Exhibit 300: Part I: Summary Information and Justification (All Capital Assets)

I.A. Overview

1. Date of Submission:	8/4/2006
2. Agency:	Department of Justice
3. Bureau:	Federal Bureau of Investigation
4. Name of this Capital Asset:	FBI National Crime Information Center (NCIC)
5. Unique Project (Investment) Identifier: (For IT investment only, see section 53. For all other, use agency ID system.)	011-10-01-04-01-2502-00
6. What kind of investment will this be in FY2008? (Please NOTE: Investments moving to O&M ONLY in FY2008, with Planning/Acquisition activities prior to FY2008 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?	FY2001 or earlier

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:

The National Crime Information Center (NCIC) is a computerized criminal justice information system available 24 hours a day, 365 days a year. NCIC is accessed by over 6 million Federal, State, and Tribal entities, including the Department of Homeland Security and the Department of Defense. The NCIC database consists of 18 files, including seven property files and eleven person files. NCIC also contains the Originating Agency Identifier (ORI) file. The NCIC ORI File contains contact information, such as the agency's address and telephone number, for agencies that have an ORI. The NCIC is may also be used to search and retrieve the criminal history records of 50 subjects. The NCIC is considered a Sensitive But Unclassified system and is subject to all DOJ and FBI policy, standards and practices governing the collection and dissemination of SBU data. Access to the NCIC system is controlled at the agency level by ORI. Authorized users are authenticated by user ID and password. Users are also required to be trained and tested on NCIC policy and practices. In order to protect individual privacy, all major changes to the system must undergo a Privacy Impact Assessment. The NCIC is an invaluable tool that aids that aids law enforcement and criminal justice agency officials in the successful completion of their day-to-day operations and protect the United States from terrorist attack. The Terrorist Screening Center enters terrorist information in the Violent Gang and Terrorist Organization File (VGTOF) and maintains the documentation to support the terrorist watchlist. Additionally, the National Counterterrorism Center, the Joint Terrorism Task Forces, and the Field Intelligence Groups have electronic access to NCIC through their respective CJIS System Agency. Federal, State, local and tribal entities may search and retrieve VGTOF, and other person records, electronically by name, and a unique numeric identifier such as date of birth. Records may also be obtained as a result of a query of the Wanted Person File and Stolen Vehicle File. Finally, NCIC will send a notification to the Terrorist Screening Center whenever a fingerprint search results in a hit on a VGTOF record. NCIC is in the operations and maintenance phase of the Life Cycle Management Directive. In FY 2008, the FBI CJIS Division will continue to

upgrade hardware that has reached the end of its life-cycle and add new services such as an enhanced ad hoc search capability.

9. Did the Agency's Executive/Investment Committee approve this request?	Yes
a. If "yes," what was the date of this approval?	5/19/2006
10. Did the Project Manager review this Exhibit?	Yes
11. Contact information of Project Manager?	
Name	
Cuthertson, David	
Phone Number	304-625-2740
Email	dcuthber@leo.gov
12. Has the agency developed and/or promoted cost effective, energy efficient and environmentally sustainable techniques or practices for this project.	No
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?	No
2. If "yes," will this investment meet sustainable design principles?	No
3. If "yes," is it designed to be 30% more energy efficient than relevant code?	
13. Does this investment support one of the PMA initiatives?	Yes
If "yes," check all that apply:	Expanded E-Government
13a. Briefly describe how this asset directly supports the identified initiative(s)?	NCIC is a customer-centered program that provides law enforcement officers, criminal justice administrators, and other individuals with electronic access to the information they need to make decisions and take appropriate actions when interacting with citizens. By providing a single point of access to criminal justice information in the United States, NCIC significantly reduces costs and improves efficiencies for the federal, tribal, state, and local criminal justice agencies.

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 the PART review?	No
b. If "yes," what is the name of the PART program assessed by OMB's Program Assessment Rating Tool?	Criminal Justice Services
c. If "yes," what PART rating did it receive?	Moderately Effective
15. Is this investment for information technology?	Yes
If the answer to Question: "Is this investment for information technology?" was "Yes," complete this sub-section. If the answer is "No," do not answer this sub-section.	
For information technology investments only:	
16. What is the level of the IT Project? (per CIO Council PM Guidance)	Level 2
17. What project management qualifications does the Project Manager have? (per CIO Council PM Guidance):	(4) Project manager assigned but qualification status review has not yet started
18. Is this investment identified as "high risk" on the Q4 - FY 2006 agency high risk report (per OMB's "high risk" memo)?	No
19. Is this a financial management system?	No
a. If "yes," does this investment address a FFMIA compliance area?	No
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 FY2008 funding request for the following? (This should total 100%)	
Hardware	35
Software	17
Services	48

Other	0
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	Kelley, Patrick W
Phone Number	(202) 324-8067
Title	Deputy General Counsel/Senior Privacy Official
E-mail	Patrick.Kelly@ic.fbi.gov
23. Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval?	Yes

I.B. Summary of Funding

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 2006	CY 2007	BY 2008	BY + 1 2009	BY + 2 2010	BY + 3 2011	BY + 4 and Beyond	Total
Planning									
Budgetary Resources	0.438	0.072	0.188	0.216					
Acquisition									

Budgetary Resources	192.263	5.096	6.754	3.31					
Subtotal Planning & Acquisition									
Budgetary Resources	192.701	5.168	6.942	3.526					
Operations & Maintenance									
Budgetary Resources	46.317	6.041	8.594	6.313					
TOTAL									
Budgetary Resources	239.018	11.209	15.536	9.839					
Government FTE Costs									
Budgetary Resources	76.386	14.256	14.534	14.818					
Number of FTE represented by Costs:	936	199	199	199					

Note: For the cross-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? No

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

3. If the summary of spending has changed from the FY2007 President's budget request, briefly explain those changes:

The FBI CJIS Division's spend plan is reviewed and approved by the Division's Information Technology Resources Management (ITRM) Board. The FY 2007 summary of spending represented estimated costs for FY 2008 planning, acquisition and operations and maintenance. The FY 2008 spending plan represents the actual budgeted amounts as approved by the ITRM.

I.C. Acquisition/Contract Strategy

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.

Contracts/Task Orders Table:

Contracts/Task Orders Table

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:

M6D603500 is for maintenance agreements only.

3. Do the contracts ensure Section 508 compliance?	Yes
a. Explain why:	M6D603500 is for maintenance agreements only
4. Is there an acquisition plan which has been approved in accordance with agency requirements?	Yes
a. If "yes," what is the date?	10/1/2005
b. If "no," will an acquisition plan be developed?	
1. If "no," briefly explain why:	

I.D. Performance Information

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 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 Table 1 below for reporting performance goals and measures for all non-IT investments and for existing IT investments that were initiated prior to FY 2005. The table can be extended to include measures for years beyond FY 2006.

Performance Information Table 1:

Fiscal Year	Strategic Goal(s) Supported	Performance Measure	Actual/baseline (from Previous Year)	Planned Performance Metric (Target)	Performance Metric Results (Actual)
2004	1. Protect the United States from terrorist attack. 2. Reduce the impact transnational/national crime enterprises have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a sec	System Response Time	For FY 2003, an average response time of 0.1244 seconds per transaction was achieved/To maintain an average response time less than 0.5 seconds per transaction.	Maintain an average response time less than 0.5 seconds per transaction.	For FY 2004, an average response time of 0.0966 seconds was achieved.

2004	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Transactions	In FY 2003, 1,332,489,509 user support transactions were processed /The baseline is 1,332,489,509 transactions a year	Support an 8.9% increase in user support transactions	In FY 20041,515,134,229 user support transactions were processed for an increase of 182,644,720 transactions.
2004	1. Protect the United States from terrorist attack. 2. Reduce the impact transnational/national crime enterprises have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a sec	System Availability	For FY 2003, NCIC had a 99.66% system availability/The baseline is 99.5% or above.	Maintain 99.5% or above of NCIC system availability	For FY 2004, NCIC had a 99.70% system availability.
2004	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Continuity	For FY 2003, 0% of information systems and networks had business continuity/baseline is 100%	100% of information systems and networks with business continuity.	For FY 2004, 100% of information systems and networks had business continuity.
2005	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	Crime Information Service Availability	In FY 2003, crime information service availability was 99.66%/baseline is 99% crime information service availability.	Maintain crime information service availability at 99% or above.	For FY 2004, crime information service availability was 99.67%
2005	1. Protect the United States from terrorist attack. .	System Response Time	For FY 2004, an average response time of 0.0966	To maintain an average response time less than 0.5	For FY 2005, an average response time of 0.0562

	Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure		seconds per transaction was achieved/To maintain an average response time less than 0.5 seconds per transaction	seconds per transaction.	seconds was achieved.
2005	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Transactions	In FY 2004 1,515,134,229 user support transactions were processed/The baseline is 1,332,489,509 transactions	Support an 8.9% increase in user support transactions	In FY 2005, 1,639,554,366 user support transactions were processed for an increase of 124,420,137 transactions a year.
2005	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Availability	In FY 2004, NCIC had a system availability of 99.70%/ the baseline is 99.5% system availability.	Maintain 99.5% or above of NCIC system availability.	In FY 2005, NCIC had a 99.69% system availability.
2005	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Continuity	In FY 2004, 100% of information systems and networks had business continuity.	Maintain 100% of information systems and networks with business continuity.	In FY 2005, 100% of information systems and networks had business continuity.
2005	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime	Crime Information Service Availability	In FY 2004, crime information service availability was 99.67%/ baseline is 99%.	Maintain crime information service availability at 99% or above.	In FY 2005, crime information service availability was 99.70%.

	enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure				
2006	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Response Time	In FY 2005, an average response time of 0.0562 seconds was achieved/baseline is 0.5 seconds per transaction.	Maintain an average response time less than 0.5 seconds per transaction.	In FY 2006, an average system response time of 0.0541 seconds per transaction was achieved (Oct-May).
2006	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Transactions	In FY 2005,1,639,554,366 user support transaction were processed/ baseline is 1,332,489,509 transaction a year.	Support an 8.9% increase in user support transactions.	In FY 2006, 1,148,671,872 user support transactions were processed (Oct-May).
2006	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Availability	In FY 2005, NCIC had 99.69% system availability/ baseline is 99.5% system availability.	Maintain 99.5% or above of NCIC system availability.	In FY 2006, NCIC had 99.76% system availability (Oct-May).
2006	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase	System Continuity	In FY 2005, 100% of information systems and networks had business continuity/ baseline is 100% information system and network business continuity.	Maintain 100% of information systems and networks with business continuity.	In FY 2006, 100% of information systems and networks had business continuity (Oct-May).

	support to our federal, state, county, municipal, and international partners. 4. Establish a secure				
2006	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	Crime Information Service Availability	In FY 2005, crime information service availability was 99.70% / baseline is 99% crime information service availability.	Maintain crime information service availability at 99% or above.	In FY 2006, crime information service availability was 99.79% (Oct-May).
2007	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Response Time		Maintain an average response time less than 0.5 seconds per transaction.	
2007	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Transactions		Support an 8.9% increase in user support transactions.	
2007	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and	System Availability		Maintain 99.5% or above of NCIC system availability.	

	international partners. 4. Establish a secure				
2007	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Continuity		Maintain 100% of information systems and networks with business continuity.	
2007	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	Crime Information Service Availability		Maintain crime information service availability at 99% or above.	
2008	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Response Time		Maintain an average response time less than 0.5 seconds per transaction	
2008	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Transactions		Support an 8.9% increase in user support transactions	

2008	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Availability		Maintain 99.5% or above of NCIC system availability	
2008	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Continuity		Maintain 100% of information systems and networks with business continuity.	
2008	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	Crime Information Service Availability		Maintain crime information service availability at 99% or above.	
2009	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Response Time		Maintain an average response time less than 0.5 seconds per transaction	
2009	1. Protect the United States from terrorist attack. .	System Transactions		Support an 8.9% increase in user support transactions	

	Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure				
2009	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Availability		Maintain 99.5% or above of NCIC system availability	
2009	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Continuity		Maintain 100% of information systems and networks with business continuity.	
2009	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	Crime Information Service Availability		Maintain crime information service availability at 99% or above.	
2010	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime	System Response Time		Maintain an average response time less than 0.5 seconds per transaction	

	enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure				
2010	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Transactions		Support an 8.9% increase in user support transactions	
2010	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Availability		Maintain 99.5% or above of NCIC system availability	
2010	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Continuity		Maintain 100% of information systems and networks with business continuity.	
2010	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase	Crime Information Service Availability		Maintain crime information service availability at 99% or above	

	support to our federal, state, county, municipal, and international partners. 4. Establish a secure				
2011	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Response Time		Maintain an average response time less than 0.5 seconds per transaction	
2011	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Transactions		Support an 8.9% increase in user support transactions	
2011	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Availability		Maintain 99.5% or above of NCIC system availability	
2011	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and	System Continuity		Maintain 100% of information systems and networks with business continuity.	

	international partners. 4. Establish a secure				
2011	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	Crime Information Service Availability		Maintain crime information service availability at 99% or above	
2012	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Response Time		Maintain an average response time less than 0.5 seconds per transaction	
2012	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Transactions		Support an 8.9% increase in user support transactions	
2012	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Availability		Maintain 99.5% or above of NCIC system availability	

2012	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	System Continuity		Maintain 100% of information systems and networks with business continuity.	
2012	1. Protect the United States from terrorist attack. . Reduce the impact transnational/national crime enterprise have on the United States 3. Increase support to our federal, state, county, municipal, and international partners. 4. Establish a secure	Crime Information Service Availability		Maintain crime information service availability at 99% or above	

All new IT investments initiated for FY 2005 and beyond must use Table 2 and are required to use the Federal Enterprise Architecture (FEA) Performance Reference Model (PRM). Please use Table 2 and the PRM to identify the performance information pertaining to this major IT investment. 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 at least four different Measurement Areas (for each fiscal year). The PRM is available at www.egov.gov.

Performance Information Table 2:

Fiscal Year	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Planned Improvement to the Baseline	Actual Results

I.E. Security and Privacy

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).

All systems supporting and/or part of this investment should be included in the tables below, inclusive of both agency owned systems and contractor systems. For IT investments under development, security and privacy planning must proceed in parallel with the development of the system/s to ensure IT security and privacy requirements and costs are identified and incorporated into the overall lifecycle of the system/s.

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:	Yes
a. If "yes," provide the "Percentage IT Security" for the budget year:	2.50
2. Is identifying and assessing security and privacy risks a part of the overall risk management effort for each system supporting or part of this investment.	Yes

3. Systems in Planning - Security Table:

Name of System	Agency/ or Contractor Operated System?	Planned Operational Date	Planned or Actual C&A Completion Date
National Crime Information Center	Government Only	9/30/2008	8/30/2008

4. Operational Systems - Security Table:

Name of System	Agency/ or Contractor Operated System?	NIST FIPS 199 Risk Impact level	Has C&A been Completed, using NIST 800-37?	Date C&A Complete	What standards were used for the Security Controls tests?	Date Complete(d): Security Control Testing	Date the contingency plan tested
National Crime Information Center	Government Only		Yes	3/29/2005	FIPS 200 / NIST 800-53	5/26/2006	4/19/2006

5. Have any weaknesses 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 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, validated by the agency for the contractor systems above?

8. Planning & Operational Systems - Privacy Table:					
Name of System	**Is this a new system?**	**Is there a Privacy Impact Assessment (PIA) that covers this system?**	**Is the PIA available to the public?**	**Is a System of Records Notice (SORN) required for this system?**	**Was a new or amended SORN published in FY 06?**
National Crime Information Center	No	Yes.	Yes.	Yes	No, because the existing Privacy Act system of records was not substantially revised in FY 06.

I.F. Enterprise Architecture (EA)

In order to successfully address this area of the business case and capital asset plan you must ensure the investment is included in the agency's EA and Capital Planning and Investment Control (CPIC) process, and is mapped to and supports the FEA. You must also ensure the business case demonstrates 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.	National Crime Information Center
b. If "no," please explain why?	

3. Service 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.whitehouse.gov/omb/egov/.								
Agency Component Name	**Agency Component Description**	**Service Domain**	**FEA SRM Service Type**	**FEA SRM Component**	**FEA Service Component Reused Name**	**FEA Service Component Reused UPI**	**Internal or External Reuse?**	**BY Funding Percentage**
		Back Office Services	Data Management	Data Cleansing			No Reuse	0
		Back Office Services	Data Management	Data Exchange			No Reuse	1
		Back Office Services	Data Management	Data Mart			No Reuse	1
		Back Office Services	Data Management	Data Recovery			No Reuse	1
		Back Office Services	Data Management	Data Warehouse			No Reuse	1
		Back Office Services	Data Management	Extraction and Transformation			No Reuse	3
		Back Office Services	Data Management	Loading and Archiving			No Reuse	3
		Business Analytical Services	Reporting	Ad Hoc			No Reuse	7
		Business Analytical Services	Reporting	Standardized / Canned			No Reuse	3
		Business Management Services	Management of Processes	Change Management			No Reuse	1
		Business Management Services	Management of Processes	Configuration Management			No Reuse	3
		Customer Services	Customer Preferences	Alerts and Notifications			No Reuse	2
		Digital Asset Services	Knowledge Management	Categorization			No Reuse	15
		Digital Asset Services	Knowledge Management	Information Mapping / Taxonomy			No Reuse	5

		Digital Asset Services	Knowledge Management	Information Retrieval			No Reuse	5
		Digital Asset Services	Knowledge Management	Information Sharing			No Reuse	15
		Digital Asset Services	Knowledge Management	Knowledge Capture			No Reuse	15
		Digital Asset Services	Knowledge Management	Knowledge Distribution and Delivery			No Reuse	10
		Support Services	Search	Classification			No Reuse	3
		Support Services	Search	Query			No Reuse	3
		Support Services	Security Management	Access Control			No Reuse	0
		Support Services	Security Management	Audit Trail Capture and Analysis			No Reuse	0
		Support Services	Security Management	Identification and Authentication			No Reuse	0

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

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

'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.

Please provide the percentage of the BY requested funding amount used for each service component listed in the table. If external, provide the funding level transferred to another agency to pay for the service.

4. 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	FEA TRM Service Area	FEA TRM Service	FEA TRM Service Standard	Service Specification (i.e. vendor or

		Category		product name)
Data Exchange	Component Framework	Data Interchange	Data Exchange	FBI Developed Software
Information Mapping / Taxonomy	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Information Sharing	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Knowledge Distribution and Delivery	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Ad Hoc	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Standardized / Canned	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Data Exchange	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Data Mart	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Data Warehouse	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Data Cleansing	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Classification	Component Framework	Data Management	Reporting and Analysis	FBI Developed Software
Identification and Authentication	Component Framework	Security	Supporting Security Services	Computer Associates Top Secret
Access Control	Component Framework	Security	Supporting Security Services	Computer Associates Top Secret
Audit Trail Capture and Analysis	Component Framework	Security	Supporting Security Services	Computer Associates Top Secret
Information Retrieval	Service Access and Delivery	Access Channels	Other Electronic Channels	TCP/IP
Knowledge Capture	Service Access and Delivery	Access Channels	Other Electronic Channels	TCP/IP
Information Retrieval	Service Access and Delivery	Delivery Channels	Extranet	TCP/IP
Knowledge Capture	Service Access and Delivery	Delivery Channels	Extranet	TCP/IP
Knowledge Distribution and Delivery	Service Access and Delivery	Delivery Channels	Extranet	TCP/IP
Data Exchange	Service Access and Delivery	Delivery Channels	Extranet	TCP/IP
Information Retrieval	Service Access and Delivery	Service Transport	Service Transport	TCP/IP
Knowledge Capture	Service Access and Delivery	Service Transport	Service Transport	TCP/IP
Data Exchange	Service Interface and Integration	Integration	Middleware	IBM MQ Series
Alerts and Notifications	Service Interface and Integration	Interface	Service Description / Interface	FBI Developed Software
Ad Hoc	Service Interface and Integration	Interface	Service Description / Interface	FBI Developed Software
Standardized / Canned	Service Interface and	Interface	Service Description /	FBI Developed Software

	Integration		Interface	
Query	Service Interface and Integration	Interface	Service Description / Interface	FBI Developed Software
Information Retrieval	Service Interface and Integration	Interoperability	Data Format / Classification	FBI Developed Software
Information Mapping / Taxonomy	Service Interface and Integration	Interoperability	Data Format / Classification	FBI Developed Software
Information Sharing	Service Interface and Integration	Interoperability	Data Format / Classification	FBI Developed Software
Categorization	Service Interface and Integration	Interoperability	Data Format / Classification	FBI Developed Software
Knowledge Capture	Service Interface and Integration	Interoperability	Data Format / Classification	FBI Developed Software
Knowledge Distribution and Delivery	Service Interface and Integration	Interoperability	Data Format / Classification	FBI Developed Software
Data Exchange	Service Interface and Integration	Interoperability	Data Format / Classification	FBI Developed Software
Information Retrieval	Service Interface and Integration	Interoperability	Data Transformation	FBI Developed Software
Information Sharing	Service Interface and Integration	Interoperability	Data Transformation	FBI Developed Software
Data Exchange	Service Interface and Integration	Interoperability	Data Transformation	FBI Developed Software
Information Retrieval	Service Interface and Integration	Interoperability	Data Types / Validation	FBI Developed Software
Information Sharing	Service Interface and Integration	Interoperability	Data Types / Validation	FBI Developed Software
Data Exchange	Service Interface and Integration	Interoperability	Data Types / Validation	FBI Developed Software
Data Mart	Service Platform and Infrastructure	Database / Storage	Database	DB2 v.8
Data Warehouse	Service Platform and Infrastructure	Database / Storage	Database	DB2 v.8
Data Cleansing	Service Platform and Infrastructure	Database / Storage	Database	DB2 v.8
Extraction and Transformation	Service Platform and Infrastructure	Database / Storage	Database	DB2 v.8
Loading and Archiving	Service Platform and	Database / Storage	Database	DB2 v.8

	Infrastructure			
Data Recovery	Service Platform and Infrastructure	Database / Storage	Database	DB2 v.8
Information Mapping / Taxonomy	Service Platform and Infrastructure	Database / Storage	Database	DB2v.8
Information Retrieval	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBM 2105
Knowledge Capture	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBM 2105
Data Mart	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBM 2105
Data Warehouse	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBM 2105
Information Sharing	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBM Z990
Knowledge Capture	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBM Z990
Data Mart	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBM Z990
Data Warehouse	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBM Z990
Information Sharing	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBM2105
Information Retrieval	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	IBMZ990
Information Retrieval	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	STK 9940
Information Sharing	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	STK 9940
Knowledge Capture	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	STK 9940
Data Mart	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	STK 9940
Data Warehouse	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	STK 9940
Change Management	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	ASG Lifecycle Management
Configuration Management	Service Platform and	Software Engineering	Software Configuration	ASG Lifecycle Management

	Infrastructure		Management	

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

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.

5. Will the application leverage existing components and/or applications across the Government (i.e., FirstGov, Pay.Gov, etc)?	No
a. If "yes," please describe.	
6. Does this investment provide the public with access to a government automated information system?	No
a. If "yes," does customer access require specific software (e.g., a specific web browser version)?	
1. If "yes," provide the specific product name(s) and version number(s) of the required software and the date when the public will be able to access this investment by any software (i.e. to ensure equitable and timely access of government information and services).	

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

II.A. Alternatives Analysis

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:

Use the results of your alternatives analysis to complete the following table:

Send to OMB	Alternative Analyzed	Description of Alternative	Risk Adjusted Lifecycle Costs estimate	Risk Adjusted Lifecycle Benefits estimate
True	2	Perform O&M and make major changes to the system every few years.	295.468	862.34

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

The FBI CJIS Division selected alternative two (modular and incremental changes). If the system remained at baseline, the projected growth in workload would exceed system capacity in a few years and new programs and services could not be added. For the O&M, TRDP, and TRP contracts, a government and contractor integrated solution was determined to have the best chance of technical and schedule success.

4. What specific qualitative benefits will be realized?

The purpose of NCIC is provide timely and relevant criminal justice services to the FBI and to authorized law enforcement and criminal justice communities. The key indicators of the benefits of the program are the number of criminals apprehended, the amount of stolen property recovered, the number of fugitives located, and the number of missing persons located. In 2004, the FBI conducted a customer survey to obtain information about the benefits of NCIC to law enforcement. Below are the results of the survey: Persons and Property Apprehended or Found Survey Totals April Estimate 2004 Estimate Apprehended 1,574 26,330 315,963 Missing Persons Found 249 4,165 49,984 Wanted Persons Found 1,577 26,280 316,566 Vehicles Found 1,299 21,730 260,760 Value of Recovered Property Survey Totals April Estimate 2004 Estimate Value of Recovered Contraband $102,589 $1,716,136 $20,593.627 Value of Recovered Vehicles $6,426,765 $107,508,601 $1,290,103,218 Value of Recovered Property $90,842 $1,519,622 $18,235,460 Total Recovered Property $6,620.196 $13,986,618 $1,328,932,305 The benefits to the FBI are system savings, cost avoidance, and improved system performance. System savings are achieved by applying just-in-time acquisitions which reduces maintenance costs. Cost avoidance is achieved by reducing the risk of equipment failure or obsolescence. Improved system performance is achieved through technical refreshment and the employment of new and improved services. However, the benefits to society and to our customers far outweigh the benefits to the FBI. The table below illustrates the benefit value of recovered property.

II.B. Risk Management

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?	6/26/2006
b. Has the Risk Management Plan been significantly changed since last year's submission to OMB?	No
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:

Investment risks are identified through-out the life-cycle of NCIC. A risk mitigation strategy has been developed to maintain system performance, availability, maintainability, and security. The specific hardware, software, and services required to mitigate a specific risk are identified and a request for funding is submitted through the FBI CJIS Information Technology Resources Management (ITRM) Board. The ITRM Board reviews all proposals for CJIS funding and prioritizes each by project by its criticality to CJIS operations and other factors. The available funding is then allocated to projects according to priority and the availability of technical resources. The source of the funding is determined by the Financial Management Unit and is reflected in the FBI Spend Plan. Depending on the type of risk, the strategy chosen to mitigate the risk, and the source of funding, the costs may be reflected within the planning, acquisition, and/or operations and maintenance life cycle costs.

II.C. Cost and Schedule Performance

1. Does the earned value management system meet the criteria in ANSI/EIA Standard-748?	No

2. Answer the following questions about current cumulative cost and schedule performance. The numbers reported below should reflect current actual information. (Per OMB requirements Cost/Schedule Performance information should include both

Government and Contractor Costs):	
a. What is the Planned Value (PV)?	16055
b. What is the Earned Value (EV)?	3210
c. What is the actual cost of work performed (AC)?	3309
d. What costs are included in the reported Cost/Schedule Performance information (Government Only/Contractor Only/Both)?	Contractor and Government
e. "As of" date:	6/23/2006
3. What is the calculated Schedule Performance Index (SPI= EV/PV)?	0.19
4. What is the schedule variance (SV = EV-PV)?	-12845
5. What is the calculated Cost Performance Index (CPI = EV/AC)?	0.97
6. What is the cost variance (CV=EV-AC)?	-99
7. Is the CV% or SV% greater than +/- 10%? (CV% = CV/EV x 100; SV% = SV/PV x 100)	No
a. If "yes," was it the?	
b. If "yes," explain the variance:	
c. If "yes," what corrective actions are being taken?	
d. What is most current "Estimate at Completion"?	
8. Have any significant changes been made to the baseline during the past fiscal year?	No
8. If "yes," when was it approved by OMB?	No

Comparison of Initial Baseline and Current Approved Baseline

Milestone Number	Description of Milestone	Initial Baseline		Current Baseline				Current Baseline Variance		Percent Complete
		Planned Completion Date	Total Cost (Estimated)	Completion Date		Total Cost		Schedule (# days)	Cost	
				Planned	Actual	Planned	Actual			
1	Upgrade NCIC Hardware/Software	09/30/2005	$183.022	09/30/2005	09/30/2005	$315.404	$315.404	0	$0.000	100%
2	Upgrade NCIC Hardware/Software	09/30/2006	$34.531	09/30/2006		$24.554				%
3	Upgrade NCIC Hardware/Software	09/30/2007	$26.532	09/30/2007		$27.390				%
4	Expand and Enhance NCIC Services	09/30/2008	$70.775	09/30/2008		$21.622				%
5										
6										
7										
8										
Project Totals		**09/30/2012**	**$**	**09/30/2012**	**09/30/2005**		**$315.404**	**2557**	**$**	