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:	9/10/2007
2. Agency:	Department of State
3. Bureau:	Irm/Ops/Mso/Eml E-Mail
4. Name of this Capital Asset:	Exhibit 300 - E-Mail Operations
5. Unique Project (Investment) Identifier: (For IT investment only, see section 53. For all other, use agency ID system.)	014-00-01-04-01-1090-00
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.)	Operations and Maintenance

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 E-Mail Operations Division (EML) provides a quality e-mail system to the Department of State's (DoS) 47,000 employees worldwide. EML operates and maintains (O&M) three 7x24 facilities to support its mission; the Network Control Center (NCC); the Combined Bureau Processing Center (CBPC); and Firewall Operations. EML also operates the Remote Access (RA) operations on a 7x16 basis. EML manages the Microsoft Premier Support Services contract for the Department.

EML supports new programs being implemented within the DoS by providing the development efforts for new requirements for programs such as the State Messaging Archival Retrieval Tool (SMART), ONE (OpenNet Everywhere), OpenNet+, and the Open Source Information System (OSIS). EML supports several projects that are either still in development or transitioning from development to O&M such as Windows 2000/2003 Migrations, Exchange 2000/2003 Migration, Disaster Recovery, and Public Key Infrastructure (PKI) initiatives along with numerous monitoring enhancements. EML provides Microsoft Exchange and Network Security subject matter expertise and operational world-wide E-Mail routing capability.

9. Did the Agency's Executive/Investment Committee approve this request?	Yes
a. If "yes," what was the date of this approval?	8/28/2007
10. Did the Project Manager review this Exhibit?	Yes
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?	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 directly support one of the PMA initiatives?	Yes
If "yes," check all that apply:	Expanded E-Government Competitive Sourcing Right Sized Overseas Presence

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?	No
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 2
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)	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:	N/A
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

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
23. Are the records produced by this investment appropriately scheduled with the National Archives and Records Administration's approval?	No

Question 24 must be answered by all Investments:

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
2005	Strengthening Consular and Management Capabilities	Customer Results	Service Accessibility	Availability	Time to restore access to corporate unclassified network resources and applications from non-DoS locations	Single instance of each system at one physical site; no redundancy or failover capability.	Implement additional redundant hot sites at other IRM core processing facilities (e.g., BIMC, ACS).	In process of adding a secondary physical site within five miles of primary site for limited redundancy and failover.
2005	Strengthening	Mission and	Internal Risk	Contingency	Decrease the	Less than 5% of	Less than 4%	To date no

Performance Information Table

Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
	Consular and Management Capabilities	Business Results	Management and Mitigation	Planning	number of Internet virus/worm traffic against internal/users network.	Internet virus/worm traffic impacts internal network/users	Internet virus/worm traffic impacts internal network/users	major Internet virus/worm has impacted the internal network/users since September 2003
2005	Strengthening Consular and Management Capabilities	Processes and Activities	Security and Privacy	Security	Security - Percent of network availability after primary site failure on classified network	100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites; 0% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	Maintain 100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites; Increase to 2% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	No funding provided to build redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.
2005	Strengthening Consular and Management Capabilities	Technology	Reliability and Availability	Availability	Availability - time to restore access to corporate email resources and applications	100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites; 0% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	Maintain 100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites; Increase to 2% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	No funding provided to build redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.
2006	Strengthening Consular and Management Capabilities	Customer Results	Timeliness and Responsiveness	Delivery Time	Responsiveness - Percent of network availability after primary site failure	100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites (60% of Email sites); 0% redundant EML infrastructure and support for routing to alternate location for Exchange 2000 sites (40% of Email sites	Maintain 100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites; Increase to 2% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	End of FY06, EML identified funding (outside of base) and location for ClassNet Exchange 2000/2003 operations. FY06, EML had deployed and made operational Unclassified/SBU Exchange 2000/2003 operations & DR. EML provided O&M for Exchange 5.5 & DR.
2006	Strengthening Consular and Management Capabilities	Mission and Business Results	Information and Technology Management	Information Systems Security	IT Infrastructure Maintenance - Percentage of malicious attacks against internal networks defeated.	Less than 5% of Internet virus/worm traffic impacts internal network/users	Maintain less than 3.5% Internet virus/worm traffic impacts internal network/users	To date no major Internet virus/worm has impacted the internal network/users since September 2003. EML worked with other elements of IRM to mitigate the effects of a Cyber attack that occurred in June, 2006.
2006	Strengthening Consular and Management Capabilities	Processes and Activities	Security and Privacy	Security	Security - Percent of network availability after primary site	100% redundant email infrastructure and support for routing to	Maintain 100% redundant email infrastructure and support for routing to	End of FY06, EML identified funding (outside of base) and location for

Performance Information Table

Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
					failure on classified network	alternate location for Exchange 5.5 sites (35% of Email sites); 0% redundant EML infrastructure and support for routing to alternate location for Exchange 2000 sites (65% of Email sites	alternate location for Exchange 5.5 sites; Increase to 2% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	ClassNet Exchange 2000/2003 DR operations. EML provided O&M for ClassNet Exchange 5.5 & DR.
2006	Strengthening Consular and Management Capabilities	Technology	Reliability and Availability	Availability	Reliability - increase the availability of hot sites for remote access	Single instance of each system at one physical site; no redundancy or failover capability.	Implement additional redundant hot sites at other IRM core processing facilities (e.g., BIMC, ACS).	No funding in base for redundant hot sites. At the end of FY06, EML identified funding (outside base) and location for redundant ClassNet hot site for Exchange 2000/2003 email routing. FY 06, EML had made operational OpenNet hot site for routing.
2007	Strengthening Consular and Management Capabilities	Customer Results	Timeliness and Responsiveness	Delivery Time	Responsiveness - Percent of network availability after primary site failure	100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites (<10% of email sites); 0% redundant EML infrastructure and support for routing to alternate location for Exchange 2000/2003 sites (>90% of sites)	Maintain 100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites; Increase to 2% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	Met Target. EML has operated and maintained OpenNet & ClassNet Exchange 5.5/2000/2003 operations. For ClassNet and OpenNet, alt site routing is in place for 2000/2003. OpenNet alt site routing for 5.5 was retired.
2007	Strengthening Consular and Management Capabilities	Mission and Business Results	Internal Risk Management and Mitigation	Contingency Planning	Decrease the number of Internet virus/worm traffic against internal network/users	Less than 5% of Internet virus/worm traffic impacts internal network/users	Maintain less than 3% Internet virus/worm traffic impacts internal network/users	Met target. 0% of the Internet virus/worm traffic impacted internal network/users this year.
2007	Strengthening Consular and Management Capabilities	Processes and Activities	Security and Privacy	Security	Security - Percent of network availability after primary site failure on classified network	100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites (<10% of email sites); 0% redundant EML infrastructure and support for routing to alternate location for Exchange 2000/2003 sites (>90% of sites)	Maintain 100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites; Increase to 2% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	Met Target. EML has operated and maintained OpenNet & ClassNet Exchange 5.5/2000/2003 operations. For ClassNet and OpenNet, alt site routing is in place for 2000/2003. OpenNet alt site routing for 5.5 was retired.
2007	Strengthening Consular and Management Capabilities	Technology	Reliability and Availability	Availability	Reliability - increase the availability of hot sites for remote access	Single instance of each system at one physical site; no redundancy or failover capability.	Implement additional redundant hot sites at other IRM core processing facilities (e.g., BIMC, ACS).	Met target. No funding in base for redundant hot sites. EML has operated and maintained OpenNet & ClassNet

Performance Information Table

Fiscal Year	Strategic Goal(s) Supported	Measurement Area	Measurement Category	Measurement Grouping	Measurement Indicator	Baseline	Target	Actual Results
								Exchange 5.5/2000/2003 operations. For ClassNet and OpenNet, alt site routing is in place for 2000/2003.
2008	Strengthening Consular and Management Capabilities	Customer Results	Timeliness and Responsiveness	Delivery Time	Responsiveness - Percent of network availability after primary site failure	100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites (<2% of email sites); 0% redundant EML infrastructure and support for routing to alternate location for Exchange 2000/2003 sites (>99% of sites)	Maintain 100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites; Increase to 2% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	
2008	Strengthening Consular and Management Capabilities	Mission and Business Results	Internal Risk Management and Mitigation	Contingency Planning	Decrease the number of Internet virus/worm traffic against internal network/users	Less than 5% of Internet virus/worm traffic impacts internal network/users	Maintain less than 2.75% Internet virus/worm traffic impacts internal network/users	
2008	Strengthening Consular and Management Capabilities	Processes and Activities	Security and Privacy	Security	Security - Percent of network availability after primary site failure on classified network	100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites (<2% of email sites); 0% redundant EML infrastructure and support for routing to alternate location for Exchange 2000/2003 sites (>99% of sites)	Maintain 100% redundant email infrastructure and support for routing to alternate location for Exchange 5.5 sites; Increase to 2% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	
2008	Strengthening Consular and Management Capabilities	Technology	Reliability and Availability	Availability	Reliability - increase the availability of hot sites for remote access	Single instance of each system at one physical site; no redundancy or failover capability.	Implement additional redundant hot sites at other IRM core processing facilities (e.g., BIMC, ACS).	

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

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
Classified E-mail SSP	No	Yes	None because no PII needed.	No	No PII
Classified Perimeter Security GSS	No	Yes	None because no PII needed	No	No PII
Unclassified (SBU) Email	No	Yes	None because no PII needed	No	No PII
Unclassified Perimeter Security GSS	No	Yes	None because no PII needed	No	No PII

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

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. Email Operations

b. If "no," please explain why?

4. Service Component Reference Model (SRM) Table:
Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.egov.gov.

Agency Component Name	Agency Component Description	FEA SRM Service Domain	FEA SRM Service Type	FEA SRM Component (a)	Service Component Reused Name (b)	Service Component Reused UPI (b)	Internal or External Reuse? (c)	BY Funding Percentage (d)
Data Recovery	Support the restoration and stabilization of data sets to a consistent desired state.	Back Office Services	Data Management	Data Recovery			No Reuse	10
Configuration Management	Control the hardware and software environments, as well as the documents of an organization	Business Management Services	Management of Processes	Configuration Management			No Reuse	5
Library / Storage	Support document and data warehousing and archiving	Digital Asset Services	Document Management	Library / Storage			No Reuse	10
Email	Support the transmission of memos and messages over a network.	Support Services	Collaboration	Email			No Reuse	30
Access Control	Support the management of permissions to log onto a computer, application, service, or network; includes user management and role/privilege management	Support Services	Security Management	Access Control			No Reuse	5

4. Service Component Reference Model (SRM) Table:

Identify the service components funded by this major IT investment (e.g., knowledge management, content management, customer relationship management, etc.). Provide this information in the format of the following table. For detailed guidance regarding components, please refer to http://www.egov.gov.

Agency Component Name	Agency Component Description	FEA SRM Service Domain	FEA SRM Service Type	FEA SRM Component (a)	Service Component Reused Name (b)	Service Component Reused UPI (b)	Internal or External Reuse? (c)	BY Funding Percentage (d)
Identification and Authentication	Support obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users.	Support Services	Security Management	Identification and Authentication			No Reuse	5
Issue Tracking	Receive and track user-supported issues and problems in using IT systems, including help desk calls	Support Services	Systems Management	Issue Tracking			No Reuse	30
License Management	Support the purchase, upgrade, and tracking of legal usage contracts for system software and applications	Support Services	Systems Management	License Management			No Reuse	5

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:

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

FEA SRM Component (a)	FEA TRM Service Area	FEA TRM Service Category	FEA TRM Service Standard	Service Specification (b) (i.e., vendor and product name)
Access Control	Component Framework	Security	Certificates / Digital Signatures	Secure Sockets Layer (SSL)
Access Control	Component Framework	Security	Supporting Security Services	Secure Shell (SSH)
Access Control	Component Framework	Security	Supporting Security Services	Transport Layer Security (TLS)
Access Control	Component Framework	Security	Supporting Security Services	Web Services Security (WS-Security)
Email	Service Access and Delivery	Access Channels	Collaboration / Communications	Electronic Mail (E-mail)
Email	Service Access and Delivery	Access Channels	Collaboration / Communications	Electronic Mail (E-mail)
Access Control	Service Access and Delivery	Access Channels	Other Electronic Channels	System to System
Email	Service Access and Delivery	Access Channels	Other Electronic Channels	Web Service
Identification and Authentication	Service Access and Delivery	Service Requirements	Legislative / Compliance	Security
Access Control	Service Access and Delivery	Service Transport	Service Transport	File Transfer Protocol (FTP)
Access Control	Service Access and Delivery	Service Transport	Service Transport	Hyper Text Transfer Protocol (HTTP)
Access Control	Service Access and Delivery	Service Transport	Service Transport	Hyper Text Transfer Protocol Secure (HTTPS)
Email	Service Access and Delivery	Service Transport	Supporting Network Services	Internet Message Protocol/Post Office Protocol (IMAP/POP3)
Email	Service Access and Delivery	Service Transport	Supporting Network Services	Lightweight Directory Access Protocol (LDAP)
Email	Service Access and Delivery	Service Transport	Supporting Network Services	Simple Mail Transfer Protocol

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

FEA SRM Component (a)	FEA TRM Service Area	FEA TRM Service Category	FEA TRM Service Standard	Service Specification (b) (i.e., vendor and product name)
				(SMTP)
Email	Service Access and Delivery	Service Transport	Supporting Network Services	Simple Mail Transfer Protocol (SMTP)
Email	Service Access and Delivery	Service Transport	Supporting Network Services	Simple Network Management Protocol (SNMP)
Email	Service Access and Delivery	Service Transport	Supporting Network Services	X.400
Library / Storage	Service Platform and Infrastructure	Database / Storage	Storage	Network-Attached Storage
Library / Storage	Service Platform and Infrastructure	Database / Storage	Storage	Storage Area Network (SAN)
Email	Service Platform and Infrastructure	Delivery Servers	Web Servers	Internet Information Server
Library / Storage	Service Platform and Infrastructure	Hardware / Infrastructure	Embedded Technology Devices	Hard Disk Drive
Email	Service Platform and Infrastructure	Hardware / Infrastructure	Local Area Network (LAN)	Ethernet
Access Control	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Firewall
Identification and Authentication	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Firewall
Data Recovery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Snap Mirror
Data Recovery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Snap Vault
Data Recovery	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Snapshot
Identification and Authentication	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Enterprise Server
Configuration Management	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Change Management
License Management	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Configuration Management

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

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.

Exhibit 300: Part III: For "Operation and Maintenance" investments ONLY (Steady State)

Section A: Risk Management (All Capital Assets)

Part III should be completed only for investments identified as "Operation and Maintenance" (Steady State) in response to Question 6 in Part I, Section A above.

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? 8/8/2006

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?