

Exhibit 300: Capital Asset Plan and Business Case Summary

Part I: Summary Information And Justification (All Capital Assets)

Section A: Overview (All Capital Assets)

1. Date of Submission: 6/6/2008
2. Agency: Department of Justice
3. Bureau: Federal Bureau Of Investigation
4. Name of this Capital Asset: FBI Terrorist Screening System (TSS)
5. Unique Project (Investment) Identifier: (For IT investment only, see section 53. For all other, use agency ID system.) 011-10-01-02-01-3177-00
6. What kind of investment will this be in FY 2010? (Please NOTE: Investments moving to O&M in FY 2010, with Planning/Acquisition activities prior to FY 2010 should not select O&M. These investments should indicate their current status.) Mixed Life Cycle
7. What was the first budget year this investment was submitted to OMB? FY2006
8. Provide a brief summary and justification for this investment, including a brief description of how this closes in part or in whole an identified agency performance gap:

This investment directly supports HSPD-6 which created the Terrorist Screening Center (TSC) as a combined multi-agency effort with the DOJ, DOS, DHS, DOD, Treasury, and the intelligence community. The investment is aligned to the President's Management Agenda for an expanded E-government, and the FBI's highest strategic goal-to protect the US from terrorist and foreign intelligence activity. The TSC developed a comprehensive database of known and suspected terrorists (KSTs) to promulgate information sharing across foreign and domestic screening partners. The TSC, through Information Technology (IT) initiatives and innovation, consolidated 12 agencies' terrorist watchlists into one consolidated US watchlist; the Terrorist Screening Data Base (TSDB). The TSC supports Federal, state, local, and tribal law enforcement (LE) agencies as well as international partners by maintaining the US consolidated watchlist and through its 24 hour operations center for real time terrorist identification resolution. The TSC maintains this capability through the TSC's watchlisting capacity and support, known as the Terrorist Screening System (TSS). These components include the TSDB, Encounter Management Application (EMA), and Advanced Search Program (ASP). TSDB holds over 900,000 records and is increasing at about 1.7% per month. The TSC and its partners, through the TSS, have developed a layered US defense stretching from overseas visa processes to US local LE encounters. The TSC still faces daunting IT challenges to balancing national security, objectives with privacy/civil liberty concerns. TSC seeks to build upon its pioneering search technology and foreign expansion to substantially increase the fidelity of KST identifications through mandated by Addendum B to HSPD-6, as well as gain efficiencies by combining individual components of the TSS into a larger framework, and greatly expanding its volume and information sharing capacity. This allows TSC to strengthen its information sharing through the TSS, as it continues to develop and improve data integration/exchange with partner agencies, foreign and domestic. The TSC continues this effort by leading in IT innovation as well as legislative, diplomatic, and policy formulation. TSC incremental improvements in efficiency and functionality continue as it acquires/develops IT capabilities to meet evolving requirements/directives, as well as findings and recommendations by the DOJ IG and the GAO.
9. Did the Agency's Executive/Investment Committee approve this request? Yes
 - a. If "yes," what was the date of this approval? 6/6/2008
10. Did the Project Manager review this Exhibit? Yes
11. Contact information of Program/Project Manager?
 Name
 Phone Number
 Email
- a. What is the current FAC-P/PM (for civilian agencies) or DAWIA (for defense agencies) certification level of the program/project manager? Senior/Expert/DAWIA-Level 3
- b. When was the Program/Project Manager Assigned? 1/8/2006
- c. What date did the Program/Project Manager receive the FAC-P/PM certification? If the certification has not been issued, what is the anticipated date for certification? 1/8/2006
12. Has the agency developed and/or promoted cost No

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

effective, energy-efficient and environmentally sustainable techniques or practices for this project?

a. Will this investment include electronic assets (including computers)? Yes

b. Is this investment for new construction or major retrofit of a Federal building or facility? (answer applicable to non-IT assets only) No

1. If "yes," is an ESPC or UESC being used to help fund this investment?

2. If "yes," will this investment meet sustainable design principles?

3. If "yes," is it designed to be 30% more energy efficient than relevant code?

13. Does this investment directly support one of the PMA initiatives? Yes

If "yes," check all that apply: Expanded E-Government

a. Briefly and specifically describe for each selected how this asset directly supports the identified initiative(s) (e.g. If E-Gov is selected, is it an approved shared service provider or the managing partner?) TSC supports PMA E-Gov through IT initiatives such as interagency information sharing policies, processes, and technologies. The TSC developed the TSDB from 12 disparate agency lists maintained on spreadsheets as well as initiated interagency communication at Federal, state, local and international levels. Along with TSDB, TSC continues its efforts and initiatives through technological innovation and evolutionary processes and policies. TSC initiatives have drawn domestic and international partners.

14. Does this investment support a program assessed using the Program Assessment Rating Tool (PART)? (For more information about the PART, visit www.whitehouse.gov/omb/part.) Yes

a. If "yes," does this investment address a weakness found during a PART review? Yes

b. If "yes," what is the name of the PARTed program? 10003802 - FBI Counterterrorism Program

c. If "yes," what rating did the PART receive? Adequate

15. Is this investment for information technology? Yes

If the answer to Question 15 is "Yes," complete questions 16-23 below. If the answer is "No," do not answer questions 16-23.

For information technology investments only:

16. What is the level of the IT Project? (per CIO Council PM Guidance) Level 3

17. In addition to the answer in 11(a), what project management qualifications does the Project Manager have? (per CIO Council PM Guidance) (1) Project manager has been validated as qualified for this investment

18. Is this investment or any project(s) within this investment identified as "high risk" on the Q4 - FY 2008 agency high risk report (per OMB Memorandum M-05-23) Yes

19. Is this a financial management system? No

a. If "yes," does this investment address a FFIA compliance area?

1. If "yes," which compliance area:

2. If "no," what does it address?

b. If "yes," please identify the system name(s) and system acronym(s) as reported in the most recent financial systems inventory update required by Circular A-11 section 52

20. What is the percentage breakout for the total FY2010 funding request for the following? (This should total 100%)

Hardware	21
Software	11
Services	64
Other	4

21. If this project produces information dissemination products for the public, are these products published to the Internet in conformance with OMB Memorandum 05-04 and included in your agency inventory, schedules and priorities? N/A

22. Contact information of individual responsible for privacy related questions:

Name

Phone Number

Title

E-mail

23. Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval? Yes

Question 24 must be answered by all Investments:

24. Does this investment directly support one of the GAO High Risk Areas? Yes

Section B: Summary of Spending (All Capital Assets)

1. Provide the total estimated life-cycle cost for this investment by completing the following table. All amounts represent budget authority in millions, and are rounded to three decimal places. Federal personnel costs should be included only in the row designated "Government FTE Cost," and should be excluded from the amounts shown for "Planning," "Full Acquisition," and "Operation/Maintenance." The "TOTAL" estimated annual cost of the investment is the sum of costs for "Planning," "Full Acquisition," and "Operation/Maintenance." For Federal buildings and facilities, life-cycle costs should include long term energy, environmental, decommissioning, and/or restoration costs. The costs associated with the entire life-cycle of the investment should be included in this report.

Table 1: SUMMARY OF SPENDING FOR PROJECT PHASES (REPORTED IN MILLIONS)									
(Estimates for BY+1 and beyond are for planning purposes only and do not represent budget decisions)									
	PY-1 and earlier	PY 2008	CY 2009	BY 2010	BY+1 2011	BY+2 2012	BY+3 2013	BY+4 and beyond	Total
Planning:	41.456	13.114	4.11	4.11					
Acquisition:	33.581	12.455	10.55	10.55					
Subtotal Planning & Acquisition:	75.037	25.569	14.66	14.66					
Operations & Maintenance:	46.583	11.252	24.25	24.25					
TOTAL:	121.620	36.821	38.91	38.91					
Government FTE Costs should not be included in the amounts provided above.									
Government FTE Costs	2.13	0.677	0.686	0.861					
Number of FTE represented by Costs:	26	8	8	10					

Note: For the multi-agency investments, this table should include all funding (both managing partner and partner agencies). Government FTE Costs should not be included as part of the TOTAL represented.

2. Will this project require the agency to hire additional FTE's? Yes

a. If "yes," How many and in what year?

Bio Info Sharing 1 FTE For each initiative beginning FY10-14

3. If the summary of spending has changed from the FY2009 President's budget request, briefly explain those changes:

The TSC FY2010 Budget Request demonstrates a shift in resource allocation with a majority of the Information Technology's (IT) budget shifting from planning and acquisition to operations and maintenance as part of the TSC TSS strategy and program maturity. This planned transition of resources from the Developmental and Acquisition stages of the program to Operations and Maintenance contrasts with the FY2009 President's Budget Request as a planned progression of the TSS. Developmental programs continue in support of the Homeland Security Presidential Directive - 11 (HSPD - 11) requiring inclusion of biometrical data to be included in Terrorist Screening Data Base (TSDB) records. Additionally, as part of HSPD-6 and other initiatives, TSC continues to improve its architecture to efficiencies and further effectiveness through Information Sharing initiatives across the TSS both domestically and internationally. To meet these new requirements and evolutionary roles and responsibilities of the TSC, an appropriate amount of the IT budget

remains in planning development.

Section C: Acquisition/Contract Strategy (All Capital Assets)

1. Complete the table for all (including all non-Federal) contracts and/or task orders currently in place or planned for this investment. Total Value should include all option years for each contract. Contracts and/or task orders completed do not need to be included.

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

Contracts/Task Orders Table:																* Costs in millions
Contract or Task Order Number	Type of Contract/ Task Order (In accordance with FAR Part 16)	Has the contract been awarded (Y/N)	If so what is the date of the award? If not, what is the planned award date?	Start date of Contract/ Task Order	End date of Contract/ Task Order	Total Value of Contract/ Task Order (\$M)	Is this an Interagency Acquisition ? (Y/N)	Is it performance based? (Y/N)	Competitively awarded? (Y/N)	What, if any, alternative financing option is being used? (ESPC, UESC, EUL, N/A)	Is EVM in the contract? (Y/N)	Does the contract include the required security & privacy clauses? (Y/N)	Name of CO	CO Contact information (phone/email)	Contracting Officer FAC-C or DAWIA Certification Level (Level 1, 2, 3, N/A)	If N/A, has the agency determined the CO assigned has the competencies and skills necessary to support this acquisition ? (Y/N)
										NA	Yes	Yes				
PO A7G705352	Time-and-Materials	Yes	9/1/2004	9/1/2004	8/31/2009		No	No	No	NA	No	Yes				
PO A61605356	Time-and-Materials	Yes	11/1/2003	11/1/2003	10/31/2008	126.9	No	No	No	NA	No	Yes				
PO S5N0209321	Time-and-Materials	Yes	9/28/2004	9/28/2004	6/30/2008	18.7	No	No	No	NA	No	Yes				

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

2. If earned value is not required or will not be a contract requirement for any of the contracts or task orders above, explain why:

TSC received an OMB waiver and continues the process and procedure agreed to as a result of the June 5, 2006 brief to OMB, DOJ and FBI addressing EVM, ANSI/EIA STD 748, and the TSC's Rational Unified Process (RUP) approach. The agreement from the Office of the CIO, FBI, allowed the TSC to deviate from the ANSI/EIA standard and institute cost accounting RUP measures for managing contract value, while providing specific informative elements necessary for external reporting to the FBI and DOJ.

3. Do the contracts ensure Section 508 compliance? N/A

a. Explain why not or how this is being done? N/A

4. Is there an acquisition plan which reflects the requirements of FAR Subpart 7.1 and has been approved in accordance with agency requirements? Yes

a. If "yes," what is the date? 2/18/2006

1. Is it Current? No

b. If "no," will an acquisition plan be developed?

1. If "no," briefly explain why:

Section D: Performance Information (All Capital Assets)

In order to successfully address this area of the exhibit 300, performance goals must be provided for the agency and be linked to the annual performance plan. The investment must discuss the agency's mission and strategic goals, and performance measures (indicators) must be provided. These goals need to map to the gap in the agency's strategic goals and objectives this investment is designed to fill. They are the internal and external performance benefits this investment is expected to deliver to the agency (e.g., improve efficiency by 60 percent, increase citizen participation by 300 percent a year to achieve an overall citizen participation rate of 75 percent by FY 2xxx, etc.). The goals must be clearly measurable investment outcomes, and if applicable, investment outputs. They do not include the completion date of the module, milestones, or investment, or general goals, such as, significant, better, improved that do not have a quantitative or qualitative measure.

Agencies must use the following table to report performance goals and measures for the major investment and use the Federal Enterprise Architecture (FEA) Performance Reference Model (PRM). Map all Measurement Indicators to the corresponding "Measurement Area" and "Measurement Grouping" identified in the PRM. There should be at least one Measurement Indicator for each of the four different Measurement Areas (for each fiscal year). The PRM is available at www.egov.gov. The table can be extended to include performance measures for years beyond the next President's Budget.

Performance Information Table								
Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
2007	Prevent Terrorism and Promote the Nation's Security	Customer Results	Service Coverage	New Customers and Market Penetration	Increase the number of new foreign customer for information sharing of terrorist watchlist data.			
2007	Prevent Terrorism and Promote the Nation's Security	Mission and Business Results	Intelligence Operations	Intelligence Dissemination	Increase and disseminate of photos of known or suspected terrorists--			
2007	Prevent Terrorism and Promote the Nation's Security	Processes and Activities	Management and Innovation	Innovation and Improvement	Increased photo imports to the TSS database			
2007	Prevent Terrorism and Promote the Nation's Security	Technology	Information and Data	Data Reliability and Quality	Establish an approach to improve TSC data quality.	.Informal methods exist to perform quality measures and corrections.		
2008	Prevent Terrorism and Promote the Nation's Security	Customer Results	Service Coverage	New Customers and Market Penetration	Increase the number of new foreign customer for information sharing of terrorist watchlist data			
2008	Prevent Terrorism and Promote the Nation's Security	Mission and Business Results	Intelligence Operations	Intelligence Dissemination	Increase and disseminate of photos and fingerprints of known or suspected terrorists--			
2008	Prevent Terrorism and Promote the Nation's Security	Processes and Activities	Management and Innovation	Innovation and Improvement	Increase volume of biometric data in the watchlist			

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

Performance Information Table								
Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
2008	Prevent Terrorism and Promote the Nation's Security	Technology	Information and Data	Data Reliability and Quality	Implement and maintain the Data Integrity Officer's Improvement plan			TBD
2009	Prevent Terrorism and Promote the Nation's Security	Customer Results	Service Coverage	New Customers and Market Penetration	Increase the number of new foreign customer for information sharing of terrorist watchlist data			TBD
2009	Prevent Terrorism and Promote the Nation's Security	Mission and Business Results	Intelligence Operations	Intelligence Dissemination				
2009	Prevent Terrorism and Promote the Nation's Security	Processes and Activities	Management and Innovation	Innovation and Improvement	Increased volume of biometric data in terrorist screening data base to support dissemination goals.			TBD
2009	Prevent Terrorism and Promote the Nation's Security	Technology	Information and Data	Data Reliability and Quality	Implement and maintain the Data Integrity Officer's Improvement plan			TBD
2010	Prevent Terrorism and Promote the Nation's Security	Customer Results	Service Coverage	New Customers and Market Penetration	Increase the number of new foreign customer for information sharing of terrorist watchlist data			TBD
2010	Prevent Terrorism and Promote the Nation's Security	Mission and Business Results	Intelligence Operations	Intelligence Dissemination				TBD
2010	Prevent Terrorism and Promote the Nation's Security	Processes and Activities	Management and Innovation	Innovation and Improvement	Increased volume of biometric data in terrorist screening data base to support dissemination goals.			TBD
2010	Prevent Terrorism and Promote the Nation's Security	Technology	Information and Data	Data Reliability and Quality	Implement and maintain the Data Integrity Officer's Improvement plan			TBD
2011	Prevent Terrorism and Promote the Nation's Security	Customer Results	Service Coverage	New Customers and Market Penetration				TBD
2011	Prevent Terrorism and Promote the Nation's Security	Mission and Business Results	Intelligence Operations	Intelligence Dissemination				TBD
2011	Prevent Terrorism and Promote the Nation's Security	Processes and Activities	Management and Innovation	Innovation and Improvement				TBD
2011	Prevent Terrorism and Promote the Nation's Security	Technology	Information and Data	Data Reliability and Quality				TBD
2012	Prevent Terrorism and Promote the Nation's Security	Customer Results	Service Coverage	New Customers and Market Penetration				TBD
2012	Prevent Terrorism and Promote the Nation's Security	Mission and Business Results	Intelligence Operations	Intelligence Dissemination				TBD
2012	Prevent Terrorism and Promote the Nation's Security	Processes and Activities	Management and Innovation	Innovation and Improvement				TBD

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

Performance Information Table								
Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
2012	Prevent Terrorism and Promote the Nation's Security	Technology	Information and Data	Data Reliability and Quality				TBD
2013	Prevent Terrorism and Promote the Nation's Security	Customer Results	Service Coverage	New Customers and Market Penetration				TBD
2013	Prevent Terrorism and Promote the Nation's Security	Mission and Business Results	Intelligence Operations	Intelligence Dissemination				TBD
2013	Prevent Terrorism and Promote the Nation's Security	Processes and Activities	Management and Innovation	Innovation and Improvement				TBD
2013	Prevent Terrorism and Promote the Nation's Security	Technology	Information and Data	Data Reliability and Quality				TBD
2014	Prevent Terrorism and Promote the Nation's Security	Customer Results	Service Coverage	New Customers and Market Penetration				TBD
2014	Prevent Terrorism and Promote the Nation's Security	Mission and Business Results	Intelligence Operations	Intelligence Dissemination				TBD
2014	Prevent Terrorism and Promote the Nation's Security	Processes and Activities	Management and Innovation	Innovation and Improvement				TBD
2014	Prevent Terrorism and Promote the Nation's Security	Technology	Information and Data	Data Reliability and Quality				TBD

Section E: Security and Privacy (IT Capital Assets only)

In order to successfully address this area of the business case, each question below must be answered at the system/application level, not at a program or agency level. Systems supporting this investment on the planning and operational systems security tables should match the systems on the privacy table below. Systems on the Operational Security Table must be included on your agency FISMA system inventory and should be easily referenced in the inventory (i.e., should use the same name or identifier).

For existing Mixed-Life Cycle investments where enhancement, development, and/or modernization is planned, include the investment in both the "Systems in Planning" table (Table 3) and the "Operational Systems" table (Table 4). Systems which are already operational, but have enhancement, development, and/or modernization activity, should be included in both Table 3 and Table 4. Table 3 should reflect the planned date for the system changes to be complete and operational, and the planned date for the associated C&A update. Table 4 should reflect the current status of the requirements listed. In this context, information contained within Table 3 should characterize what updates to testing and documentation will occur before implementing the enhancements; and Table 4 should characterize the current state of the materials associated with the existing system.

All systems listed in the two security tables should be identified in the privacy table. The list of systems in the "Name of System" column of the privacy table (Table 8) should match the systems listed in columns titled "Name of System" in the security tables (Tables 3 and 4). For the Privacy table, it is possible that there may not be a one-to-one ratio between the list of systems and the related privacy documents. For example, one PIA could cover multiple systems. If this is the case, a working link to the PIA may be listed in column (d) of the privacy table more than once (for each system covered by the PIA).

The questions asking whether there is a PIA which covers the system and whether a SORN is required for the system are discrete from the narrative fields. The narrative column provides an opportunity for free text explanation why a working link is not provided. For example, a SORN may be required for the system, but the system is not yet operational. In this circumstance, answer "yes" for column (e) and in the narrative in column (f), explain that because the system is not operational the SORN is not yet required to be published.

Please respond to the questions below and verify the system owner took the following actions:

1. Have the IT security costs for the system(s) been identified and integrated into the overall costs of the investment?:
 - a. If "yes," provide the "Percentage IT Security" for the budget year:
2. Is identifying and assessing security and privacy risks a part Yes of the overall risk management effort for each system supporting or part of this investment?

3. Systems in Planning and Undergoing Enhancement(s), Development, and/or Modernization - Security Table(s):

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

Name of System	Agency/ or Contractor Operated System?	Planned Operational Date	Date of Planned C&A update (for existing mixed life cycle systems) or Planned Completion Date (for new systems)
TSS (TSDB with Biometrics)	Government Only	10/30/2009	8/30/2009
TSS (TSDB/EMA Information Sharing)	Government Only	12/10/2008	10/10/2008

4. Operational Systems - Security Table:

Name of System	Agency/ or Contractor Operated System?	NIST FIPS 199 Risk Impact level (High, Moderate, Low)	Has C&A been Completed, using NIST 800-37? (Y/N)	Date Completed: C&A	What standards were used for the Security Controls tests? (FIPS 200/NIST 800-53, Other, N/A)	Date Completed: Security Control Testing	Date the contingency plan tested
TSS (EMA)	Government Only		Yes		FIPS 200 / NIST 800-53		
TSS (OWTCI)	Government Only		Yes		FIPS 200 / NIST 800-53		
TSS (RQI)	Government Only		Yes		FIPS 200 / NIST 800-53		
TSS (TSCNET)	Government Only		Yes		FIPS 200 / NIST 800-53		
TSS (TSDB-1B)	Government Only		Yes		FIPS 200 / NIST 800-53		

5. Have any weaknesses, not yet remediated, related to any of the systems part of or supporting this investment been identified by the agency or IG?

a. If "yes," have those weaknesses been incorporated into the agency's plan of action and milestone process?

6. Indicate whether an increase in IT security funding is requested to remediate IT security weaknesses?

a. If "yes," specify the amount, provide a general description of the weakness, and explain how the funding request will remediate the weakness.

7. How are contractor security procedures monitored, verified, and validated by the agency for the contractor systems above?

8. Planning & Operational Systems - Privacy Table:

(a) Name of System	(b) Is this a new system? (Y/N)	(c) Is there at least one Privacy Impact Assessment (PIA) which covers this system? (Y/N)	(d) Internet Link or Explanation	(e) Is a System of Records Notice (SORN) required for this system? (Y/N)	(f) Internet Link or Explanation
TSS (EMA)	No	Yes	This is a national security system and therefore not subject to the PIA requirement under Section 208 of the E-Government Act of 2002. As a matter of privacy policy, however, DOJ conducts a PIA on national security systems, but does not publish the PIA due to the sensitive nature of the system.	Yes	Federal Register: August 22,2007 (Volume 72, Number 162)http://edocket.access.gpo.gov/2007/E7-16487.htm
TSS (OWTCI)	No	Yes	This is a national security system and therefore not subject to the PIA requirement under Section 208 of the E-Government Act of 2002. As a matter of privacy policy, however, DOJ conducts a PIA on national security systems, but does not publish the PIA due to the sensitive nature of the system.	Yes	Federal Register: August 22,2007 (Volume 72, Number 162)http://edocket.access.gpo.gov/2007/E7-16487.htm
TSS (RQI)	No	Yes	This is a national security system and therefore not subject to the PIA requirement under Section 208 of the E-	Yes	Federal Register: August 22,2007 (Volume 72, Number 162)http://edocket.access.gpo.gov/2007/E7-

8. Planning & Operational Systems - Privacy Table:					
(a) Name of System	(b) Is this a new system? (Y/N)	(c) Is there at least one Privacy Impact Assessment (PIA) which covers this system? (Y/N)	(d) Internet Link or Explanation	(e) Is a System of Records Notice (SORN) required for this system? (Y/N)	(f) Internet Link or Explanation
			Government Act of 2002. As a matter of privacy policy, however, DOJ conducts a PIA on national security systems, but does not publish the PIA due to the sensitive nature of the system.		16487.htm
TSS (TSCNET)	No	Yes	This is a national security system and therefore not subject to the PIA requirement under Section 208 of the E-Government Act of 2002. As a matter of privacy policy, however, DOJ conducts a PIA on national security systems, but does not publish the PIA due to the sensitive nature of the system.	Yes	Federal Register: August 22, 2007 (Volume 72, Number 162) http://edocket.access.gpo.gov/2007/E7-16487.htm
TSS (TSDB-1B)	No	Yes	This is a national security system and therefore not subject to the PIA requirement under Section 208 of the E-Government Act of 2002. As a matter of privacy policy, however, DOJ conducts a PIA on national security systems, but does not publish the PIA due to the sensitive nature of the system.	Yes	Federal Register: August 22, 2007 (Volume 72, Number 162) http://edocket.access.gpo.gov/2007/E7-16487.htm
Details for Text Options: Column (d): If yes to (c), provide the link(s) to the publicly posted PIA(s) with which this system is associated. If no to (c), provide an explanation why the PIA has not been publicly posted or why the PIA has not been conducted. Column (f): If yes to (e), provide the link(s) to where the current and up to date SORN(s) is published in the federal register. If no to (e), provide an explanation why the SORN has not been published or why there isn't a current and up to date SORN. Note: Working links must be provided to specific documents not general privacy websites. Non-working links will be considered as a blank field.					

Section F: Enterprise Architecture (EA) (IT Capital Assets only)

In order to successfully address this area of the capital asset plan and business case, the investment must be included in the agency's EA and Capital Planning and Investment Control (CPIC) process and mapped to and supporting the FEA. The business case must demonstrate the relationship between the investment and the business, performance, data, services, application, and technology layers of the agency's EA.

1. Is this investment included in your agency's target enterprise architecture? Yes

a. If "no," please explain why?

2. Is this investment included in the agency's EA Transition Strategy? Yes

a. If "yes," provide the investment name as identified in the Transition Strategy provided in the agency's most recent annual EA Assessment. Terrorist Screening System (TSS)

b. If "no," please explain why?

3. Is this investment identified in a completed and approved segment architecture? Yes

a. If "yes," provide the six digit code corresponding to the agency segment architecture. The segment architecture codes are maintained by the agency Chief Architect. For detailed guidance regarding segment architecture codes, please refer to <http://www.egov.gov>. 113-000

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

4. Service Component Reference Model (SRM) Table:								
Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.egov.gov .								
Agency Component Name	Agency Component Description	FEA SRM Service Domain	FEA SRM Service Type	FEA SRM Component (a)	Service Component Reused Name (b)	Service Component Reused UPI (b)	Internal or External Reuse? (c)	BY Funding Percentage (d)
Computers/Automation Management	Support the identification, upgrade, allocation and replacement of physical devices, including servers and desktops, used to facilitate production and process	Back Office Services	Asset / Materials Management	Computers / Automation Management			No Reuse	8
Information Exchange	Define the set of capabilities that support the interchange of information between multiple systems or applications	Back Office Services	Data Management	Data Exchange			No Reuse	5
Data Warehouse	Support the archiving and storage of large volumes of data	Back Office Services	Data Management	Data Warehouse			No Reuse	7
Data Integration	Support the organization of data from separate data sources using middleware or application integration as well as the modification of system data models to capture new information within a single system.	Back Office Services	Development and Integration	Data Integration			No Reuse	9
IT Resource Management	Defines the set of capabilities that support the determination and specification of it assets and management of the relationships/processes. Includes the aggregation of needs and negotiation for favorable discounts from suppliers who provide the necessary IT resources.	Back Office Services	Human Capital / Workforce Management	Resource Planning and Allocation			No Reuse	6
Decision Support and Planning	Defines the set of capabilities that support the analysis of information and predict the impact of decision before they are made.	Business Analytical Services	Business Intelligence	Decision Support and Planning			No Reuse	3
Standard/Canned	Defines the set of capabilities that support the use of pre-conceived or pre-written reports.	Business Analytical Services	Reporting	Standardized / Canned			No Reuse	4
Mapping / Geospatial / Elevation / GPS	Defines the set of capabilities that support the representation of position information through the use of attributes such as elevation,	Business Analytical Services	Visualization	Mapping / Geospatial / Elevation / GPS			No Reuse	2

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

4. Service Component Reference Model (SRM) Table: Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.egov.gov .								
Agency Component Name	Agency Component Description	FEA SRM Service Domain	FEA SRM Service Type	FEA SRM Component (a)	Service Component Reused Name (b)	Service Component Reused UPI (b)	Internal or External Reuse? (c)	BY Funding Percentage (d)
	latitude, and longitude coordinates.							
Requirements Management	Defines the set of capabilities for gathering analyzing and fulfilling the needs and prerequisites of an organization's efforts.	Business Management Services	Management of Processes	Requirements Management			No Reuse	6
Risk Management	Define the set of capabilities for gathering, analyzing and fulfilling the needs and prerequisites of an organization's efforts.	Business Management Services	Management of Processes	Risk Management			No Reuse	7
Content Review and Approval	.Data Integrity Analysis and Corrective actions	Digital Asset Services	Content Management	Content Review and Approval			No Reuse	5
Categorization	Defines the set of capabilities that allow classification of data and information into specific layers or types to support an organization.	Digital Asset Services	Knowledge Management	Categorization			No Reuse	4
Information access	Defines the set of capabilities to support mission information sharing	Digital Asset Services	Knowledge Management	Information Sharing			No Reuse	11
Knowledge Distribution and Delivery	Defines the set of capabilities that facilitate collection of data and information.	Digital Asset Services	Knowledge Management	Knowledge Distribution and Delivery			No Reuse	10
Query	Support retrieval of records that satisfy specific query selection criteria	Support Services	Search	Query			No Reuse	7
Access Provisioning and Authorization	Defines the set of capabilities that support the administration and management of the access rights/privileges.	Support Services	Security Management	Access Control			No Reuse	3
User Identification	Defines the set of capabilities that provide user identification. Identification is the process taken where a user claims their identity (as distinct from authentication where this identification is confirmed as authentic)	Support Services	Security Management	Identification and Authentication			No Reuse	3

a. Use existing SRM Components or identify as "NEW". A "NEW" component is one not already identified as a service component in the FEA SRM.

b. A reused component is one being funded by another investment, but being used by this investment. Rather than answer yes or no, identify the reused service component funded by the other investment and identify the other investment using the

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

Unique Project Identifier (UPI) code from the OMB Ex 300 or Ex 53 submission.

c. 'Internal' reuse is within an agency. For example, one agency within a department is reusing a service component provided by another agency within the same department. 'External' reuse is one agency within a department reusing a service component provided by another agency in another department. A good example of this is an E-Gov initiative service being reused by multiple organizations across the federal government.

d. Please provide the percentage of the BY requested funding amount used for each service component listed in the table. If external, provide the percentage of the BY requested funding amount transferred to another agency to pay for the service. The percentages in the column can, but are not required to, add up to 100%.

5. Technical Reference Model (TRM) Table:
To demonstrate how this major IT investment aligns with the FEA Technical Reference Model (TRM), please list the Service Areas, Categories, Standards, and Service Specifications supporting this IT investment.

FEA SRM Component (a)	FEA TRM Service Area	FEA TRM Service Category	FEA TRM Service Standard	Service Specification (b) (i.e., vendor and product name)
Standardized / Canned	Component Framework	Data Management	Reporting and Analysis	
Query	Component Framework	Data Management	Reporting and Analysis	
Standardized / Canned	Component Framework	Data Management	Reporting and Analysis	
Standardized / Canned	Component Framework	Data Management	Reporting and Analysis	
Mapping / Geospatial / Elevation / GPS	Component Framework	Data Management	Reporting and Analysis	
Mapping / Geospatial / Elevation / GPS	Component Framework	Data Management	Reporting and Analysis	
Query	Component Framework	Data Management	Reporting and Analysis	
Categorization	Component Framework	Data Management	Reporting and Analysis	
Standardized / Canned	Component Framework	Data Management	Reporting and Analysis	
Decision Support and Planning	Component Framework	Data Management	Reporting and Analysis	
Identification and Authentication	Component Framework	Security	Supporting Security Services	
Identification and Authentication	Component Framework	Security	Supporting Security Services	
Identification and Authentication	Component Framework	Security	Supporting Security Services	
Identification and Authentication	Component Framework	Security	Supporting Security Services	
Identification and Authentication	Component Framework	Security	Supporting Security Services	
Access Control	Component Framework	Security	Supporting Security Services	
Query	Service Access and Delivery	Access Channels	Web Browser	
Knowledge Distribution and Delivery	Service Access and Delivery	Delivery Channels	Extranet	
Identification and Authentication	Service Access and Delivery	Service Requirements	Authentication / Single Sign-on	
Resource Planning and Allocation	Service Access and Delivery	Service Requirements	Legislative / Compliance	
Information Sharing	Service Access and Delivery	Service Transport	Supporting Network Services	
Data Integration	Service Interface and Integration	Integration	Enterprise Application Integration	
Information Sharing	Service Interface and Integration	Integration	Enterprise Application Integration	
Knowledge Distribution and Delivery	Service Interface and Integration	Integration	Enterprise Application Integration	
Data Warehouse	Service Interface and Integration	Integration	Enterprise Application Integration	
Requirements Management	Service Interface and Integration	Interface	Service Discovery	
Data Exchange	Service Interface and Integration	Interoperability	Data Format / Classification	
Computers / Automation Management	Service Platform and Infrastructure	Database / Storage	Storage	
Information Sharing	Service Platform and Infrastructure	Delivery Servers	Portal Servers	
Access Control	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	
Risk Management	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	
Content Review and Approval	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	

a. Service Components identified in the previous question should be entered in this column. Please enter multiple rows for FEA SRM Components supported by multiple TRM Service Specifications

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

b. In the Service Specification field, agencies should provide information on the specified technical standard or vendor product mapped to the FEA TRM Service Standard, including model or version numbers, as appropriate.

6. Will the application leverage existing components and/or applications across the Government (i.e., USA.gov, Pay.Gov, etc)? No

a. If "yes," please describe.

Exhibit 300: Part II: Planning, Acquisition and Performance Information

Section A: Alternatives Analysis (All Capital Assets)

Part II should be completed only for investments identified as "Planning" or "Full Acquisition," or "Mixed Life-Cycle" investments in response to Question 6 in Part I, Section A above.

In selecting the best capital asset, you should identify and consider at least three viable alternatives, in addition to the current baseline, i.e., the status quo. Use OMB Circular A-94 for all investments and the Clinger Cohen Act of 1996 for IT investments to determine the criteria you should use in your Benefit/Cost Analysis.

1. Did you conduct an alternatives analysis for this project? Yes
 - a. If "yes," provide the date the analysis was completed?
 - b. If "no," what is the anticipated date this analysis will be completed?
 - c. If no analysis is planned, please briefly explain why:

2. Alternative Analysis Results:			
* Costs in millions			
Use the results of your alternatives analysis to complete the following table:			
Alternative Analyzed	Description of Alternative	Risk Adjusted Lifecycle Costs estimate	Risk Adjusted Lifecycle Benefits estimate
Fusion - Existing FBI-based database & OGA tools			

3. Which alternative was selected by the Agency's Executive/Investment Committee and why was it chosen?

TSC chose Alt #3 over Alt #1 and #2 due to tangible benefits identified, ability to mitigate and buy-down risk, and a higher return on investment apparent during start-up efforts for Initial Operating Capability (IOC) under HSPD directives. This modification of different GOTS software capabilities allowed risk buy-down as well as leveraging previous USG investment of \$29M. The estimated TIPOFF value was \$13.2M cost savings. TSC assumed the following from HLS Institute and RAND papers in its selective calculations: 1) 8 years between terrorist attacks, 2) attack success rate of 50% without mitigation, 3) an estimated TSC mitigation rate of between 5 - 10% between Alternatives, and 4) a USG cost for terrorist attack calculated to be \$28B/event. The TSC goal, in the time allotted by HSPD-6, was to develop a multi-functional instrument providing a centralized point of validation, accountability, responsibility, and exportability to ensure data from various agency sources was accurate, timely and thorough and met security and privacy concerns. TSC viewed the alternative selection process as an evolutionary process to attain IOC, address critical areas, while attaining Full Operating Capability (FOC). Alt #3 met, and continues to, meet those criteria. TSC balanced the immediacy of the requirement, the necessary level of functionality, and the levels of acceptable risk. These risks included attack due to access of known or suspected terrorists (KST), but also likelihood of false identifications of innocent US citizens. TSC market research aimed to meet HSPD goals and objectives as well as determining agencies' best business practices. This initial platform and methodology had to provide the ability to develop new functionality each year for at least five years. The Government Off-The Shelf (GOTS) product (TIPOFF) easily accepts COTS products during incremental development, with cost benefits and manageability over the lifecycle. TSC chose Alt #3 over Alts #1 and #2. For perspective, the TSC's start-up assembled in late Oct 03, organized/implemented within 33 days, and operated with an IOC for a year allowing time/resource investment against the GOTS platform. TSC enacted a sole source acquisition, FBI supported, to conform to Alt #3 under urgent and compelling needs. This acquisition was completed in accordance with provisions outlined by the Federal Acquisition Regulations governing Unusual and Compelling Urgency, and National Security.

a. What year will the investment breakeven? (Specifically, 2004
when the budgeted costs savings exceed the cumulative costs.)

4. What specific qualitative benefits will be realized?

Alt #3 allowed reduction/buy-down risk immediately with an available capability which was both supportable and functional vice alternatives that exposed the Nation to vulnerabilities during developmental and start-up phases. The probable annualized cost of an attack in Baseline is \$1.75B. Alt#3 reduced this to \$1.4B netting with an expected additional annual reduction of \$175M while Alt#1 was \$1.575 and Alt#2 was \$1.4B. Alt#3 gains are realized immediately versus 3 yrs development for Alt#2 leading to an annualized risk reduction of \$175M. TSC successfully consolidated 12 disparate, autonomous databases, with different scope, function, and data points into one overarching entity. TSC surmised that Alt #3 provided a verified product, easier to reverse engineer to meet end-user agency mission requirements as well as technologies. TSC reached a working baseline many supported agencies could leverage. Alt #3 also offered an immediate and responsive level of personnel expertise from/through the Department of State and FBI that far outweighed prototype product or managing costs as presented by Alts #1 or #2. This was immensely important particularly with respect to the TSC's immature infrastructure and the lack of tools necessary to communicate with the partnering agencies and national security efforts. TSC surmised that leveraging existing GOTS with the ability to infuse COTS products where applicable, would decrease costs/lead time over many years. Using personnel knowledgeable in this process and the requirements set forth, allowed for system development accountability in a manner acceptable for the users.

5. Federal Quantitative Benefits
What specific quantitative benefits will be realized (using current dollars) Use the results of your alternatives analysis to complete the following table:

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

	Budgeted Cost Savings	Cost Avoidance	Justification for Budgeted Cost Savings	Justification for Budgeted Cost Avoidance
PY - 1 2007 & Prior				
PY 2008				
CY 2009				
			LCC = Life-cycle Cost	

6. Will the selected alternative replace a legacy system in-part No or in-whole?

a. If "yes," are the migration costs associated with the migration to the selected alternative included in this investment, the legacy investment, or in a separate migration investment?

b. If "yes," please provide the following information:

5b. List of Legacy Investment or Systems		
Name of the Legacy Investment of Systems	UPI if available	Date of the System Retirement

Section B: Risk Management (All Capital Assets)

You should have performed a risk assessment during the early planning and initial concept phase of this investment's life-cycle, developed a risk-adjusted life-cycle cost estimate and a plan to eliminate, mitigate or manage risk, and be actively managing risk throughout the investment's life-cycle.

1. Does the investment have a Risk Management Plan? Yes

a. If "yes," what is the date of the plan?

b. Has the Risk Management Plan been significantly No changed since last year's submission to OMB?

c. If "yes," describe any significant changes:

2. If there currently is no plan, will a plan be developed?

a. If "yes," what is the planned completion date?

b. If "no," what is the strategy for managing the risks?

3. Briefly describe how investment risks are reflected in the life cycle cost estimate and investment schedule:

The TSC measures risk based on the organization's ability to achieve program objectives within defined program requirements and constraints. The TSC identifies and manages risk by use of an internal risk management process, designed to identify critical risks that could adversely impact the program; analyze risks to determine consequences, probability & impact of occurrence, as well as the timeframe during which consequences are likely to occur. The TSC collects program data, reflects the life cycle cost estimates in project reports, and balances both against the risks identified. The TSC process determines the priority of each risk for action, uses the matrix database as the core tool estimates in project reports, and balances these against the risks identified. The process also determines the priority of each risk for action, using the matrix database as the core tool for reporting risks regularly to the proper authorities (i.e. FBI, DOJ), using risk-handling techniques that determine expected effectiveness, and affect technical, operational and programmatic performance. In managing risks, the TSC concluded very low risk is associated with most project activity due to the short life-cycles involved in their development. However, the TSC manages the cost of risk with funding from the organization's management reserve, if a risk should occur that requires additional funds outside of the project budget. Because most systems under development are upgrades to existing systems, the TSC gains in functionality, effectiveness and efficiency with delivery of the new system; with low risks based on schedules. The TSC identifies the risk exposure (cost and schedule), the probability of occurrence, determining the best way to mitigate any issues with the necessary cost reserves. Cost and schedule risk include the probability that shipments will be delayed, equipment will be less costly than originally estimated, product defects, etc. In all, these risks can either be positive or negatives impacts, with the positives viewed as opportunities.

Section C: Cost and Schedule Performance (All Capital Assets)

EVM is required only on DME portions of investments. For mixed lifecycle investments, O&M milestones should still be included in the table (Comparison of Initial Baseline and Current Approved Baseline). This table should accurately reflect the milestones

in the initial baseline, as well as milestones in the current baseline.

1. Does the earned value management system meet the criteria in ANSI/EIA Standard-748?
2. Is the CV% or SV% greater than +/- 10%? (CV%= CV/EV x 100; SV%= SV/PV x 100)
 - a. If "yes," was it the CV or SV or both?
 - b. If "yes," explain the causes of the variance:

As mentioned in section I.C.2 the TSC attributes variances primarily to the amount of time scheduled for each work package, versus the actual schedule due to uncontrollable requirements from internal and/or external sources that force changes to the product delivery timeline. This is the first FY the TSC has assessed true development, maintenance and enhancement costs, based on the actual receipt of product, with the functionality necessary to increase efficiency. The above totals reflect a rollup of multiple FY06 project DME costs.

- c. If "yes," describe the corrective actions:

The TSC is working to develop stronger requirement methods that will not interrupt delivery or product or cause changes in the application development. The organization has implemented the process in FY06 for current and future development. Once requirements are "locked", projects will not accept new changes until delivery for the next iteration.

3. Has the investment re-baselined during the past fiscal year? Yes
 - a. If "yes," when was it approved by the agency head?

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

4. Comparison of Initial Baseline and Current Approved Baseline										
Complete the following table to compare actual performance against the current performance baseline and to the initial performance baseline. In the Current Baseline section, for all milestones listed, you should provide both the baseline and actual completion dates (e.g., "03/23/2003"/ "04/28/2004") and the baseline and actual total costs (in \$ Millions). In the event that a milestone is not found in both the initial and current baseline, leave the associated cells blank. Note that the 'Description of Milestone' and 'Percent Complete' fields are required. Indicate '0' for any milestone no longer active.										
Milestone Number	Description of Milestone	Initial Baseline		Current Baseline				Current Baseline Variance		Percent Complete
		Planned Completion Date (mm/dd/yyyy)	Total Cost (\$M) Estimated	Completion Date (mm/dd/yyyy)		Total Cost (\$M)		Schedule (# days)	Cost (\$M)	
				Planned	Actual	Planned	Actual			
1	TSS (FY08) Acquisitions									
2	TSS (FY08) Network and Engineering Support									
3	TSS (FY08) TSDB Project Management									
4	TSS (FY08) TSDB Requirements									
5	TSS (FY08) TSDB Development									
6	TSS (FY08) TSDB Test									
7	TSS (FY08) EMA Project Management									
8	TSS (FY08) EMA Requirements									
9	TSS (FY08) EMA Development									
10	TSS (FY08) EMA Test									
11	TSS (FY08) ASP Project Management									
12	TSS (FY08) ASP Requirements									
13	TSS (FY08) ASP Development									
14	TSS (FY08) ASP Test									
15	TSS (FY09) Acquisitions									
16	TSS (FY09) Network and Engineering Support									
17	TSS (FY09) TSDB Project Management									
18	TSS (FY09) TSDB Requirements									
19	TSS (FY09) TSDB Development									
20	TSS (FY09) TSDB Test									
21	TSS (FY09) EMA Project Management									
22	TSS (FY09) EMA Requirements									

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

4. Comparison of Initial Baseline and Current Approved Baseline

Complete the following table to compare actual performance against the current performance baseline and to the initial performance baseline. In the Current Baseline section, for all milestones listed, you should provide both the baseline and actual completion dates (e.g., "03/23/2003"/ "04/28/2004") and the baseline and actual total costs (in \$ Millions). In the event that a milestone is not found in both the initial and current baseline, leave the associated cells blank. Note that the 'Description of Milestone' and 'Percent Complete' fields are required. Indicate '0' for any milestone no longer active.

Milestone Number	Description of Milestone	Initial Baseline		Current Baseline				Current Baseline Variance		Percent Complete
		Planned Completion Date (mm/dd/yyyy)	Total Cost (\$M) Estimated	Completion Date (mm/dd/yyyy)		Total Cost (\$M)		Schedule (# days)	Cost (\$M)	
				Planned	Actual	Planned	Actual			
23	TSS (FY09) EMA Development									
24	TSS (FY09) EMA Test									
25	TSS (FY09) ASP Project Management									
26	TSS (FY09) ASP Requirements									
27	TSS (FY09) ASP Development									
28	TSS (FY09) ASP Test									
29	TSS (FY10) Acquisitions									
30	TSS (FY10) Network and Engineering Support									
31	TSS (FY10) TSDB Project Management									
32	TSS (FY10) TSDB Requirements									
33	TSS (FY10) TSDB Development									
34	TSS (FY10) TSDB Test									
35	TSS (FY10) EMA Project Management									
36	TSS (FY10) EMA Requirements									
37	TSS (FY10) EMA Development									
38	TSS (FY10) EMA Test									
39	TSS (FY10) ASP Project Management									
40	TSS (FY10) ASP Requirements									
41	TSS (FY10) ASP Development									
42	TSS (FY10) ASP Test									
43	TSS (FY11) Acquisitions									
44	TSS (FY11) Network and Engineering Support									

Exhibit 300: FBI Terrorist Screening System (TSS) (Revision 5)

4. Comparison of Initial Baseline and Current Approved Baseline

Complete the following table to compare actual performance against the current performance baseline and to the initial performance baseline. In the Current Baseline section, for all milestones listed, you should provide both the baseline and actual completion dates (e.g., "03/23/2003"/ "04/28/2004") and the baseline and actual total costs (in \$ Millions). In the event that a milestone is not found in both the initial and current baseline, leave the associated cells blank. Note that the 'Description of Milestone' and 'Percent Complete' fields are required. Indicate '0' for any milestone no longer active.

Milestone Number	Description of Milestone	Initial Baseline		Current Baseline				Current Baseline Variance		Percent Complete
		Planned Completion Date (mm/dd/yyyy)	Total Cost (\$M) Estimated	Completion Date (mm/dd/yyyy)		Total Cost (\$M)		Schedule (# days)	Cost (\$M)	
				Planned	Actual	Planned	Actual			
89	TSS (FY14) TSDB Development									
90	TSS (FY14) TSDB Test									
91	TSS (FY14) EMA Project Management									
92	TSS (FY14) EMA Requirements									
93	TSS (FY14) EMA Development									
94	TSS (FY14) EMA Test									
95	TSS (FY13) ASP Project Management									
96	TSS (FY14) ASP Requirements									
97	TSS (FY14) ASP Development									
98	TSS (FY14) ASP Test									
Project Totals										