Federal Bureau of Investigation
Fiscal Year (FY) 2008
Internal Planning & Budget Review
Program Narrative Summary for ENHANCEMENTS/INCREASES

SUMMARY*	
(U) Division Name:	Counterterrorism
(U) Program Name/Number:	National Security Branch / Program 1
(U) Item Name:	National Security Branch Analytical Capabilities
(U) Director's Priority:	Protect US from terrorist Attack
(U) Division Ranking of Item:	
(U) Program Enhancement/Increase Personnel: ***Positions (Agents/Intelligence Analysts/Other Support)***	56 Positions (10 Agents, 5 Intelligence Analysts, 41 Other Support)
(U) Program Enhancement/Increase Non-Personnel: ***Dollars***	$127,362,446

*All requested amounts must tie to requests completed in the Internal Budget Request Excel template.

(U) Summary of Program. Describe the organizational program and activities funded by this item. Explain why it matters in achieving the overall goals and mission of the FBI.

(U) On June 28, 2005, the President of the United States issued a Memorandum (White House Memorandum 28 June 2005: Strengthening the ability of the Department of Justice to Meet Challenges of the Security of the Nation) directing the Attorney General to establish a "National Security Service" and to combine the missions, capabilities, and resources of counterterrorism, counterintelligence, and intelligence elements of the FBI under the leadership of a senior FBI official. This was based on the recommendation of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission).

(U) The FBI subsequently created the National Security Branch (FBI EC 12 SEP 2005: ESTABLISHMENT OF THE FBI NATIONAL SECURITY BRANCH) to integrate the FBI's national security programs for counterterrorism, counterintelligence, and intelligence under the leadership of the Executive Assistant Director for the National Security Branch (EAD-NSB). The FBI also established policies and initiatives to enhance the capability of the entire Bureau to support its national security missions.

(U) In 2001, Homeland Security Presidential Directive-2 (HSPD-2) established the Foreign Terrorist Tracking Task Force (FTTTF) as part of the National Counterterrorism Community under the leadership of the Counterterrorism Division of the FBI. Existing HSPD-2 operations will be enhanced and expanded to provide analysis and technology support to the NSB. The new center will capitalize on existing personnel, practices, tools, infrastructure, and access to datasets already established within FTTTF, and cooperate with the FBI's reorganized Office of the Chief Information Officer (OCIO) and the consolidation of technology and data resources. The new center will is tentatively called the National Security Analysis Center (NSAC).

(U) The mission of the NSAC is to fulfill the FTTTF mission objectives under HSPD-2 and support the Federal Bureau of Investigation's National Security Branch (NSB) components (Counterintelligence and Counterterrorism (U) Divisions, and Intelligence Directorate) in the detection, identification, and tracking of individuals or

entities that pose threats to the United States and its interests through the use of advanced analytical techniques, technologies, and data resources.

(U) Thus, the FTTTF becomes a part of the NSAC, to capitalize on the existing expertise and infrastructure of the FTTTF. The NSB's Investigative Data Warehouse (IDW) combined with the FTTTF's existing applications and business processes will form the backbone of the NSB's data exploitation system. The strategy to implement the mission of NSAC is to capitalize on existing applications within FTTTF and the addition of IDW to support the NSB. This enhancement will support the core strategy of the NSB.

(U) This FY2008 enhancement request is designed to implement the IT requirements for the NSAC by augmenting the existing HSPD-2 operations to provide the additional analysis and technology support for the NSB.

(U) Justification of Personnel and Non-Personnel Resources Requested (Enhancements). Program managers should provide a clear understanding of what is being requested and why it is requested. Justifications should include how the level of resources and dollar amounts were derived, including relevant workload data (please see Expected Outcome/Results section and Workload/Performance and Resources Table below). Justifications should clearly explain the types of positions requested. The rationale and assumptions for amounts and quantities of non-personnel requests should be full explained. Most importantly, justifications should clearly describe the difference between what can be accomplished with base resources versus what could be accomplished with the requested increases.

(U) Expected Outcome/Results. Identify what benefit or results will be realized by funding this program and item at the requested level. You must provide workload data and assessments and other data as appropriate. Use the Workload/Performance and Resources Table below to provide a more detailed description of the expected outcome of continuing current services and providing additional resources.

(U) The FTTTF is charged with ensuring that Federal, law enforcement and intelligence agencies have the best available information with which to keep foreign terrorists and their supporters out of the country. This is accomplished by providing these agencies with critical and timely intelligence supporting their investigative activities, to locate, detain, prosecute or support the denial and removal of any such aliens present in the United States. For over three years, the FTTTF has been the primary center for finding and tracking terrorists and their supporters already inside the US, or trying to enter into this country. Using sophisticated electronic search tools, analysts sift through data to assemble and provide actionable intelligence to law enforcement, government agencies, and the intelligence community. The Task Force is recognized as a major center of excellence for its ability to assemble, manage, and exploit large amounts of public and proprietary data from multiple sources.

(U) Concurrently, as a consequence of the terrorist attacks of September 2001, the FBI identified the need to develop tools that could serve broader FBI investigative needs by accessing a myriad of data sources previously not readily available through conventional software tools. The Secure Collaborative Operative Prototype Environment (SCOPE) was the initial prototype effort designed to support counter-terrorism initiatives. As a proof-of-concept, the SCOPE prototype succeeded in enhancing FBI investigative and analytical capabilities. Subsequently, the IDW project was initiated, building upon the successes of the SCOPE prototype and extending its operational capabilities to a larger number of users and data sets.

(U) Therefore, both the FTTTF and IDW became the two central gatherers of diverse sources of raw data from many different critically important sources. The FTTTF developed mission specific technological tools to explore that data. Also, the FTTTF built a collaborative environment for multiple agencies to acquire and disseminate vital information on terrorists and their supporters. The IDW objective was to create a data warehouse that uses certain data elements to provide a single-access repository for information related to issues beyond counterterrorism to include counterintelligence, criminal and cyber investigations.

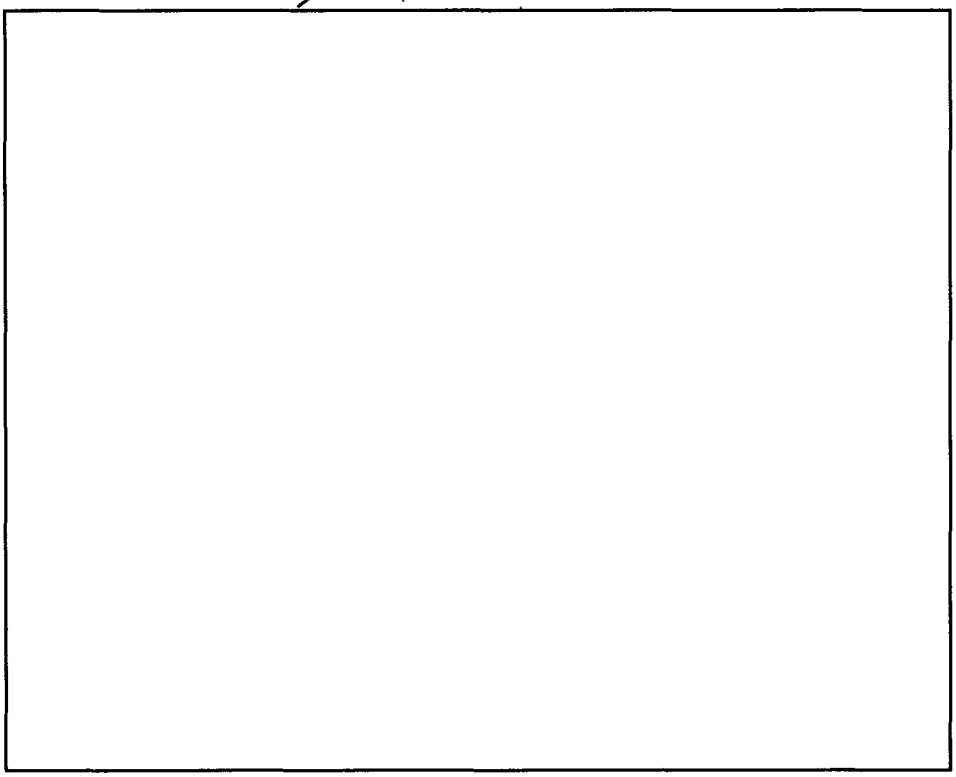
(U) Currently the FTTTF is composed of three operational units: the Tracking and Detection Unit (TDU), the Threat Processing and Assessment Unit (TPAU) and the Risk Assessment Unit (RAU). Additionally the FTTTF recently established the Joint FTTTF CIO Engineering Support Unit, supported by the OCIO's office, to provide

the Information Technology services. Finally, the other support functions such as Requirements, Training, Budget, Facilities Management, etc, are supported by smaller teams

(U) The NSB proposes the generation of the NSAC to fill a data exploitation gap across the branch. Coordinated analytical teams will be established to exploit the entire NSB with particular focus on the requirements of operational entities. Additionally, the NSB is sponsoring an integrated solution between the core applications supporting FTTTF and IDW. Between the two entities, the FBI has assembled a strong collection of valuable operational data and highly successfully analytical and technical applications that realize operational successes.

(U) NSAC will contain three main functions: Operations, Support, and Information Technology.

- (U) Operations consist of 4 analysis groups: 1) Tracking & Detection; 2) Threat Processing & Assessment; 3) Risk Assessment; and 4) Special Projects.
- (U) Support consists of three groups: 1) Program Management, Metrics, Training/Outreach, Policy/Legal; 2) Budget/Human Resources, Facilities, and Security; and 3) Requirements.
- (U) The Information Technology portion reports to the Chief Information Officer (CIO) and the Chief Technology Officer (CTO) of the FBI. However, all activity at the NSAC is responsible to the NSAC Director. Information Technology consists of two primary areas: 1) Proof of Concept OPS which is rapid development fast-track operations, and 2) Projects and Programs that develop long-term efforts in accordance with established best practices.



b2
b7E

(U) The National Security Analysis Center (NSAC) will include FTTTF Operations under HSPD-2 and expand to support National Security Branch requirements.

The below plan represents the overall staffing requirements of the NSAC to be implemented over a three year budget cycle. The plan considers the FBI hiring process and proven contractor hiring pace. Furthermore, the three year phased approach allows the NSB to evaluate and monitor the workload associated with function to ensure staffing estimates are neither to great or too small.

National Security Analysis Center (NSAC)
FY2008 - FY2010 Enhancement Proposal
Including Foreign Terrorist Tracking Task Force (FTTTF) and Integrated Data Warehouse (IDW) Base Infrastructure

		Base					NSAC Enhancement					FY2008 Total				
FY2008	FTTTF & IDW Base	FBI	OGA & CON	CON (Non-IT)	CON (IT)	Total	FBI	OGA	CON (Non-IT)	CON (IT)	Total	FBI Total	OGA	CON (Non-IT)	CON (IT)	Total
	Front Office	3	1	5	0	9	0	3	-4	0	-1	3	4	1	0	8
	Program Management	0	0	3	0	3	6	0	8	0	14	6	0	11	0	17
	Budget/HR/ Facilities	2	0	7	0	9	3	0	13	0	16	5	0	20	0	25
	Security	2	0	12	0	14	0	0	10	0	10	2	0	22	0	24
	Requirements	2	0	11	0	13	2	0	3	0	5	4	0	14	0	18
	Tracking and Detection	7	1	27	0	35	20	14	18	0	52	27	15	45	0	87
	Threat Processing & Assmt	5	0	23	0	28	8	2	28	0	38	13	2	51	0	66
	Risk Assessment	4	0	8	0	12	8	2	7	0	17	12	2	15	0	29
	[redacted]	7	0	4	0	11	11	3	9	0	23	18	3	13	0	34
	Operations Support	2	0	14	0	16	-2	0	-14	0	-16	0	0	0	0	0
	Information Technology	5	0	0	137	142	0	0	0	114	114	5	0	0	251	256
	IDW	1	0	0	57	58	0	0	0	39	39	1	0	0	96	97
	TOTAL	40	2	114	194	350	56	24	78	114	272	96	26	192	347	661
		FY2009 Base (with FY08 Enhancement)					FY2009 Enhancement					FY2009 Total				
FY2009	NSAC, FTTTF & IDW	FBI Total	OGA	CON (Non-IT)	CON (IT)	Total	FBI Total	OGA	CON (Non-IT)	CON (IT)	Total	FBI Total	OGA	CON (Non-IT)	CON (IT)	Total
	Front Office	3	4	1	0	8	2	1	0	0	3	5	5	1	0	11
	Program Management	6	0	11	0	17	0	0	0	0	0	6	0	11	0	17

b2
b7E

Budget/HR/ Facilities	5	0	20	0	25	0	0	1	0	1	5	0	21	0	26
Security	2	0	22	0	24	0	0	2	0	2	2	0	24	0	26
Requirements	4	0	14	0	18	4	0	0	0	4	8	0	14	0	22
Tracking and Detection	27	15	45	0	87	24	0	35	0	59	51	15	80	0	146
Threat Processing & Assmt	13	2	51	0	66	7	1	47	0	55	20	3	98	0	121
Risk Assessment	12	2	15	0	29	16	0	4	0	20	28	2	19	0	49	
[redacted]	18	3	13	0	34	10	1	3	0	14	28	4	16	0	48
Operations Support	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Information Technology	5	0	0	251	256	0	0	0	0	0	5	0	0	251	256
IDW	1	0	0	95	96	0	0	0	0	0	1	0	0	95	96
Total	96	26	192	346	660	63	3	92	0	158	159	29	284	346	818

FY2010

	FY2010 Base (With FY2009 Enhancement)					FY2010 Enhancement					FY2010 Total				
NSAC, FTTTF & IDW	FBI Total	OGA	CON (Non-IT)	CON (IT)	Total	FBI Total	OGA	CON (Non-IT)	CON (IT)	Total	FBI Total	OGA	CON (Non-IT)	CON (IT)	Total
Front Office	5	5	1	0	11	0	1	0	0	1	5	6	1	0	12
Program Management	6	0	11	0	17	0	0	0	0	0	6	0	11	0	17
Budget/HR/Facilities	5	0	21	0	26	0	0	0	0	0	5	0	21	0	26
Security	2	0	24	0	26	0	0	0	0	0	2	0	24	0	26
Requirements	8	0	14	0	22	0	0	2	0	2	8	0	16	0	24
Tracking and Detection	51	15	80	0	146	24	0	18	0	42	75	15	98	0	188
Threat Processing & Assmt	20	3	98	0	121	0	0	26	0	26	20	3	124	0	147
Risk Assessment	28	2	19	0	49	11	0	5	0	16	39	2	24	0	65
[redacted]	28	4	16	0	48	0	0	0	0	0	28	4	16	0	48
Operations Support	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Information Technology	5	0	0	251	256	0	0	0	0	0	5	0	0	251	256
IDW	1	0	0	95	96	0	0	0	1	1	1	0	0	96	97
Total	158	29	284	251	722	35	1	51	0	87	194	30	335	347	906

b2
b7E

(U) The NSAC will be a service oriented organization. In addition to fulfilling HSPD-2 mission objectives, NSAC will provide the following critical services to NSB components and customers:

- (U) Use innovative analytical techniques to enhance the detection, identification, and tracking of terrorism and intelligence threats.
- (U) Provide information that helps to locate, remove or disrupt the actions of terrorists or others who pose a threat to national security.
- (U) Perform evaluations of unknown persons to identify those who may be or have links to those who pose threats to national security.
- (U) Support NSB development of tailored assessment products regarding individuals, entities, or trends that pose threats to national security.
- (U) Provide rapid response and surge capabilities for special events, short-term projects, and proactive initiatives.
- (U) Support NSB program management oversight and coordinates training, outreach and liaison efforts.
- (U) Provide oversight and supervision of budget formulation, execution, resource usage, facilities, and security matters.
- (U) Identify and gather operational, analytic, and technical requirements to support data and tool evaluation and acquisition strategies for the NSB.
- (U) Provide enabling technology to support NSB components in responding to emerging operational needs.

(U) The IT consolidation will provide the following services:

- (U) Singular extraction, transformation, and load process
- (U) Consolidated data sources
- (U) Consolidated metadata repository
- (U) Consolidated investigative and analytical portal
- (U) Investigative and analytical alert capability
- (U) Integrated portal with authorized investigative and analytical tool sets
- (U) EA standards based relational data model and exchange model

Workload is in the process of being complete and will be forwarded by April 10.

WORKLOAD/PERFORMANCE AND RESOURCES TABLE										
Program:										
WORKLOAD/PERFORMANCE AND RESOURCES	**Projected**		**Projected**		**FY08 (Base and Enhancement)**				**Requested (Total)**	
Workload	**FY 2006**		**2007 President's Budget**		**Current Services (Base)**		**FY 2008 Program Enhancement**		**FY 2008 Request**	
										0
										0
	FY 2006		**FY 2007 President's Budget**		**Current Services (Base)**		**FY 2008 Program Enhancement**		**FY 2008 Request**	
Resources	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**	**FTE**	**$0**

(U) The FTTTF is charged with ensuring that Federal, law enforcement and intelligence agencies have the best available information with which to keep foreign terrorists and their supporters out of the country. This is accomplished by providing these agencies with critical and timely intelligence supporting their investigative activities, to locate, detain, prosecute or support the denial and removal of any such aliens present in the United States. For over three years, the FTTTF has been the primary center for finding and tracking terrorists and their supporters already inside the US, or trying to enter into this country. Using sophisticated electronic search tools, analysts sift through data to assemble and provide actionable intelligence to law enforcement, government agencies, and the intelligence community. The Task Force is recognized as a major center of excellence for its ability to assemble, manage, and exploit large amounts of public and proprietary data from multiple sources.

Historical Outcome Measures and Workload

(U) For example, recently counter-terrorist analysts needed to search for [redacted] persons of interest in [redacted] different databases, collate the results and produce reports. This would have taken an analyst [redacted] to [redacted] FTTTF was able to accomplish the same task in [redacted]

Point: (U) Utilizing technology and automation, in a recent terrorism case the FTTTF analysts were able to accomplish in [redacted] what would have taken traditionally over [redacted]

(U) Additionally, the intelligence community had received information that helicopters may be used in a future terrorist attack. FTTTF's sophisticated querying of the Federal Aviation Administration's Active Pilots Dataset produced a list of 165 helicopter pilots who had licenses to fly helicopters in the U.S. and were from the designated counties of interest. Of the 165 pilots, there were 6 possible matches to derogatory information within the FTTTF's datamart. FTTTF forwarded these results and all intelligence information associated with the individuals to NJTTF and the FBI's Los Angeles Field Office.

b2
b7E

Point: (U) Utilizing technology and analysis FTTTF identified 165 helicopter pilots, 6 of which with possible derogatory information and provided this to the LA field office.

(U) Acting on information linking taxi drivers to a Pakistani terrorist group, Philadelphia law enforcement officials were attempting to review [redacted] individuals licensed by the Pennsylvania Utilities Commission (PUC). This represented a major threat, since Philadelphia taxi drivers have access to sensitive areas including two airports, bus and train stations, municipal buildings, and densely-populated tourist areas. FTTTF assisted Philadelphia in their efforts by returning dates of birth on [redacted] individuals of the [redacted] names provided through FTTTF's "batch matching" capability with the public source. This process took FTTTF [redacted] and saved Philadelphia [redacted] by not manually searching each name individually through public source records.

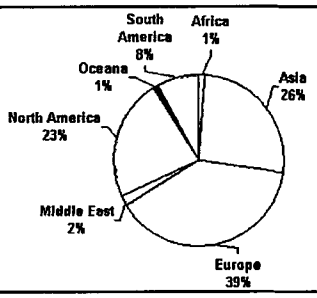
Point: (U) In a past investigation and based on a threat, FTTTF utilized its batch technology and access to open source information to review [redacted] taxi drivers to provide Philadelphia Division with additional previously unknown biographical information regarding the drivers.

(S) [redacted]

b1

(S)

(U) In 2005, approximately 1% of all I-94s filed were by visitors from African countries, 26% from Asia, 38% from Europe, 2% from the Middle East, 38% from North America, 1% from Oceana (i.e. South Pacific, Australia, etc.) and 8% from South America. Of those filed 978,619 were from former Soviet block countries and 518,298 from China. To vet a larger pool of foreign visitors for potential derogatory, intelligence and/or investigative interest will be a monumental task and will require significant resources. However, it has great potential to provide not only valuable tactical and strategic intelligence but will help ensure individuals who pose potential threats to national security are identified and addressed in a comprehensive and expeditious manner.



b1

Point: (U) Based on 2005 immigration data countries from Asia (26%) and Europe (39%) make up the majority of visitors to the U.S. Nearly 1 million of these are from the former Soviet Union countries and ½ a million from China. These pose a potential and significant counterintelligence threat.

(S)

(S)

(S)

b1

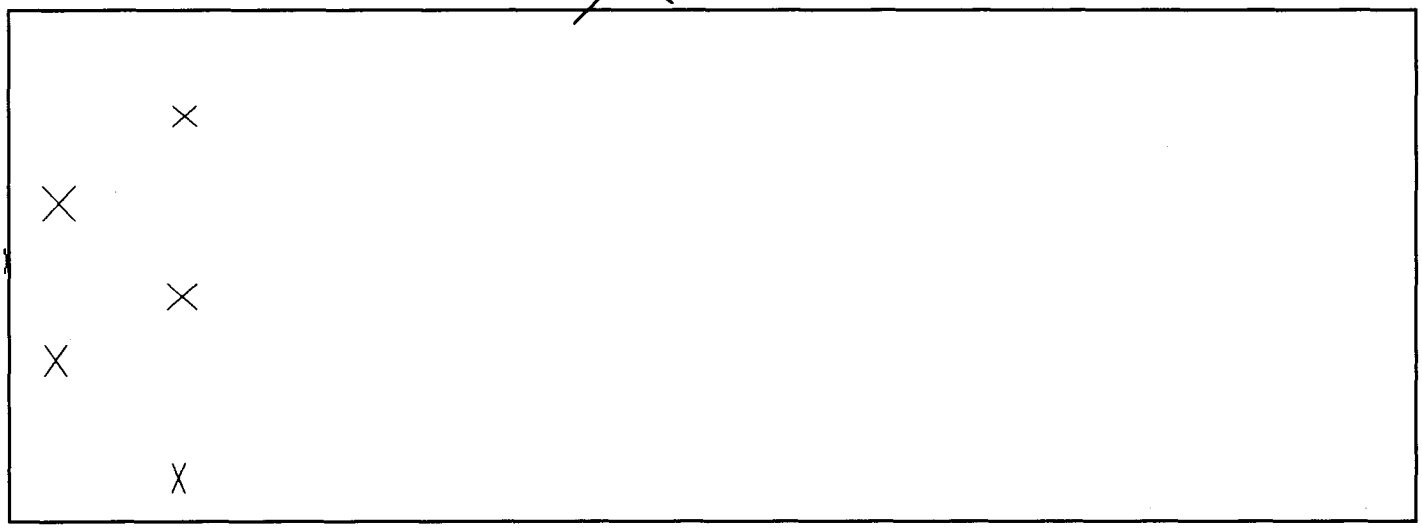
Data Mining Workload and Mandate

(U) According to the General Accounting Office (GAO) May 2004 report on federal data mining efforts, the GAO defined data mining as "the application of database technology – to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results" (GAO-05-866, Data Mining, p. 4). There are a number of security and privacy issues that government and private industry must address when contemplating the use of technology and data in these ways. While the current activities and efforts of the IDW and FTTTF programs do not provide NSB users with a the full level of data mining services as defined above it is the intention of the NSAC to pursue and refine these capabilities where permitted by statue and policy. The implementation and responsible utilization of these services will advance the FBI's ability to address national security threats in a timely fashion, uncover previously unknown patterns and trends and empower agents and analysts to better "hunt between the cases" to find those persons, places or things of investigative and intelligence interest.

Point: (U) While the IDW and FTTTF programs are not able to provide the suite of "data mining" services as defined by the GAO it is the intention of the NSAC to pursue these as statue and policy permits to enhance NSB activities and services.

Counterintelligence Workload and Outcome

(S)



(S) b1

Tracking and Detection Unit (TDU) Workload and Outcome

(U) To date, the TDU Visa Revocation program has found previously unknown locations, identifying information, and travel details on 1,026 subjects, with possible links to terrorism and provided 466 disseminations of lead information to the Terrorist Screening Center (TSC), to be forwarded to the NJTTF and appropriate Field Offices for further action.

Point: (U) To date, the FTTTF Visa Revocation program has found information regarding 1,026 subjects with possible links to terrorism and disseminated 466 leads.

(U) To date, TDU has conducted analysis on foreign Hazmat drivers operating in the U.S. and produced [ ] analytical products completed within [ ] of receipt. b2 b7E

Point: (U) FTTTF has produced [ ] analytical products regarding foreign Hazmat drivers with an average completion within [ ] of receipt.

(U) To date, TDU has run 508,906 identities on the Terrorist Watchlist against predicated and open source data a total of 132,826,300 times. These runs have resulted in

557 disseminations of information.

Point: (U) To date, FTTTF has run 508,906 identities on the Terrorist Watchlist against predicated and open source data a total of 132,826,300 times. These runs have resulted in 557 disseminations of information.

(U) Previously TDU assisted with the vetting of applicants for flight training, covered by ATSA Section 113, and reviewed them for risk to aviation and national security. All flight training candidates were processed within the legislated time constraints. Since 3/2005, 504 applicants have been vetted and derogatory information provided to TSA on 51 candidates.

Point: (U) In the past, FTTTF assisted with the vetting of 504 applicants for flight training identifying 51 with derogatory information provided to TSA.

(U) To date TDU has responded to a number of requests for actionable information on suspected associates of terrorism and completed 236,680 leads with disseminations on 80,471 individuals.

Point: (U) FTTTF has completed over 236,000 leads with disseminations on 80,471 potential terrorism subjects. .

Risk Assessment Unit (RAU) Workload and Outcome

(S) [redacted] b1

Proactive Data Exploitation Unit (PDEU) Project Workload and Outcome

(U) In support of its mission the Proactive Data Exploitation Unit (PDEU) at FTTTF (formerly of the Terrorist Financing Operations Section - TFOS) has begun a number of proactive projects and initiatives. These projects involve the exploitation and analysis of existing FBI and other agency data to identify previously unknown or realized connections between suspicious financial activities and terrorism related matters. To date, these efforts have identified 1000s of leads and previously unknown relationships between terrorism investigations and suspicious financial activities.

Point: (U) FTTTF analysts were able to uncover 1000s of previously unknown links to numerous terrorism investigations.

PDEU Investigative Data Warehouse (IDW) Batch Workload and Outcome

(U) PDEU has batched over [redacted] items through the IDW which are estimated to have generated over [redacted] query iterations. Prior to the advent of this technology this level of query activity is equal to approximately [redacted] analysts [redacted] In all, an estimated [redacted] items have been queried through the IDW resulting in approximately [redacted] query iterations, equivalent to over [redacted] of effort. This level of automation and technology dramatically increases efficiency and knowledge discovery. b2 b7E

Point: (U) FTTTF analysts' utilization of IDW was able to perform the jobs of equivalent to [redacted] This increase in efficiency results in millions of dollars saved. b2 b7E

PDEU BSA Project

(U) In the Fall of 2005, PDEU identified over 88,000 BSA documents containing 1000s of new bank account numbers related to subjects of terrorism investigations by comparing and exploiting information in common between BSA data provide by FinCEN and individuals listed on the Terrorist Watch List (TWL).

Point: (U) Utilizing technology and automation, FTTTF analysts were able to uncover 1000s of new financial information linked to terrorism subjects, thereby allowing investigators to explore additional leads that were not available to them before.

PDEU Money Service Business Project

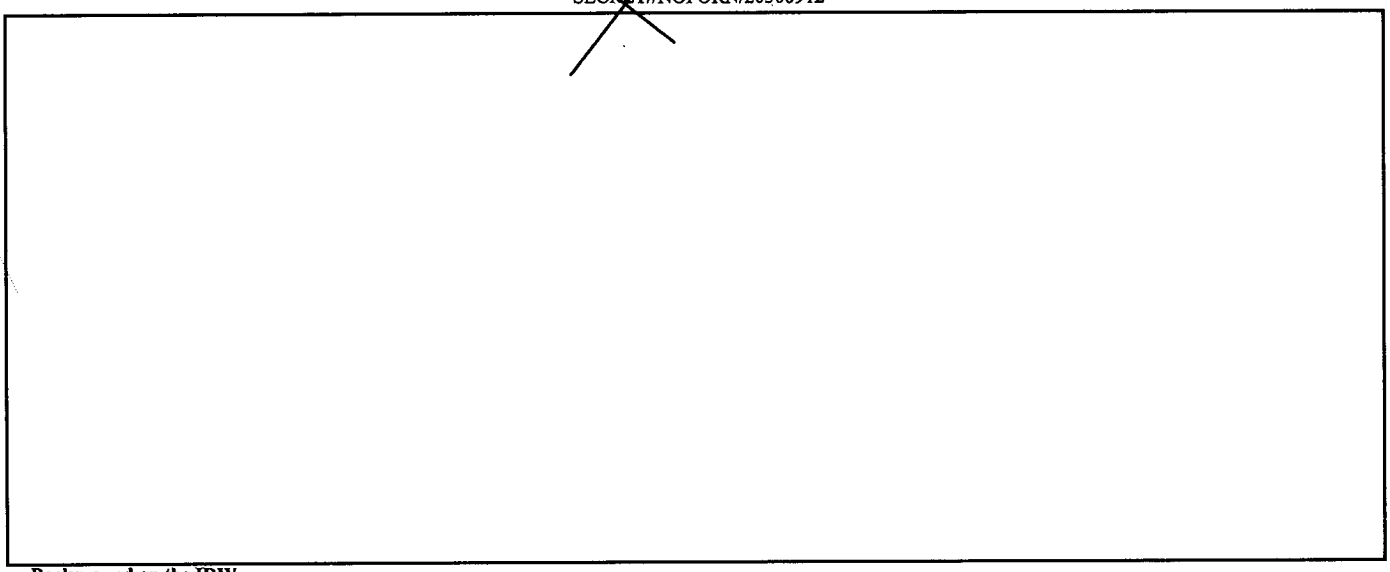
(U) Working with the TFOS Program Management and Coordination Unit (PMCU), PDEU identified over 35 terrorism subjects who owned or operated registered Money Service Businesses (MSB), 5 of which were not known by the respective case agents.

Point: (U) Utilizing technology and automation, FTTTF analysts were able to uncover terrorism subjects operating money service businesses not previously known to investigators.

Hazardous Materials – Commercial Drivers License (HAZMAT/CDL) Project

(S) [redacted] b1

(S)



b1

Background on the IDW

(U) The Investigative Data Warehouse (IDW) is a centralized, web-enabled repository for relevant intelligence and investigative data that allows users to query the information utilizing advanced software tools. The FBI has made extensive use of this system. In 2004, CTD provided IDW with additional funding to create a Special Project Team (SPT) dedicated to increase the number of data, users and services/capabilities. The PDEU, now part of FTTTF was given operational lead for the CTD SPT effort.

(U) As a result of this effort the IDW program has experienced significant growth and provides a number of services that has substantially increased the efficiency and effectiveness of the FBI. The IDW batch process alone have saved millions of dollars in time and resources. A single user can now accomplish what would have taken scores of users months to achieve.

Point: (U) The IDW has experienced a 25x growth in data and 32.5x in users.

Growth in NSB Workload and Relevant Data

(U//FOUO) As of 03/17/2006, the IDW contained over 587 million documents with 72% from non-FBI sources. This effort is a prime example of the kind of inter-agency sharing and collaboration mandated by Legislative and Executive branches. The FTTTF also maintains a large data mart containing over 1.4 billion documents/records and a suite of other services not provided by the IDW system. A review was conducted of the data sets contained in the IDW and FTTTF systems which determined that approximately 800 million of the FTTTF records are unique and not contained within the IDW. The IDW and FTTTF combined have over 50

other data sets proposed or pending ingestion with containing billions of new records. Some of these include data sets co-sponsored by other NSB divisions such as counterintelligence (e.g. Dept. of State Consular Consolidated Database) or those with Criminal Division (e.g.

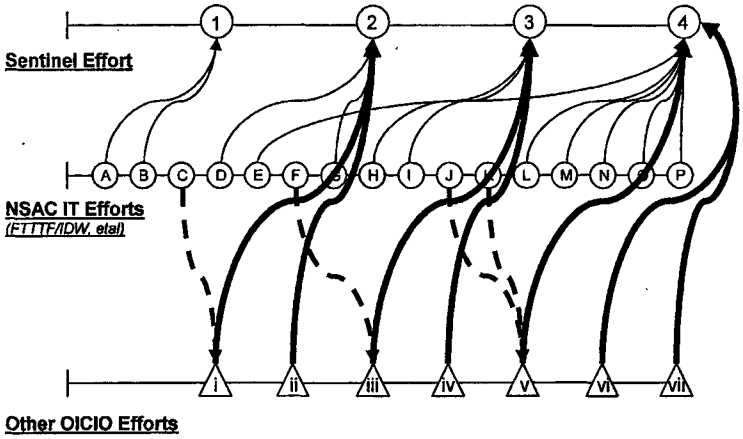
Point: (U//FOUO) Between the IDW and FTTTF systems NSB users will have access to over 1.4 billion documents/records with one to two times that pending ingestion.

(U) In an effort to better leverage these two systems and identify areas of integration the FTTTF recently tasked the MITRE Corporation to conduct an assessment to develop a baseline understanding of current information technology (IT) related aspects of FTTTF and the Investigative Data Warehouse (IDW) system. After establishing this baseline understanding, MITRE identified opportunities for integrating the IDW application and infrastructure into the FTTTF organization. The results of this assessment are being reviewed and combined with recommendations from IDW, FTTTF and the OCIO.

Point: (U) FTTTF recently tasked MITRE Corp. to conduct an assessment of the FTTTF and IDW IT and how they could be best integrated.

(U) The integration of these data sets and suites of services will allow users to quickly identify the potential investigative or intelligence significance of an item in question. Following the development principles utilized by the FTTTF and IDW/SPT of focused, and operationally driven taskings will ensure that resources expended are conserved and contribute to the long-term good. These advances will be made in concert and coordination with the OCIO. NSAC will coordinate with the various IT efforts to ensure collaboration and the periodic cut-overs.

Point: (U) The NSAC will coordinate with the various IT efforts to ensure collaboration and the periodic cut-overs to other OCIO efforts.



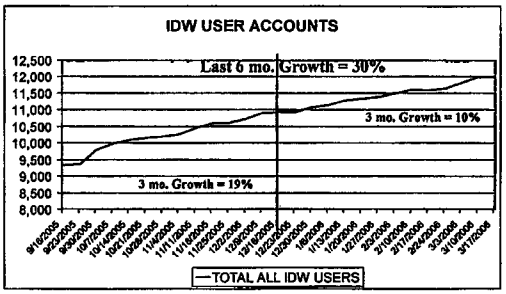
(U) Some of the critical operational enhancements needed within the IDW and FTTTF systems include such things as role-based discretionary access controls (DAC), expanded entity extraction, entity resolution, improved data ingestion, and backup, additional storage, data normalization, visualization and automated report writing. These improvements will increase the availability and reliability of data and significantly increase the productivity of the users to assimilate and analyze information.

Point: (U) Some critical operational enhancements are needed within the IDW and FTTTF systems which will afford greater access to data and analytical services.

IDW Utilization

(U) As of 03/17/2006, there were 23,759 references to IDW in ACS/ECF. Approximately 87% referred to NSB related Case Classifications. The number of counterintelligence references is steadily increasing as are those for criminal and cyber. Due to current restrictions the IDW contains only limited case data from Cyber, Civil Rights and Public Corruption investigations. The requests for new accounts has increased dramatically in last 2 months and account utilization across all programs is rising.

Point: (U) IDW utilization among all investigative programs is increasing with a historical predominance by NSB related programs. The growth in new user accounts is growing at a rate of about 200 per week.



Areas for Improvement for IDW

(U) Some areas for improvement in the IDW system include: Need capability for continuous operation given loss of primary site or capability at primary site; Additional resources needed to meet for projected growth in number of users and volume of data; Need more robust (responsiveness and capacity) backup and restore capability; and need more robust test capability

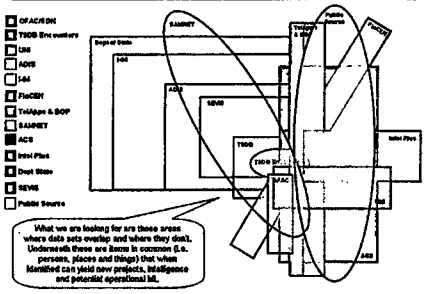
Point: Areas of improvement for the IDW system include COOP capabilities, adequate test/backup and restore as well as resources to manage the anticipated growth in data, users and services.

IDW Accomplishments in FY 2006

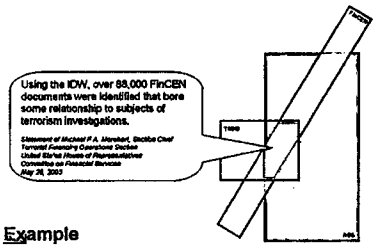
(U) Some of the program goals and achievements for FY06 include: Provided geo-coded data for NSB demonstration; conducted beta test for Chiliad Continuous

Monitoring (or Alert) for NSB; began the consolidation of SPT data with IDW core services & data; rebalanced allocation of servers and continue efforts to optimize computer resource utilization; completed storage system upgrade; completed integration with the Investigators Portal (IP) prototype; and completed preparation and testing to upgrade operating system (OS).

Looking for overlapping spheres of influence



Proactive Identification of Financial Records re: Known/Suspected Terrorists



Example

Conclusion

(U) As a consequence of the terrorist attacks of September 2001, the FBI identified the need to develop tools that could serve broader FBI investigative needs by accessing a myriad of data sources previously not readily available through conventional software tools. The Secure Collaborative Operative Prototype Environment (SCOPE) was the initial prototype effort designed to support counter-terrorism initiatives. As a proof-of-concept, the SCOPE prototype succeeded in enhancing FBI investigative and analytical capabilities. Subsequently, the IDW project was initiated, building upon the successes of the SCOPE prototype and extending its operational capabilities to a larger number of users and data sets.

(U) Therefore, both the FTTTF and IDW became the two central gatherers of diverse sources of raw data from many different critically important sources. The FTTTF developed mission specific technological tools to explore that data. Also, the FTTTF built a collaborative environment for multiple agencies to acquire and disseminate vital information on terrorists and their supporters. The IDW objective was to create a data warehouse that uses certain data elements to provide a single-access repository for information related to issues beyond counterterrorism to include counterintelligence, criminal and cyber investigations.

(U) Currently the FTTTF is composed of three operational units: the Tracking and Detection Unit (TDU), the Threat Processing and Assessment Unit (TPAU) and the Risk Assessment Unit (RAU). Additionally the FTTTF recently established the Joint FTTTF CIO Engineering Support Unit, supported by the OCIO's office, to provide the Information Technology services. Finally, the other support functions such as Requirements, Training, Budget, Facilities Management, etc, are supported by smaller teams

(U) The NSB proposes the generation of the NSAC to fill a data exploitation gap across the branch. Coordinated analytical teams will be established to exploit the entire NSB with particular focus on the requirements of operational entities. Additionally, the NSB is sponsoring an integrated solution between the core applications supporting FTTTF and IDW. Between the two entities, the FBI has assembled a strong collection of valuable operational data and highly successfully analytical and

technical applications that realize operational successes.

(U) NSAC will contain three main functions: Operations, Support, and Information Technology.

- (U) Operations consist of 4 analysis groups: 1) Tracking & Detection; 2) Threat Processing & Assessment; 3) Risk Assessment; and [redacted] b2 b7E
- (U) Support consists of four groups: 1) Program Management, Metrics, Training/Outreach, Policy/Legal; 2) Budget/Human Resources, Facilities; 3) Security; and 4) Requirements.
- (U) The Information Technology portion reports to the Chief Information Officer (CIO) and the Chief Technology Officer (CTO) of the FBI. However, all activity at the NSAC is responsible to the NSAC Director. Information Technology consists of two primary areas: 1) Proof of Concept OPS which is rapid development fast-track operations, and 2) Projects and Programs that develop long-term efforts in accordance with established best practices.