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:
9/11/2007
2. Agency:
Social Security Administration
3. Bureau:
Systems
4. Name of this Capital Asset:
IT Operations Assurance BY 09
5. Unique Project (Investment) Identifier: (For IT investment only, see section 53. For all other, use agency ID system.)
016-00-02-00-01-2128-00
6. What kind of investment will this be in FY2009? (Please NOTE: Investments moving to O&M in FY2009, with Planning/Acquisition activities prior to FY2009 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?
FY2005
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 IT Operations Assurance (ITOA) project mitigates the internally identified risks associated with single points of failure at the National Computer Center (NCC) by establishing a second, fully functional, co-processing data center located in Durham NC. named the Durham Support Center (DSC). Each center will process a portion of SSA's critical and non-critical workloads. Each center will back up the data assets of the other. In the event of a disaster, one center will assume the critical workloads of the other. The functional center will assume non-critical workloads by expanding pre-staged infrastructure to assume the entire IT requirements currently existing in the NCC.

ITOA will meet the recovery time (RTO) and recovery point objectives (RPO) for critical systems. RTO is the amount of time that will pass before an infrastructure is available. Reducing RTO requires data to be online and available at a failover site. RPO is the point in time that the restarted infrastructure will reflect. Reducing RPO requires increasing synchronicity of data replication. SSA collected and documented these objectives in the April 2004 Disaster Recovery (DR) Business Impact Analysis Report (BIAR) by Lockheed Martin. BIAR established an RTO requirement of 24 hours and a recovery point objective RPO of one hour or less. The Agency cannot currently meet RTO for any critical systems with its' current DR. BIAR reported that the current DR plan does not have the capability to meet acceptable RTO or RPO. BIAR estimated a RTO of multiple weeks if not months at a cost to the Agency of $13.2 million per day. RPO increases in proportion to the RTO.

ITOA provides a series of functional requirements for the DSC that allows the Agency to achieve recovery time and point goals. The plan assumes that the General Services Administration (GSA) is able to make the DSC ready for occupancy in fiscal year 2008. We are using a phased plan aimed at proving new technology before putting it into production at the DSC, allowing us to build critical parts of the new infrastructure within the existing NCC before moving them to the DSC. This approach provides the opportunity to effectively spread costs over multiple fiscal years, maximize the value of new technology, and determine all critical hardware, software, and human resources to ensure failover in both data centers. Each center will viably back up the other, providing an increase in availability.

9. Did the Agency's Executive/Investment Committee approve this request?
Yes
a. If "yes," what was the date of this approval?
7/23/2007
10. Did the Project Manager review this Exhibit?
Yes
11. Removed
a. What is the current FAC-P/PM certification level of the project/program manager?
TBD
12. Has the agency developed and/or promoted cost effective, energy-efficient and environmentally sustainable techniques or practices for this project?
Yes
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
Human Capital
Financial Performance
Budget Performance Integration

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?)

ITOA provides for a higher percentage availability of Government electronic services by elimination of single points of failure. It ensures reliable infrastructure to provide fast services to the public via the Internet and provides the necessary tools to increase productivity and improve job satisfaction, thus developing a high-performing workforce. It provides the ability to reduce the number of erroneous payments and supports the Financial Accounting Systems (FACTS) in the event of disaster.

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.)

No

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

b. If "yes," what is the name of the PARTed program?

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

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. 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 2007 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 FFMIA 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 FY2009 funding request for the following? (This should total 100%)

Hardware

57.370000

Software

0.000000

Services

8.650000

Other

33.980000

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. Removed

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?

No

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)

	PY-1 and earlier	PY 2007	CY 2008	BY 2009
Planning:	0	0	0	0
Acquisition:	5.507	6.735	49.206	4.173
Subtotal Planning & Acquisition:	5.507	6.735	49.206	4.173
Operations & Maintenance:	0	0	2.59	4.173
TOTAL:	5.507	6.735	51.796	8.346
Government FTE Costs	1.012	1.048	2.401	3.361
Number of FTE represented by Costs:	5	10	17	20

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?

No

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

3. If the summary of spending has changed from the FY2008 President's budget request, briefly explain those changes:

ITOA moved the unspent budget for FY 2007 into FY 2008 to reflect the delay in occupying the DSC. GSA could not provide ITOA physical access to a second data center as scheduled (November 2007) in the FY 2008 President's budget request. GSA and the lessor encountered delays in obtaining the required permits to begin construction. ITOA's project manager (PM) worked closely with GSA and the lessor to resolve permit problems, and they have provided SSA with a schedule that indicates that we will have limited access to the second data center in the spring of 2008, and a certificate of occupancy in October of 2008. This represented a major change to the overall project cost and schedule plans. ITOA's PM is monitoring construction progress. He is working closely with GSA and the lessor to insure that no avoidable delays occur in the future.

SSA has used the delay to perform much of the testing originally scheduled to occur at the DSC in the NCC. NCC testing is less costly to the project because there is a pre-established testing environment and no additional travel costs for specialized technicians are required. ITOA is also using these delays to pre-configure equipment for rapid installation once access to the DSC is available. Pre-configured equipment is also less costly, for the same reasons as listed above. Performing testing in the NCC and pre-configuring equipment allows ITOA to compress the schedule in calendar year 2008 and 2009 to avoid extending the project completion date. The original life-cycle cost of the project will remain the same.

ITOA has deferred purchasing equipment we cannot pre-configure for the DSC planned for FY 2007 until FY 2008. SSA could have funded hardware acquisitions with FY 2007 funds for delivery to the second data center (as originally planned). However, purchasing equipment at this time for future delivery to the second data center represents a technological risk to the Agency. The current schedule estimates that SSA will not gain access to DSC until mid to late FY 2008, and much of the equipment purchased in FY 2007 would be approaching its' useable half-life, or near technological obsolescence by the time SSA took delivery.

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.

Contracts/Task Orders Table:

Contract or Task Order Number	Type of Contract / Task Order	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)
FTS2001	Firm Fixed Price	Yes	1/1/2001	1/1/2008	10/1/2011	13.889	No	Yes	Yes	NA	No	Yes

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:

SSA's earned value management (EVM) policy and implementation has been reviewed by OMB, OIG and others and deemed consistent with OMB guidance and the ANSI standards defining a compliant EVM. SSA performs the vast majority of our work in-house, and conducts EVM and program management at the total program level including both Government costs and support contracts. The inclusion of earned value in SSA contracts is based on the type of contract let, the services performed, and the date when the contract was let. When applicable, earned value management requirements are applied to SSA contractors in two ways. The first is to require the contractor to satisfy requirements utilizing their own earned value management system (EVMS). The second is for the contractor to provide necessary data directly into SSA's in-house EVMS.

The supply contracts listed in the above table generally have little or no Development, Modernization or Enhancement (DME) components, and therefore do not warrant the inclusion of a separate contractor EVMS. These contracts maybe subject (as applicable, based on DME content, risk and other policy factors) to SSA EVMS. Required EVM data is furnished by the contractor and included within the program level EVM.

3. Do the contracts ensure Section 508 compliance?

Yes

a. Explain why:

SSA ensures that any applicable IT requirements comply with Section 508 standards. The SSA includes Section 508 contract clauses and evaluation criteria in its solicitations and contracts as appropriate and ensures during the review of technical proposals that offerors are fully compliant or as compliant as possible based on the state of the technology in the marketplace. This is accomplished through review of technical documentation as well as through actual testing of the product.

4. Is there an acquisition plan which has been approved in accordance with agency requirements?

Yes

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

9/7/2007

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 FY 2009.

Performance Information Table

Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
2008	Service - To deliver high-quality, citizen-centered service	Customer Results	Service Quality	Accuracy of Service or Product Delivered	Percent of original Social Security Numbers issued that are free of critical error	FY 2007 Estimated -98%	95%	Actual results available in March 2008
2008	Service - To deliver high-quality, citizen-centered service	Mission and Business Results	Disaster Management	Disaster Repair and Restore	Hours needed to restore critical systems (Recovery Time)	80 hours	60 hours	Actual results available in 2009
2008	Stewardship - To ensure superior stewardship of Social Security programs and resource	Processes and Activities	Cycle Time and Resource Time	Cycle Time	Percent of Social Security Number receipts processed up to the budgeted level	FY 2007 Actual – (17,280,000)	96% (18,240,000)	Actual results available in 2009
2008	Stewardship - To ensure superior stewardship of	Technology	Reliability and Availability	Reliability	Hours of lost transactions (Recovery Point)	16 hours	8 hours	Actual results available in 2009

Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
	Social Security programs and resource							
2009	Service - To deliver high-quality, citizen-centered service	Customer Results	Service Quality	Accuracy of Service or Product Delivered	Percent of original Social Security Numbers issued that are free of critical error	Estimated 95%	95%	Available in 2009
2009	Service - To deliver high-quality, citizen-centered service	Mission and Business Results	Disaster Management	Disaster Repair and Restore	Hours needed to restore critical systems (Recovery Time)	60 hours	40 hours	Actual results available in 2010
2009	Service - To deliver high-quality, citizen-centered service	Mission and Business Results	Workforce Management	Labor Rights Management	Provide off loading capablity of Help desk services at the NCC to the DSC	24 hour availability	Provide 24 hr staffing	Available in 2010
2009	Stewardship - To ensure superior stewardship of Social Security programs and resource	Processes and Activities	Cycle Time and Resource Time	Cycle Time	Percent of Social Security Number receipts processed up to the budgeted level	FY 2008 target (18,240,000) 96%	96% (19,200,000)	Actual results available in 2010
2009	Stewardship - To ensure superior stewardship of Social Security programs and resource	Technology	Reliability and Availability	Availability	Hours of lost transactions (Recovery Point)	8 hours	2 hours	Actual results available in 2010

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:

Yes

a. If "yes," provide the "Percentage IT Security" for the budget year:

removed

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 and Undergoing Enhancement(s), Development, and/or Modernization - Security Table(s):

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)
Enterprise Wide Area Network and Services System	Contractor and Government	9/8/2008	09/08/2008

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 Complete(d): Security Control Testing	Date the contingency plan tested
Enterprise Wide Area Network andServices System	Government Only	Moderate	Yes	7/18/2006	FIPS 200 / NIST 800-53	7/13/2007	1/18/2007

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?
No

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?
No

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?
This is not a contractor system.

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
Enterprise Wide Area Network and Services System	No	No	The system does not contain, process, or transmit personal identifying information.	No	The system is not a Privacy Act system of records.
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.

b. If "no," please explain why?

3. Is this investment identified in a completed (contains a target architecture) and approved segment architecture?
Yes

a. If "yes," provide the name of the segment architecture as provided in the agency's most recent annual EA Assessment.
Infrastructure

4. Service Component Reference Model (SRM) Table:

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)
SFA	Sunflower Asset System is the COTS package used to manage SSA physical assets.	Back Office Services	Asset / Materials Management	Property / Asset Management	Property / Asset Management	016-00-01-01-02-2129-00	Internal	0
RAID, RMF	Redundant Array of Independent Disks. This disk subsystem architecture uses multiple hard drives to write data to achieving redundancy and enhancing fault resilience. RMF (Resource Measurement Facility) operates exclusively on IBM's Multiple Virtual Space (MVS) operating systems. RMF measures performance, utilization, resource consumption, and workload levels for MVS systems.	Back Office Services	Data Management	Data Recovery	Data Recovery	016-00-02-00-01-2210-00	Internal	0
PA I/O Driver	Performance Associates software used to generate transaction traffic in an effort to simulate higher volume workloads for testing of throughput thresholds.	Back Office Services	Development and Integration	Instrumentation and Testing	Instrumentation and Testing	016-00-02-00-01-2210-00	Internal	0
DMA	Document Management Architecture and ORS which is the Online Retrieval System (ORS) that provides the ability to view any notice that has been sent to a customer. ORS also stores the notices in an exact image of the original, thus allowing SSA to adhere to Federal regulations on retention of documents, and move closer to an efficient, paperless	Business Analytical Services	Visualization	Imagery	Imagery	016-00-02-00-01-2210-00	Internal	0

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)
	environment.							
QA2	QA2 enforces the completion of an System Release Certification through its interface with the online and batch release processes.	Business Management Services	Management of Processes	Configuration Management	Configuration Management	016-00-01-04-02-2132-00	Internal	0
Omegamon	IBM Tivoli Monitoring is an enterprise-class, easy-to-use solution that optimizes the performance and availability of your entire IT infrastructure. Through a single customizable workspace portal, you can proactively manage the health and availability of your IT infrastructure, end-to-end, including operating systems, databases and servers, across distributed and host environments.	Business Management Services	Organizational Management	Network Management	Network Management	016-00-02-00-01-2210-00	Internal	0
SSASy	SSA's Streamlined Acquisition System (SSASy) is a paperless, electronic tool used to prepare, submit and process purchase requests.	Business Management Services	Supply Chain Management	Ordering / Purchasing	Ordering / Purchasing	016-00-01-01-02-2129-00	Internal	0
FECS	The Front-End Capture System (FECS) is the software used to provide the front-end capture capabilities needed to process unstructured data.	Digital Asset Services	Document Management	Document Imaging and OCR	Document Imaging and OCR	016-00-02-00-01-2210-00	Internal	0
Nokia and Netscreen Firewalls, VPN	Virtual Private Networking (VPN) is a facility that allows a user to access SSA's mainframe computers, Local Area Networks, or e-mail from a remote location. Firewalls are specially-fortified hosts which sit between two networks and control access from one network to another via a set of rules.	Support Services	Security Management	Access Control	Access Control	016-00-02-00-01-2210-00	Internal	0
S/MIME	S/MIME is a public key	Support Services	Security Management	Access Control	Access Control	016-00-02-00-01-2210-00	Internal	0

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)
	encryption protocol for securely sending Multi-purpose Internet Mail Extension (MIME) attachments. eTrust SSO provides internal SSA end users a login option (leveraging Microsoft Active Directory login) that allows them to more effectively manage UserIDs and passwords for multiple applications (Internet, Intranet and/or CISC) - each one with unique sign-on requirements.							
eTrust	eTrust SSO provides internal SSA end users a login option (leveraging Microsoft Active Directory login) that allows them to more effectively manage UserIDs and passwords for multiple applications (Internet, Intranet and/or CISC) - each one with unique sign-on requirements.	Support Services	Security Management	Access Control	Access Control	016-00-02-00-01-2210-00	Internal	0
SSL	Secure Sockets Layer (SSL) is a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data - a public key known to everyone and a private or secret key known only to the recipient of the message.	Support Services	Security Management	Cryptography	Cryptography	016-00-01-04-02-2132-00	Internal	0
Top Secret	TOP SECRET is the security software running on all of SSA's mainframe systems.	Support Services	Security Management	Identification and Authentication	Identification and Authentication	016-00-02-00-01-2210-00	Internal	0
Radia	Radia software to enables remote automated updating and maintenance of software across a large number of computers.	Support Services	Systems Management	License Management	License Management	016-00-02-00-01-2210-00	Internal	0
SSASy	SSA's Streamlined	Support Services	Systems Management	License Management	License Management	016-00-01-01-02-2129-00	Internal	0

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)
	Acquisition System (SSASy) is a paperless, electronic tool used to prepare, submit and process purchase requests.							
Omegamon, Directory Services	IBM Tivoli Monitoring is an enterprise-class, easy-to-use solution that optimizes the performance and availability of your entire IT infrastructure. Through a single customizable workspace portal, you can proactively manage the health and availability of your IT infrastructure, end-to-end, including operating systems, databases and servers, across distributed and host environments.	Support Services	Systems Management	Remote Systems Control	Remote Systems Control	016-00-02-00-01-2210-00	Internal	0
Radia	Radia software to enables remote automated updating and maintenance of software across a large number of computers.	Support Services	Systems Management	Software Distribution	Software Distribution	016-00-02-00-01-2210-00	Internal	0
Omegamon	IBM Tivoli Monitoring is an enterprise-class, easy-to-use solution that optimizes the performance and availability of your entire IT infrastructure. Through a single customizable workspace portal, you can proactively manage the health and availability of your IT infrastructure, end-to-end, including operating systems, databases and servers, across distributed and host environments.	Support Services	Systems Management	System Resource Monitoring	System Resource Monitoring	016-00-02-00-01-2210-00	Internal	0

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 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:

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)
Configuration Management	Component Framework	Business Logic	Platform Dependent	Visual Basic .Net (VB.Net)
Configuration Management	Component Framework	Data Management	Database Connectivity	Active Data Objects .Net (ADO.Net)
Imagery	Component Framework	Data Management	Database Connectivity	Java Database Connectivity (JDBC)
Configuration Management	Component Framework	Data Management	Database Connectivity	Open Database Connectivity (ODBC)
Configuration Management	Component Framework	Presentation / Interface	Dynamic Server-Side Display	Active Server Pages .Net (ASP.Net)
Document Imaging and OCR	Component Framework	Security	Supporting Security Services	Secure Multipurpose Internet Mail Extensions (S/MIME)
Access Control	Component Framework	Security	Supporting Security Services	Secure Multipurpose Internet Mail Extensions (S/MIME)
Identification and Authentication	Component Framework	Security	Supporting Security Services	TopSecret
Document Imaging and OCR	Component Framework	Security	Supporting Security Services	Transport Layer Security (TLS)
Document Imaging and OCR	Service Access and Delivery	Access Channels	Collaboration / Communications	Electronic Mail (E-mail)
Document Imaging and OCR	Service Access and Delivery	Access Channels	Collaboration / Communications	Facsimile (Fax)
Access Control	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System
Instrumentation and Testing	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System
Imagery	Service Access and Delivery	Access Channels	Other Electronic Channels	Web Service
Imagery	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Document Imaging and OCR	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Remote Systems Control	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Access Control	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Intrusion Detection	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
System Resource Monitoring	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Instrumentation and Testing	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Configuration Management	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
License Management	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Software Distribution	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Identification and Authentication	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Network Management	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Property / Asset Management	Service Access and Delivery	Service Requirements	Hosting	Internal (within Agency)
Access Control	Service Access and Delivery	Service Requirements	Legislative / Compliance	Security
Identification and Authentication	Service Access and Delivery	Service Requirements	Legislative / Compliance	Security
Document Imaging and OCR	Service Access and Delivery	Service Transport	Service Transport	File Transfer Protocol (FTP)
Document Imaging and OCR	Service Access and Delivery	Service Transport	Supporting Network Services	Multipurpose Internet Mail Extensions (MIME)
Document Imaging and OCR	Service Access and Delivery	Service Transport	Supporting Network Services	Simple Mail Transfer Protocol (SMTP)
Identification and Authentication	Service Interface and Integration	Integration	Middleware	CICS
Imagery	Service Platform and Infrastructure	Database / Storage	Database	Content Manager
Ordering / Purchasing	Service Platform and Infrastructure	Delivery Servers	Application Servers	
License Management	Service Platform and Infrastructure	Delivery Servers	Application Servers	
Cryptography	Service Platform and Infrastructure	Delivery Servers	Application Servers	
Property / Asset Management	Service Platform and Infrastructure	Delivery Servers	Application Servers	
Property / Asset Management	Service Platform and Infrastructure	Delivery Servers	Application Servers	
Ordering / Purchasing	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Hard Disk Drive
License Management	Service Platform and	Hardware / Infrastructure	Embedded Technology Devices	Hard Disk Drive

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)
	Infrastructure			
Cryptography	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Hard Disk Drive
Property / Asset Management	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Hard Disk Drive
Property / Asset Management	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Hard Disk Drive
Data Recovery	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Redundant Array of Independent Disks (RAID)
Intrusion Detection	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Firewall
Imagery	Service Platform and Infrastructure	Hardware / Infrastructure	Peripherals	Direct Access Storage Device (DASD)
Instrumentation and Testing	Service Platform and Infrastructure	Hardware / Infrastructure	Peripherals	Direct Access Storage Device (DASD)
Identification and Authentication	Service Platform and Infrastructure	Hardware / Infrastructure	Peripherals	Direct Access Storage Device (DASD)
Identification and Authentication	Service Platform and Infrastructure	Hardware / Infrastructure	Peripherals	Mainframe
Document Imaging and OCR	Service Platform and Infrastructure	Hardware / Infrastructure	Peripherals	Scanner
Remote Systems Control	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Enterprise Server
Access Control	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Enterprise Server
System Resource Monitoring	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Enterprise Server
License Management	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Enterprise Server
Software Distribution	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Enterprise Server
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Enterprise Server
Remote Systems Control	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Mainframe
System Resource Monitoring	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Mainframe
Instrumentation and Testing	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Mainframe
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Mainframe
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Wide Area Network (WAN)	Frame Relay
Instrumentation and Testing	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Configuration Testing
Instrumentation and Testing	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Installation Testing
Instrumentation and Testing	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Load/Stress/Volume Testing
Instrumentation and Testing	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Performance Profiling
Instrumentation and Testing	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Reliability Testing
Imagery	Service Platform and Infrastructure	Support Platforms	Platform Independent	Java 2 Platform Enterprise Edition (J2EE)

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

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., FirstGov, Pay.Gov, etc)?

No

a. If "yes," please describe.

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?

6/30/2004

b. If "no," what is the anticipated date this analysis will be completed?

c. If no analysis is planned, please briefly explain why:

2. Removed

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

The Dual Site, Phased alternative was chosen based on a Cost Effectiveness Analysis (CEA) and current and anticipated funding availability. The CEA measured functional, interface, performance and facilities requirements, alternative attributes including staffing losses, operational complexity, operational efficiency and outage coverage and resources. Each evaluation criteria was prioritized and ranked, and each alternative was scored. The SSA Owned Hot Site alternative scored 114 and the SSA Owned Dual Site scored 161. Given the high cost and level of redundancy of the Dual Site alternative, a third alternative, Dual Site, Phased, was developed.

The Dual Site, Phased alternative was chosen because of its high relative CEA score and its lower relative cost. A phased approach will spread costs over multiple years, but will phase in risk mitigation as well. The key factor in deciding on a phased approach was the agency's ability to take advantage of emerging new technologies that will increase capabilities while reducing the costs of data storage and transmission.

4. What specific qualitative benefits will be realized?

OMB Circular A-94 and the Federal CIO Council 1999 study, "ROI and the Value Puzzle" indicate the usefulness of a Cost Effectiveness Analysis (CEA) when federal policy require a specific service or when the alternatives yield the same annual effect. Given the specific requirements of Homeland Security Presidential Declaration 7 concerning the protection of critical infrastructure assets, we believe a Cost Effectiveness Analysis is useful. The CEA for this investment clearly shows the relative value of the chosen alternative.

In addition, a Return on Investment study was performed for this investment. However, given that this investment only shows tangible benefits in the event of a disaster, the ROI is based upon the assumption that a disaster occurs that renders SSA's National Computer Center inaccessible and unusable for a period of 10 days. This is the most likely, medium risk scenario based on the findings of the Deloitte risk assessment, and would result from biological or chemical contamination of the building. Disasters scenarios with more serious consequences could be constructed that would indicated a significantly higher return on investment.

The ROI based on the 10 day outage assumption is 114.2. The ROI is calculated only using lost productivity and the costs to the agency of working off backlogs associated with a NCC outage, and not the costs of replacing any equipment or physical plant that might be damaged as a consequence of the disaster.

Additional tangible benefits may accrue from the termination of current disaster recovery facility contracts and the repositioning of infrastructure assets from disaster recovery use to production use.

Additional intangible benefits include operational continuity during severe weather events, the opportunity to provide true 24x7 service to the public via the Internet, and expanded hours of systems availability, including improved access for Foreign Service Posts. By splitting the IT infrastructure, benefits also accrue in the area of performance management as problems affecting one facility's computing environment are unlikely to affect the other. Finally, with planned IT infrastructure expansions occurring in two locations, operational risks are mitigated by placing new infrastructure in two different locations at no additional cost.

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

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:

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?
7/2/2007

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:
The investment's phased implementation reflects a life cycle cost spread over several years. The project's primary risk dependency is the occupation of the DSC. Until ITOA can begin the initial stocking and installation of equipment at the DSC, the only costs to the project are FTE costs for planning and testing, with minor IT purchases to support proof of concept efforts. Therefore, the ITS budget at project completion is not be significantly affected by minor delays to DSC occupation. Historically, ITOA has responded to delays in occupying the DSC by re-scheduling budgets for individual years to reflect those delays.

ITOA recognizes that occupation of a second data center is a critical milestone and represented a major risk to the project. ITOA formulated a contingency plan that would allow the project to move forward and position itself for a later occupancy date than planned. ITOA designed the contingency plan to minimize risk to the project and the Agency, while accomplishing verifiable milestones that are not dependent on the occupation of a second data center.

ITOA is now implementing that plan, and intends to gain access to the DSC for initial stocking and installation of equipment early in the third quarter of FY 2008. ITOA will test the internal IT cabling, the stability of the electrical systems, the back up power, the telecommunications and network infrastructure, the physical security systems, and install the IT equipment to meet the specific mission of ITOA. ITOA will begin transferring live workloads to the DSC in the fourth quarter of FY 2008. FY 2009 and 2010 will include the phased transfer of additional workloads and personnel into the DSC. FY 2011 will feature the final transition on planned workloads along with the establishment of a fully functional, stabilized infrastructure that is capable of serving as an alternate processing center for SSA's IT requirements.

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?

Yes

2. 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 CV or SV or both?

b. If "yes," explain the causes of the variance:

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

The acquisition schedule was adjusted to account for the delay in determining the second data center's location.

3. Has the investment re-baselined during the past fiscal year?

Yes

a. If "yes," when was it approved by the agency head?

4. Removed

9/5/2007