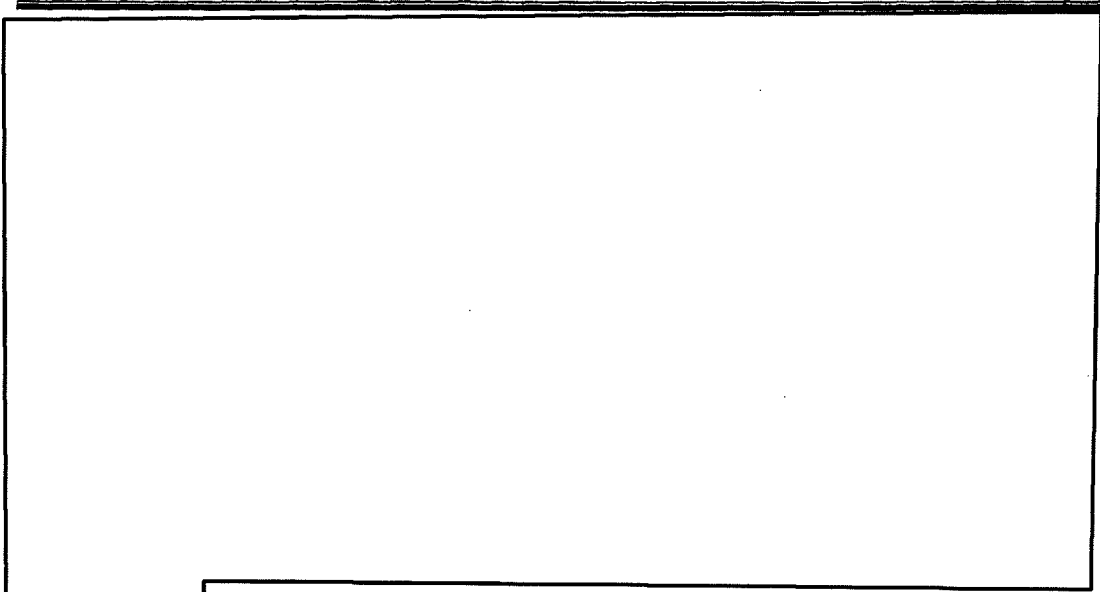
b2  
b7E



Outside the Scope

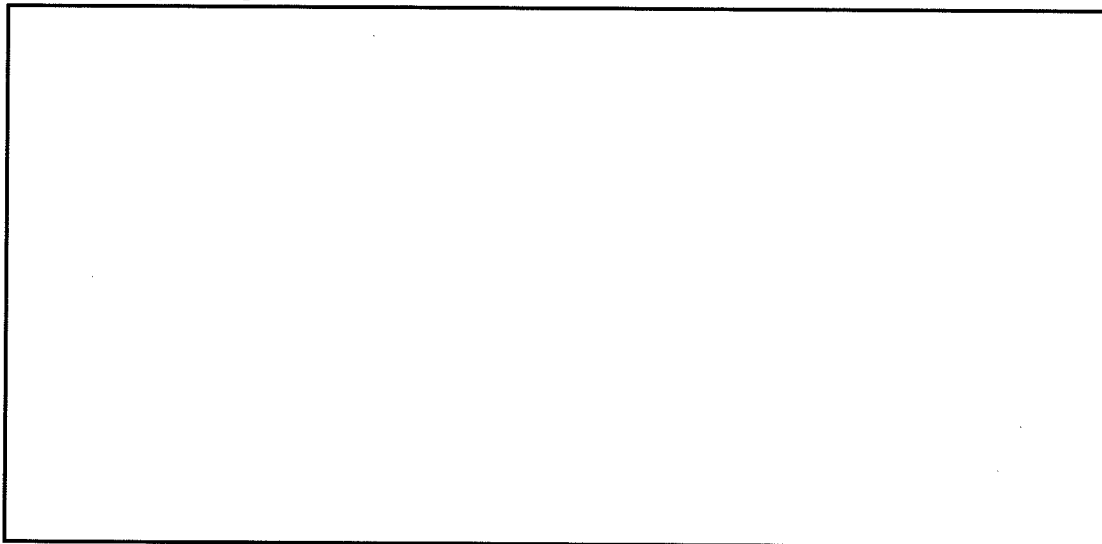
**FINAL**

**FOR OFFICIAL USE ONLY**



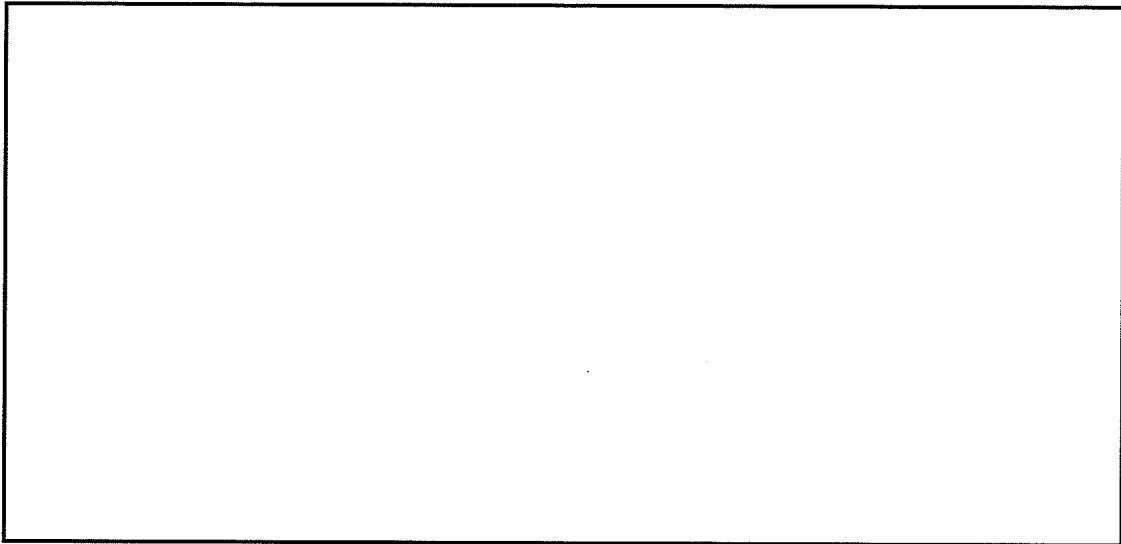
IDW-I data includes the same data sets present on IDW-S: Outside the Scope

- Approved case files from the FBI's ACS case management system,
- Electronic versions of the JICI defined archived documents,
- SAMNet message traffic;
- IntelPlus File Rooms,
- VGTOF data from the CJIS Division,
- Translingual Information Detection, Extraction and Summarization (TIDES) Program Open Source News Data

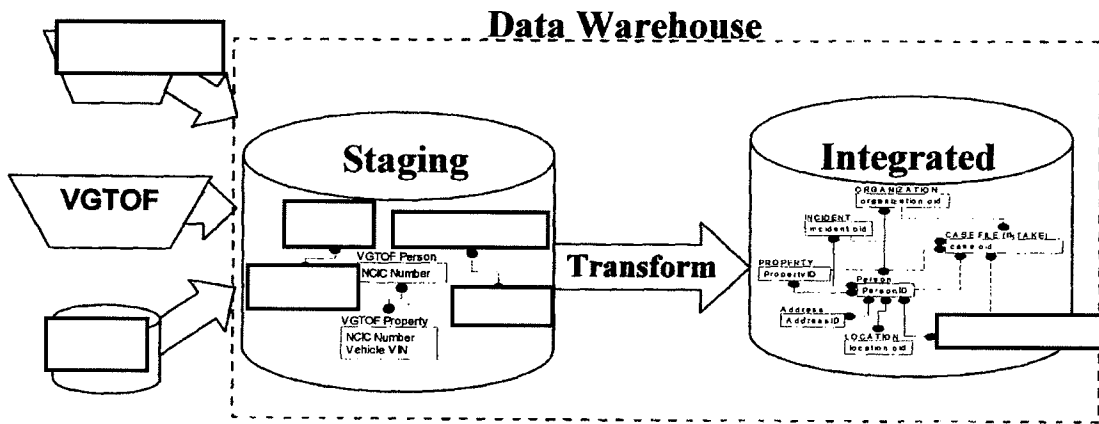


Outside the Scope





Outside the Scope



b2  
b7E

**Figure 5-2 Data Ingest Data Transformation Process**

The ingested data is transformed from a source structure to a staging structure to provide more efficient searches and database organization (see Figure 5-2). During the transformation process, the data obtained from multiple sources is integrated so that relationships between the several data elements of the original data source can be established. The new structure provides the basis for analysis by the BI tools. In addition to the transformation, the Data Ingest analyzes the data quality and will maintain this metric for manual use by the analysts and automated use by the analysis tools.



Outside the Scope

**FINAL**

**FOR OFFICIAL USE ONLY**

Outside the Scope

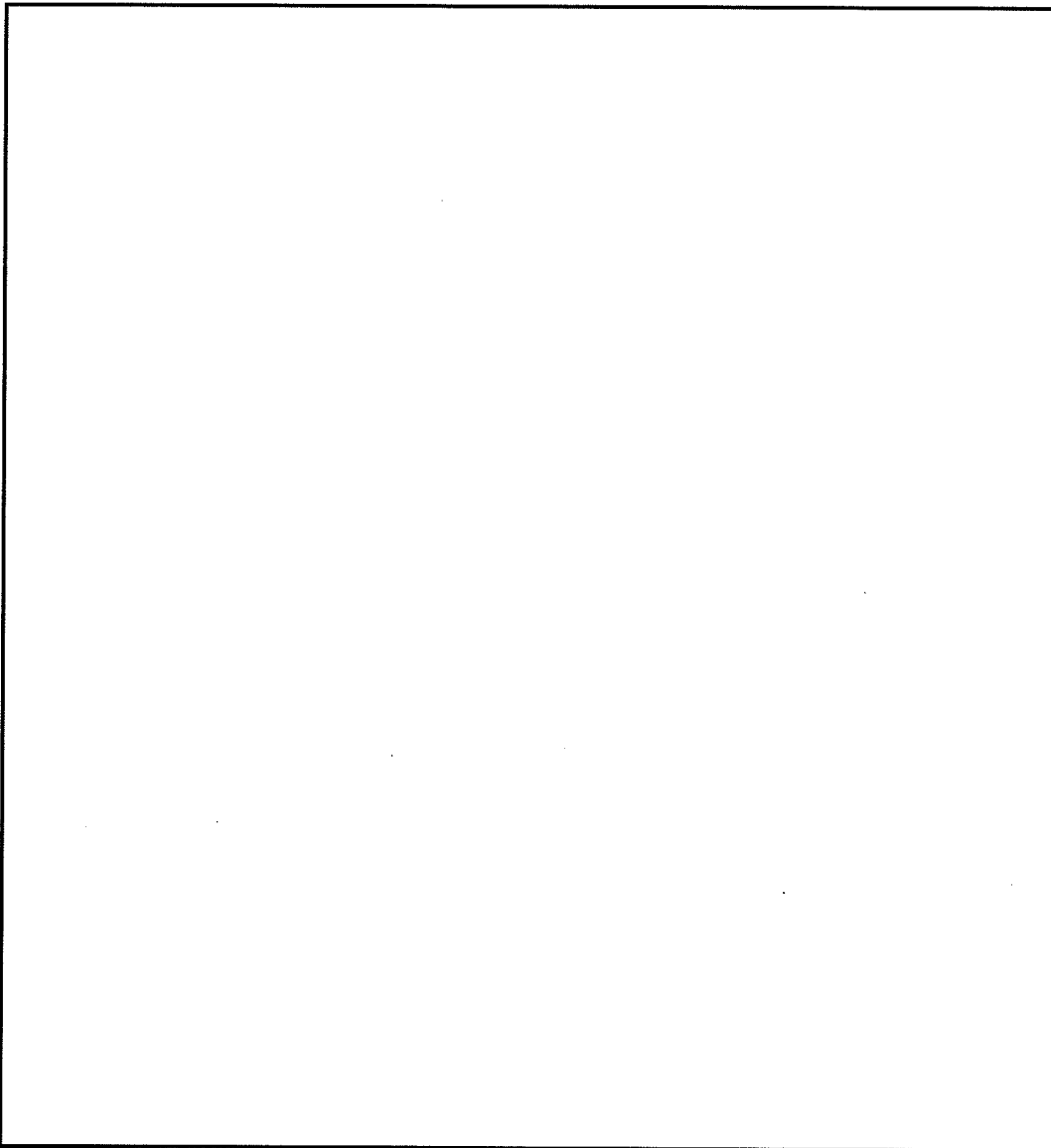


The SDMA component of the IDW-S system will process and manage all structured data by providing the following major processes:

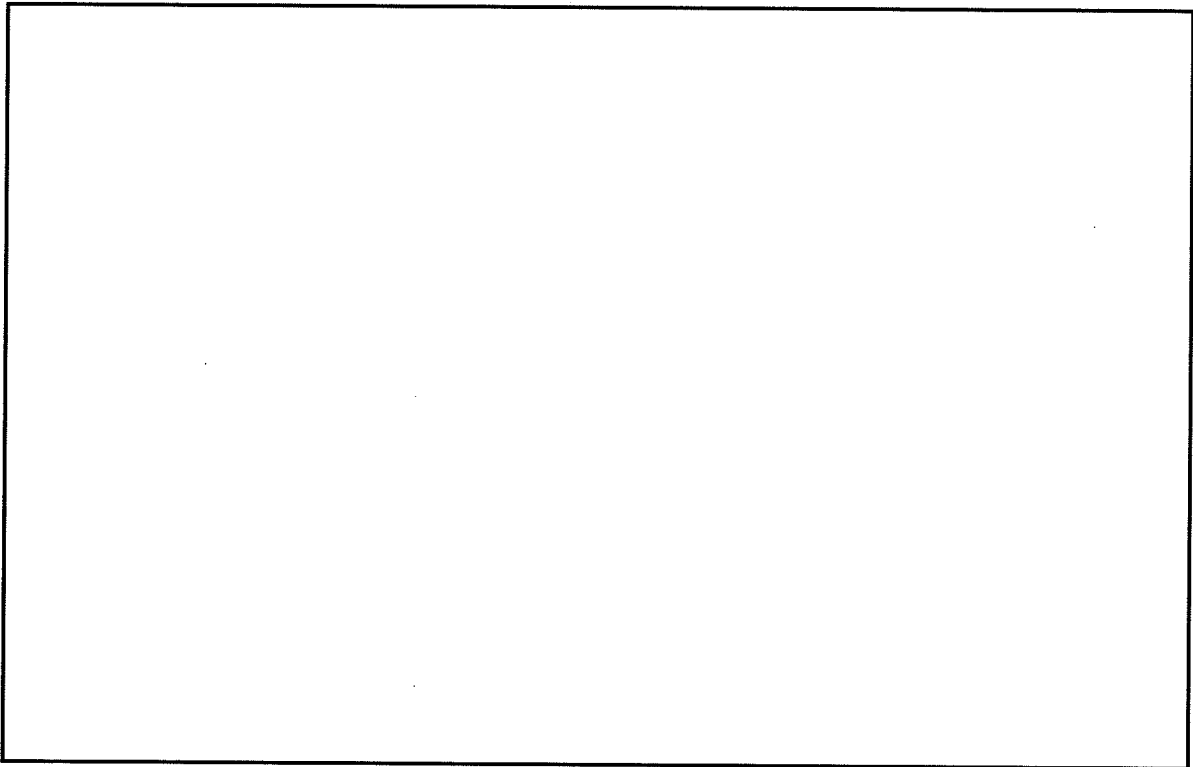
- Store and manage structured data from all external and legacy systems (IDW V2 will initially include VCF, VGTOF, [redacted] UNI, and [redacted] and other future data sources. This data will be provided to SDMA by Data Ingest.
- Store and manage unstructured data as part of the IDW Data Store.

b2  
b7E

Outside the Scope



**FOR OFFICIAL USE ONLY**

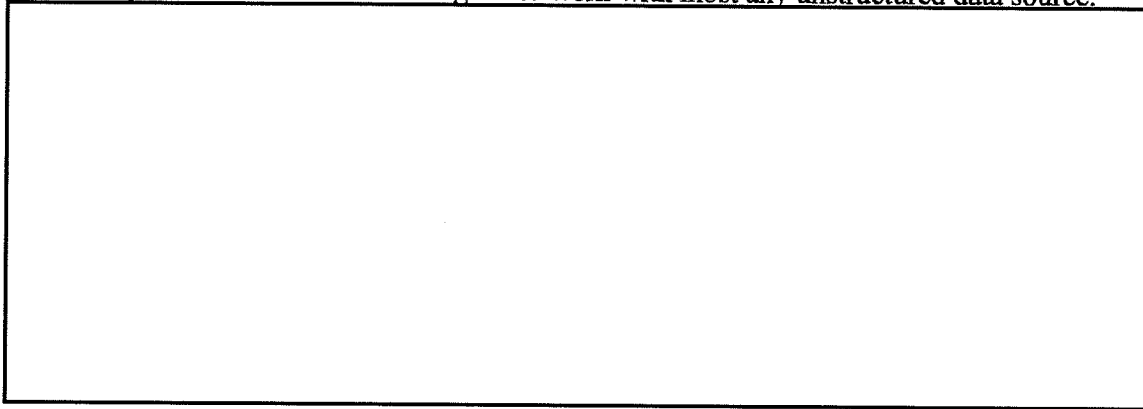


Outside the Scope

**6.3 Manage and Analyze Unstructured Data**

The unstructured data management and analysis subsystem (UDMA) provides functionality for storing, indexing, searching, and extracting information from unstructured information. This unstructured information is documented and associated with the document's metadata. The initial data sources for IDW UDMA are: ACS/VCF, INTEL+/JICI, SAMNET, and  data, however, except for some key metadata that are captured for these sources there is nothing unique about the unstructured data handled by this subsystem. UDMA will be designed to work with most any unstructured data source.

b2  
b7E

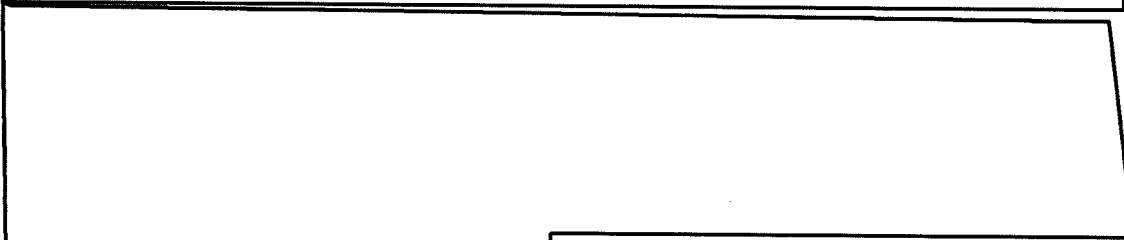
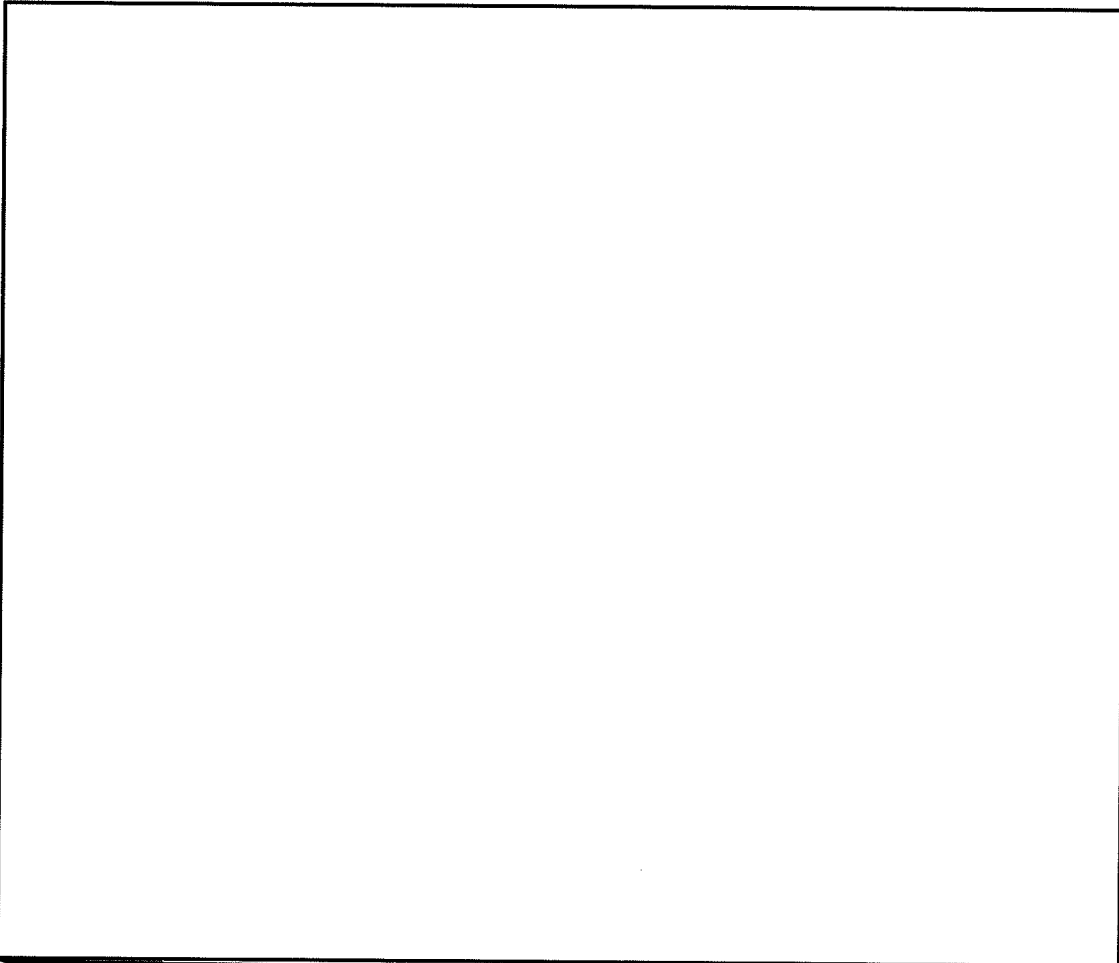


Outside the Scope

**FINAL**


**FOR OFFICIAL USE ONLY**

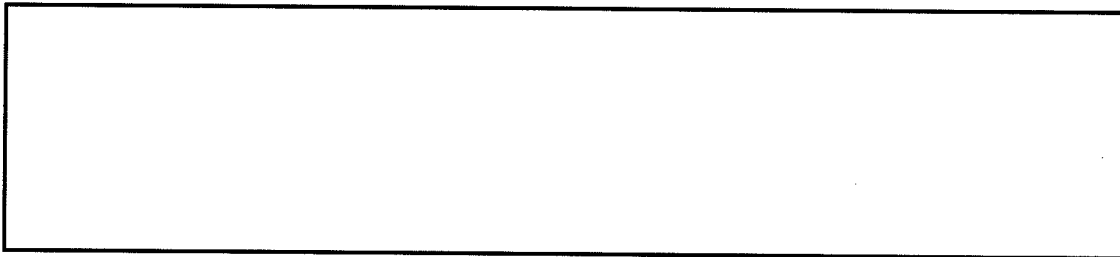
Outside the Scope



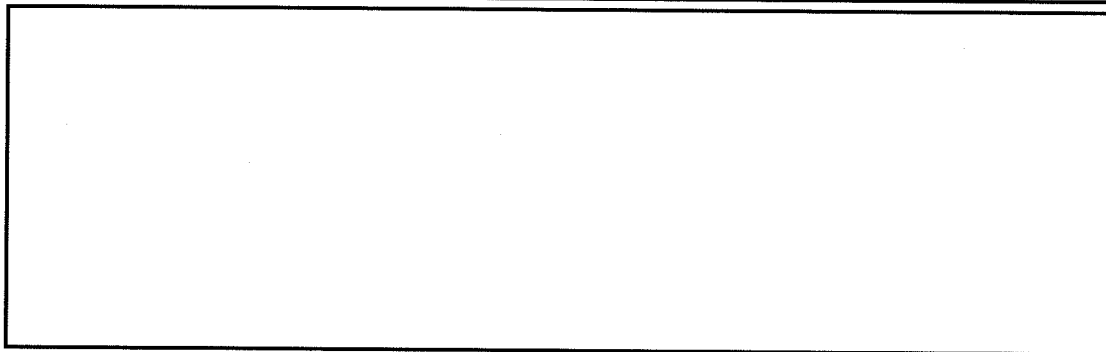
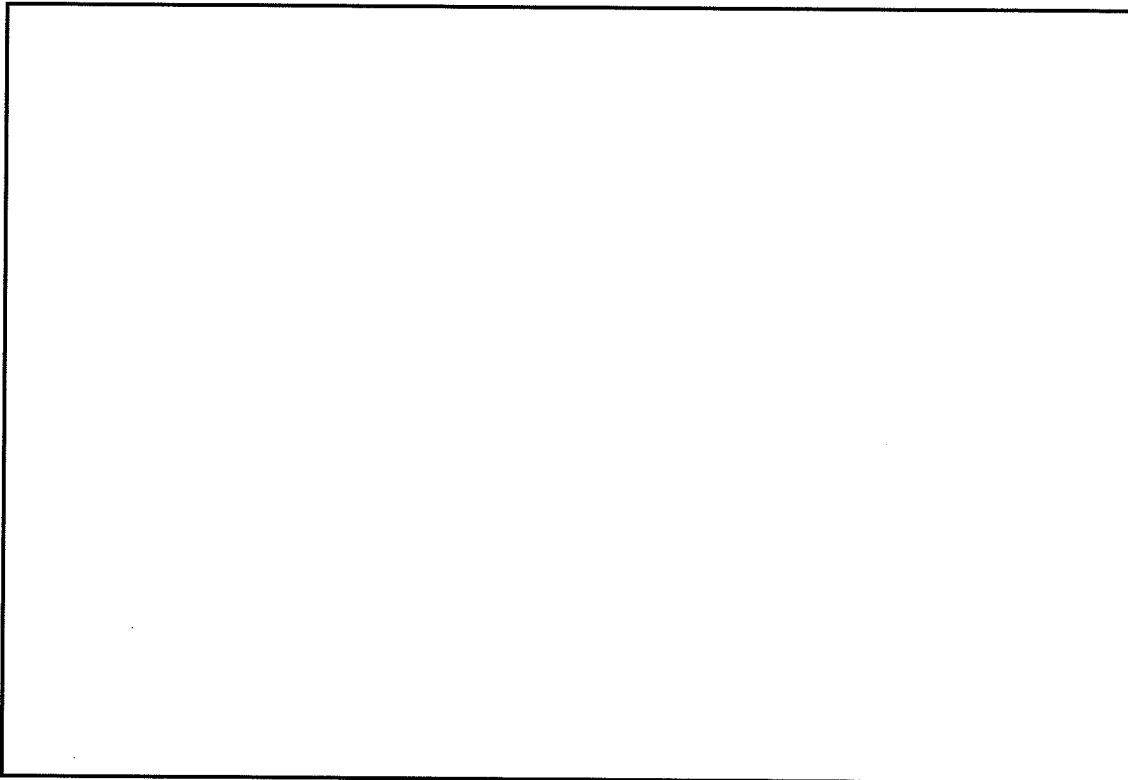
b2  
b7E

Data Ingest, including: VCF, SAMNET, Intel

Plus, JICI, and 



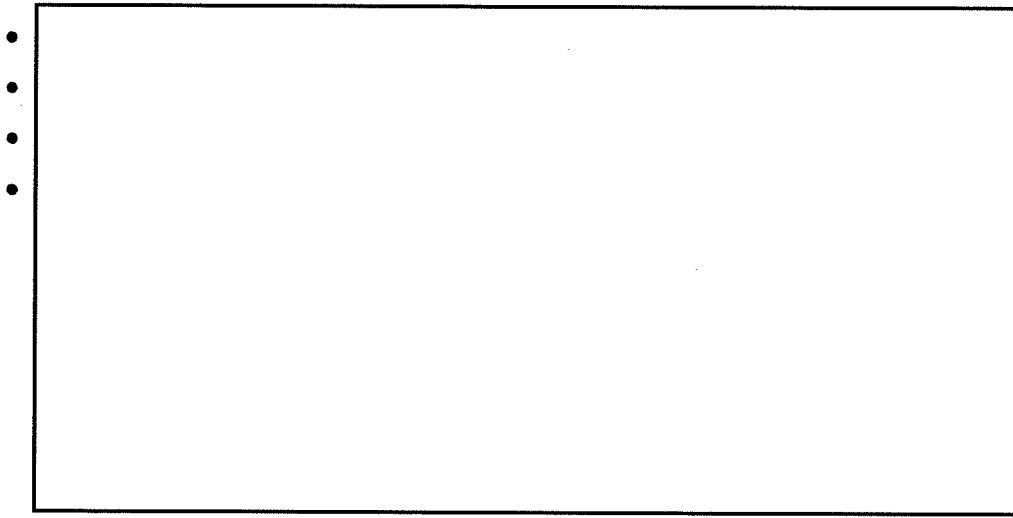
Outside the Scope



**6.10 Data Sources**

The IDW V2 system will provide one web-based interface to the user thereby allowing access to any of nine data sources with an access control system applying to all of the data sources in order to conduct global searching and analysis. These sources include four that are structured ( [redacted] VGTOF [redacted] and [redacted] ) and five that are unstructured ( VCF, Intel+, JICI, SAMNet [redacted] ). Versions of IDW beyond V2 will support the processing from additional data sources.

b2  
b7E

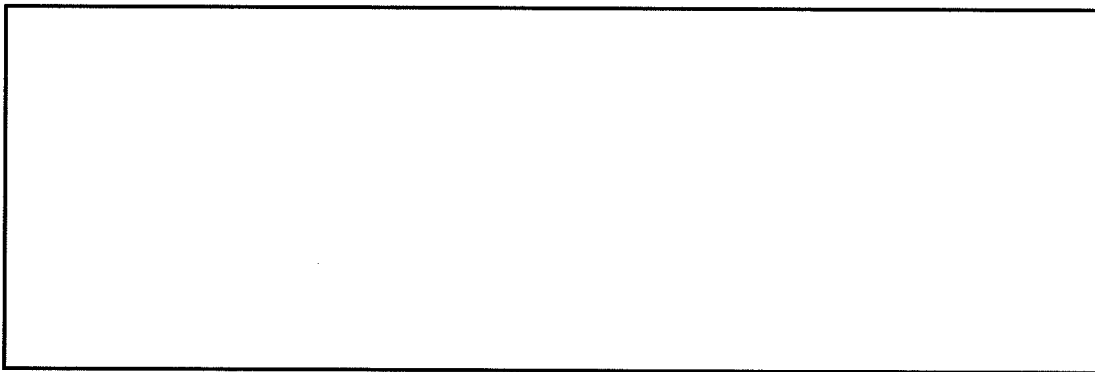


The users have requested that IDW system support searches of the following databases. Some of these are currently not funded:

- Legacy Systems
  - SAMNet-S
  - JICI
  - ACS or VCF (since VCF is planned to replace ACS)
  - VGTOF
  - [Redacted]
  - [Redacted]
  - [Redacted]
  - IntelPlus
  - FINCEN - [Redacted]

b2  
b7E

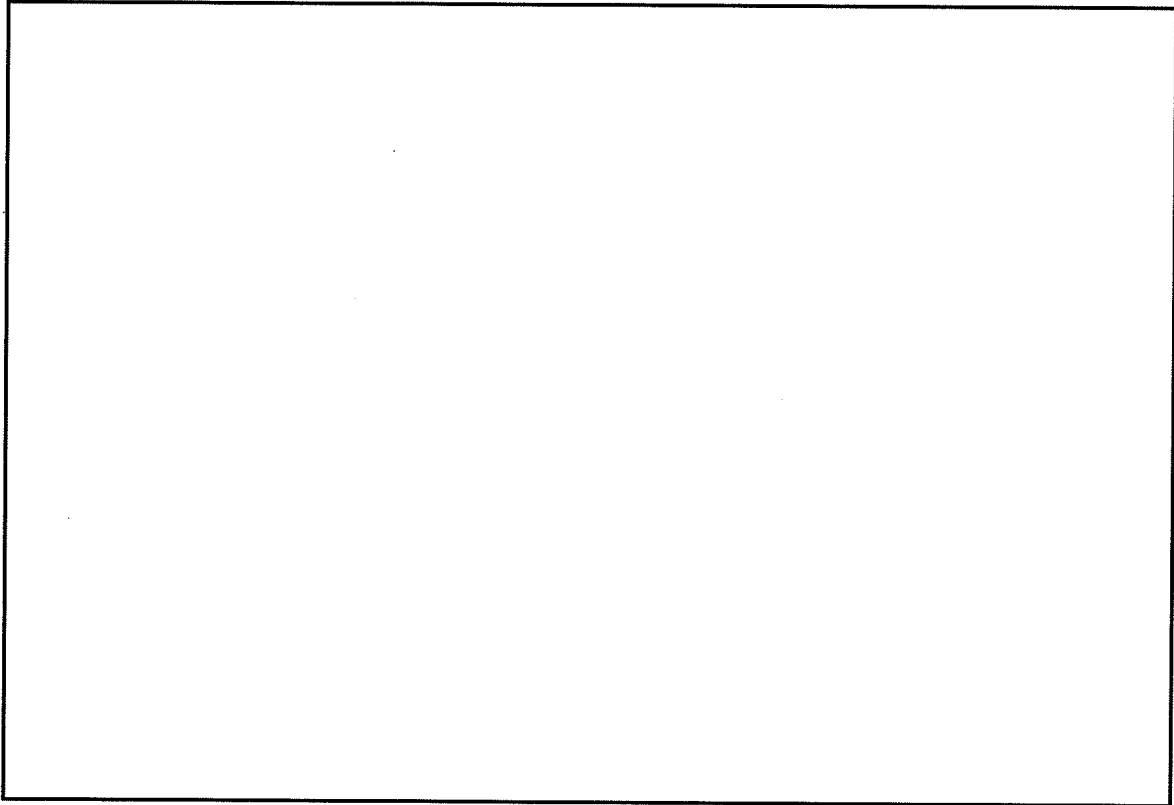
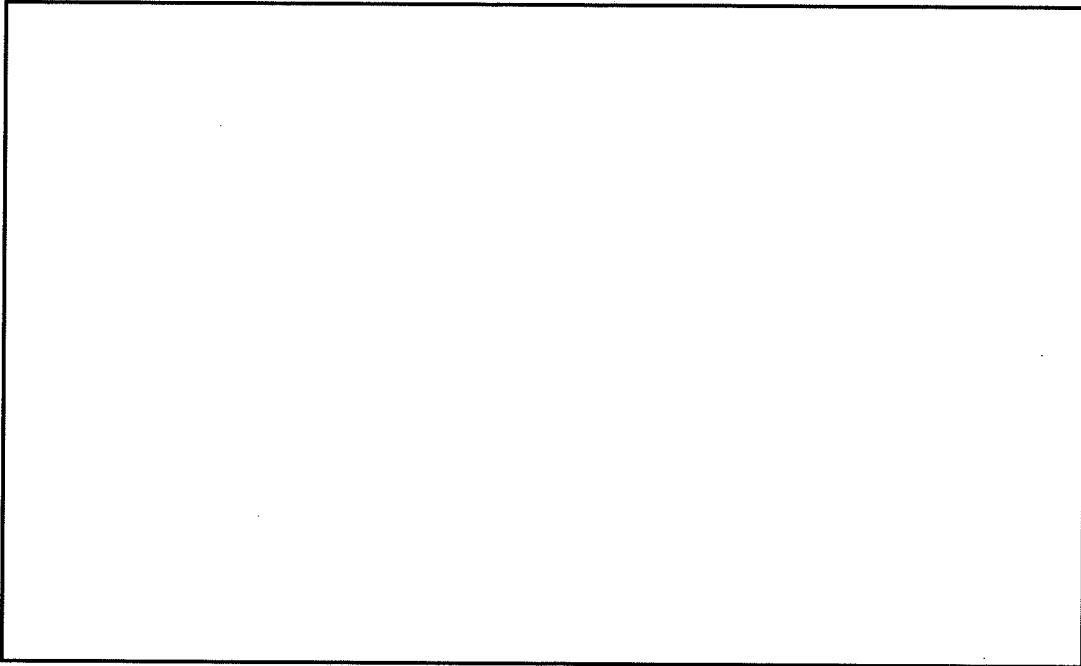
Outside the Scope



**FINAL**

**FOR OFFICIAL USE ONLY**

Outside the Scope

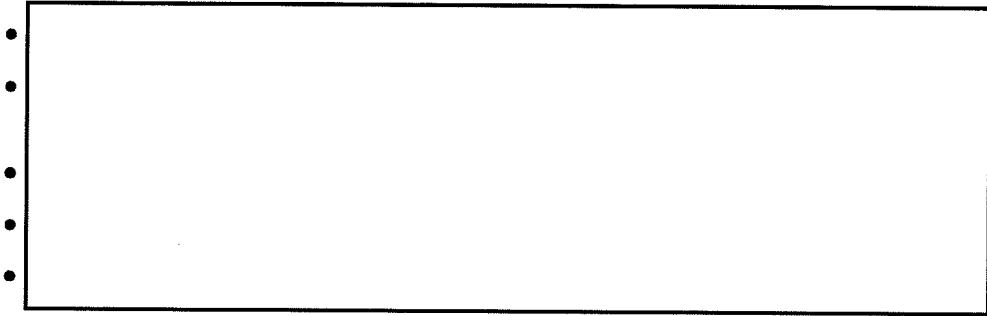


b2  
b7E  
b5

**FINAL**

**FOR OFFICIAL USE ONLY**

---



b2  
b7E  
b5



**FINAL**

**FOR OFFICIAL USE ONLY**

---

**APPENDIX B**  
**Document References**

- Department of Justice (DOJ) System Development Life Cycle (SDLC) Guidance Document
- SCOPE Concept of Operations, September 2002.
- Department of Justice, Federal Bureau of Investigation, FY2004 Exhibit 300 Capital Asset Plan, Secure Counter-terrorism Operational Prototype Environment (SCOPE) Investigative Data Warehouse (IDW), July, 2002 version.
- *"FBI Data Warehousing, Data Mining & Collaboration: An Enterprise View of Data"* a public briefing 5/30/03. Mr. Kenneth Ritchhart, Section Chief, Data Engineering & Integration Program Management Office.
- System Requirements Document, Investigative Data Warehouse, version 9, dated March 24, 2004
- Investigative Data Warehouse Business CONOPS, version 1.0, dated February 2, 2004
- System Security Plan (SSP) for the Investigative data Warehouse – Secret (IDW-S), Version 0.9, dated January 8, 2004
- System Engineering Management Plan (SEMP), Final Draft, version 1.3, dated March 17, 2004
- Unstructured Data Management and Analysis Subsystem Design Document, draft document dated February 17, 2004
- Structured Data Management and Analysis Subsystem Design Document, draft document, version 1.2, dated February 25, 2004
- Data Ingest Subsystem High-Level Design Specification, Version 0.4, dated February 4, 2004

**APPENDIX D**  
**Data Source Descriptions**

**D.1 VGTOF: Violent Gang and Terrorist Organizations File**

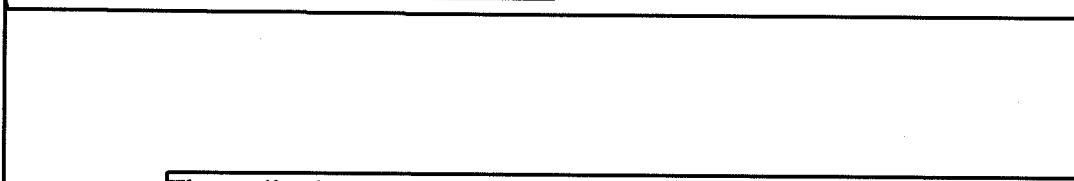
Since September 11, 2001, Director Mueller has directed field offices of the FBI to place the subjects of open terrorism related investigations into the FBI's Terrorism Watch List which is part of the Violent Gangs and Terrorist Organization File (VGTOF) maintained by the National Criminal Information Center (NCIC). The Terrorism Watch List is currently the Counterterrorism Division's integrated listing of lone terrorists, or terrorist groups, of investigative interest to the FBI.

The subjects of counterterrorism investigations are being added to the file daily and are accessed by other Federal, State and local law enforcement agencies whenever these agencies access the system for the purpose of running criminal history checks on individuals of interest to their own investigations (i.e., during routine traffic stops). When accessed by an officer, an application used with the database is capable of automatically notifying the officer that the name is of interest to the FBI and should be treated with caution. The system can provide further instructions such as requesting the officer to notify the FBI of the reason for the inquiry.

The purpose of the data base is to share pertinent biographical information with other Federal, State and local law enforcement agencies for officer safety and mutual investigative interest.

The Terrorism Watch List (VGTOF) is in the process of being consolidated into a single data base managed by the Terrorist Threat Integration Center (TTIC) and the recently announced Terrorist Screening Center (TSC).

D.2



The application is also used as an analytical tool and a source for intelligence information.

b2  
b7E

FOR OFFICIAL USE ONLY

D.3 [redacted]

[redacted] is an investigative tool that also serves as the central repository for [redacted] data obtained throughout the course of an FBI investigation, to include [redacted]. The [redacted] source data is in part obtained from FBI operations.

b2  
b7E

D.4 [redacted]

This is actually a dual program [redacted] serving as one repository.

[redacted]

b2  
b7E

provides the ability [redacted] within various criteria and provides statistical reports. [redacted] is the repository for [redacted] provided to the FBI by FINCEN.

**D.5 VCF: Virtual Case File**

This will be the central repository for FBI investigations. It is currently under development and is expected to become operational by the end of 2004. The VCF system will be a structured central database supporting investigative activities enterprise-wide. The database will contain relevant data to all cases opened for investigation including court files and related law-enforcement information from state and local field office sources. Due to security and access control challenges and programmatic constraints, current plans are for the IDW system to use a subset of the entire VCF content. This subset of VCF content will be consistent with the case classification restrictions, and other (Federal Grand Jury, Federal Taxpayer Information, Bank Secrecy Act Information) restrictions which are currently on ACS documents being copied into the IDW.

**D.6. SAMNET: Secure Automated Message Network**

This system is used to transmit and receive messages from the Intelligence Community and other agencies. SAMNET is also used by Legat Offices, and Field and Headquarters Divisions to exchange messages up to the TS/SCI level. The system is being modernized to include a migration to the Defense Message System (DMS), and replacement of an existing manual method of printing and delivering paper, with electronic delivery to the

**FOR OFFICIAL USE ONLY**

---

appropriate desktop, based on functional profile. SAMNET information can be from DoD and other Intelligence Community sources.

**D.7 JICI: Joint Intelligence Community Inquiry**

This is a static collection of anti-terrorist files collected from FBI field office files following 9/11. The collection represents a historical record of field office files and is not currently updated on a regular basis. The files are searched for target words usually in conjunction with other associated databases.

**D.8 IntelPlus: Intelligence Plus**

This is an application which allows the users to view "Table of Contents" lists from large collections of records in various formats. The user is able to display the document whether it is in text form or one of several graphic formats and then print, copy or store the information. The application allows researchers in tracking associated documents by assisting the user on going to related topics and provides a convenient search capability. The Intel Plus application is currently organized around six separate counterterrorism collections:

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

b2  
b7E

**D.9** [Redacted]

[Redacted]

The service is available to government organizations.

Table 2 Data Ingest Initiated Transaction

Item #	Ingest Initiated Transaction	2004	2005	2006	2007	2008	Record Size (average)	Reference HLF
1	Ingest data from external source							REQT30
2	Ingest data from ACS/CF							REQT30.1
3	Ingest data from VGTOF							REQT30.2
4	Ingest data from SAMNET-S							REQT30.3
5	Ingest data from [redacted]							REQT30.4
6	Ingest data from [redacted]							REQT30.5
7	Ingest data from [redacted]							REQT30.6
8	Ingest data from IntelPlus							REQT30.7
9	Ingest data from [redacted] from the field							REQT30.8
10	Ingest data from [redacted]							REQT30.9
11	Ingest data from JICI							REQT30.11
12	Ingest data from [redacted]							REQT30.12
13	Ingest data from [redacted]							REQT30.13
14	Ingest data from [redacted]							REQT30.14
15	Ingest data from [redacted]							REQT30.15
16	Ingest data from [redacted]							REQT30.16

b2  
b7E

Table 2 Ingest Initiated Transaction

Item #	Ingest Initiated Transaction	2004	2005	2006	2007	2008	Record Size (average)	Reference HLFR
17	Ingest data from [redacted]							REQT30.17
18	Ingest data from [redacted]							REQT30.18
19	Ingest data from [redacted]							REQT30.19
20	Ingest data from [redacted]							REQT30.20
21	Ingest data from [redacted]							REQT30.21
22	Ingest data from [redacted]							REQT30.22
23	Ingest data from [redacted]							REQT30.23
24	Ingest data from [redacted]							REQT30.24

b2  
b7E

Table 2 Ingest Initiated Transaction

Item #	Ingest Initiated Transaction	2004	2005	2006	2007	2008	Record Size (average)	Reference HLFR
25	Ingest data from FinCen - [redacted] Information.							REQT30.25
26	Ingest selectively from FinCen Data							REQT65.2
27	Ingest selectively [redacted]							REQT65.3
28	Ingest selectively [redacted]							REQT65.4
29	Ingest selectively [redacted]							REQT65.5
30	Ingest selectively from [redacted]							REQT67
31	Ingest selectively from [redacted]							REQT67.1
32	Ingest selectively from [redacted]							REQT67.2
33	Ingest selectively from [redacted]							REQT67.3
34	Ingest selectively from [redacted]							REQT67.4

b2  
b7E

Table 2 Ingest Initiated Transaction

Item #	Ingest Initiated Transaction	2004	2005	2006	2007	2008	Record Size (average)	Reference HLFR
35	Ingest selectively from [redacted]							REQT67.5
36	Ingest selectively from [redacted]							REQT67.6
37	Ingest selectively from [redacted]							REQT67.7
38	Ingest selectively from [redacted]							REQT67.8
39	Ingest selectively on an ad hoc basis, data from open sources.							REQT69
40	Ingest selectively from the [redacted]							REQT69.1
41	Ingest selectively from [redacted]							REQT69.2
42	Ingest selectively from [redacted] data.							REQT69.3
43	Ingest selectively from [redacted]							REQT69.4
44	Ingest selectively from [redacted]							REQT69.5

b2  
b7E



Table 2 Ingest Initiated Transaction

Item #	Ingest Initiated Transaction	2004	2005	2006	2007	2008	Record Size (average)	Reference HLF
45	Ingest selectively from [redacted]							REQT69.6
46	Ingest selectively from [redacted]							REQT69.7
47	Ingest selectively from [redacted]							REQT69.8
48	Ingest selectively from [redacted]							REQT69.9
49	Ingest selectively from data about [redacted]							REQT69.10

b2  
b7E

**Investigative Data Warehouse (IDW) Documentation**  
**26 Aug 2005**

1. Analysis of Requirements for Holding NATO Classified
2. Chiliad - Analyst Update Course
3. Computer Security Incident Response Plan
4. Configuration Management Plan
5. Data Administration Manual
6. Data Ingest Subsystem - Component Design Specifications
7. Data Ingest Subsystem - High Level Design Specifications
8. Data Ingest Subsystem - Record Tracking
9. Data Ingest Subsystem - Unstructured Data Processing
10. Data Management Manual
11. IDW - MiTap ICD
12. IDW - SAMNet ICD v1
13. IDW - Virtual Case File ICD
14. IDW 1.1 Users Guide
15. IDW Operations and Maintenance Support Plan
16. IDW Security Operations Manual
17. IDW-I Build Out Test Report - Phase 1
18. IDW-I System Security Plan -I
19. IDW-S - SAMNet ICD
20. IDW-S ACS ICD V1
21. IDW-S System Security Plan -S
22. Maintenance Manual
23. Materials Request Policy
24. Performance Monitoring and Measurements
25. Privileged Users Guide
26. Project Management Plan
27. RetrievalWare - Analyst Update Course
28. System Administrators Guide
29. System Administrators Manual
30. Test and Evaluation Test Analysis Report
31. Training Evaluation Plan
32. Training Management Plan
33. User Support Manual
34. Users Reference Guide
35. Violent Gang and Terrorist Organization File (VGTOF) ICD

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 08-02-2007 BY 65179 DMH/BJA/CAL

Data Type	Media	Frequency
Intel Plus	FTP	Weekly
JICI	N/A	One-time
SAMNet	FTP	3X Daily
Open Source	CD	Daily
VGTOF	CD	Weekly

Table 5-1 IDW Data Ingest Type, Media and Frequency

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 08-02-2007 BY 65179 DMH/BJA/CAL