

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

I.A. Overview

1. Date of Submission:	7/14/2006
2. Agency:	Department of State
3. Bureau:	IRM/OPS/MSO/EML E-Mail
4. Name of this Capital Asset:	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 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.)	Operations and Maintenance
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:	
<p>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 (PK) initiatives along with numerous monitoring enhancements. Requirements for remote access to the OpenNet system are constantly being identified.</p>	
9. Did the Agency's Executive/Investment Committee approve this request?	Yes
a. If "yes," what was the date of this approval?	8/4/2006
10. Did the Project Manager review this Exhibit?	Yes
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	No

principles?

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, Competitive Sourcing, Right Sized Overseas Presence
13a. Briefly describe how this asset directly supports the identified initiative(s)?	1. Create easy-to-find single points of access to government services for employees, citizens, businesses, and other governments 2. Reduce the reporting burden on businesses 3. Share information quicker and conveniently between federal, state, local and tribal government 4. Automate internal processes to reduce costs internally, within the federal government, by disseminating best practices across 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 .)	No
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?	
c. If "yes," what PART rating did it receive?	
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):	(1) Project manager has been validated as qualified for this investment
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 FFMI A 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	
20. What is the percentage breakout for the total FY2008 funding request for the following? (This should total 100%)	
Hardware	5
Software	20
Services	75

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

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

No

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)
2003	Strategic Goal 12: Management and Organizational Excellence - Ensure a high quality workforce supported by modern and secure infrastructure and operational capacities/Information Technology.	Service requests concerning e-mail networks, cable systems and firewalls are provided according to user requirements based on practices and specifications for each type and model of equipment.	Percent of service requests that met response time standards in each category (Routine, Priority, and Immediate).	100% of routine service requests are resolved within timeframes negotiated beforehand with customer in accordance with EML Division standard, as verified by independent procedures established by DOS. 100% of priority service requests are resolved	100% of routine service requests are resolved within timeframes negotiated beforehand with customer in accordance with EML Division standard, as verified by independent procedures established by DOS. 100% of priority service requests are resolved
2003	Strategic Goal 12: Management and Organizational Excellence - Ensure a high quality workforce supported by modern and secure infrastructure and operational capacities/Information Technology.	Department firewalls continue to meet all required USG and Department security configuration standards requirements.	100% of Department Firewalls met all required USG and Department security configuration standards.	All Department firewalls meet the USG firewall standards issued by the National Institute of Standards and Technology.	100% of firewalls meet all requirements.

2004	Strategic Goal 12: Management and Organizational Excellence - Ensure a high quality workforce supported by modern and secure infrastructure and operational capacities/Information Technology.	Continue to meet response times for service requests concerning e-mail networks, cable systems and firewalls according to user requirements based on practices and specifications for each type and model of equipment.	Percent of service requests that met response time standards in each category (Routine, Priority, and Immediate).	100% of routine service requests are resolved within timeframes negotiated beforehand with customer in accordance with EML Division standard, as verified by independent procedures established by DOS. 100% of priority service requests are resolved	100% of routine service requests are resolved within timeframes negotiated beforehand with customer in accordance with EML Division standard, as verified by independent procedures established by DOS. 100% of priority service requests are resolved
2004	Strategic Goal 12: Management and Organizational Excellence - Ensure a high quality workforce supported by modern and secure infrastructure and operational capacities/Information Technology.	Department firewalls must meet all required USG and Department security configuration standards.	100% of Department Firewalls met all required USG and Department security configuration standards.	All Department firewalls meet the USG firewall standards issued by the National Institute of Standards and Technology.	100% of firewalls meet all requirements.

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
2005	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	Mission and Business Results	Internal Risk Management and Mitigation	Contingency Planning	Decrease the number of Internet virus/worm traffic against internal/users network.	Less than 5% of Internet virus/worm traffic impacts internal network/users	Less than 4% Internet virus/worm traffic impacts internal network/users	To date no major Internet virus/worm has impacted the internal network/users since September 2003
2005	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	Technology	Reliability and Availability	Availability	Availability - time to restore access to	100% redundant email infrastructure and support for	Maintain 100% redundant email infrastructure and	No funding provided to build redundant email infrastructure

				corporate email resources and applications	routing to alternate location for Exchange 5.5 sites; 0% redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.	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.	and support for routing to alternate location for Exchange 2000 sites.
2006	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.	No funding has been identified for Classified alternate site or for Classified Exchange 2000/2003 Central Site operations. Successfully build redundant email infrastructure and support for Unclassified routing to alt location for Exchange 2000/2003
2006	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
2006	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 (35% of Email sites); 0% redundant EML infrastructure and support for routing to alternate location for Exchange 2000 sites (65% 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.	No funding provided to build redundant email infrastructure and support for routing to alternate location for Exchange 2000 sites.
2006	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).	In process of adding a secondary physical site within five miles of primary site for limited redundancy and failover.
2007	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.	
2007	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	
2007	Processes and	Security and	Security	Security - Percent of	100% redundant email	Maintain 100% redundant	

	Activities	Privacy		network availability after primary site failure on classified network	infrastructure and support for routing to 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)	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.	
2007	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).	
2008	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.	
2008	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	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 (35% of Email sites); 0% redundant EML infrastructure and support for routing to alternate location for Exchange 2000 sites (65% 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.	
2008	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).	

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:	41
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

5. Have any weaknesses 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 agency's plan of action and milestone process?	No
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.	

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?
Classified E-mail SSP	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Classified Perimeter Security GSS	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Unclassified (SBU) Email	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.
Unclassified Perimeter Security GSS	No	No, because the system does not contain, process, or transmit personal identifying information.	No, because a PIA is not yet required to be completed at this time.	No	No, because the system is not a Privacy Act system of records.

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. Email Operations

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
Messaging and Email Services	The set of capabilities that support keyboard conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Back Office Services	Data Management	Data Exchange	Email		No Reuse	20
Messaging and Email Services	The set of capabilities that support keyboard conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Back Office Services	Data Management	Data Recovery	Email		No Reuse	10
Messaging and Email Services	The set of capabilities that support keyboard conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Back Office Services	Development and Integration	Enterprise Application Integration	Email		No Reuse	10
Messaging and Email Services	The set of capabilities that support keyboard conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Business Management Services	Management of Processes	Configuration Management	Email		No Reuse	10
Messaging and Email Services	The set of capabilities that support keyboard conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Digital Asset Services	Document Management	Library / Storage	Email		No Reuse	10
Messaging and	The set of capabilities that support keyboard	Support	Collaboration	Email	Email		No Reuse	0

Email Services	conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Services						
Messaging and Email Services	The set of capabilities that support keyboard conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Support Services	Security Management	Access Control	Email		No Reuse	5
Messaging and Email Services	The set of capabilities that support keyboard conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Support Services	Security Management	Identification and Authentication	Email		No Reuse	0
Messaging and Email Services	The set of capabilities that support keyboard conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Support Services	Systems Management	Issue Tracking	Email		No Reuse	30
Messaging and Email Services	The set of capabilities that support keyboard conferencing and the electronic exchange of messages, record traffic, correspondence, documents, or other information over a network or the internet.	Support Services	Systems Management	License Management	Email		No Reuse	5

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 Category	FEA TRM Service Standard	Service Specification (i.e. vendor or 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
Data Exchange	Service Access and Delivery	Access Channels	Web Browser	Internet Explorer
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)
Data Classification	Service Access and Delivery	Service Transport	Supporting Network Services	Directory Services (X.500)
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 (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)
Data Classification	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
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

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

III.A. Risk Management

Part III should be completed only for investments which will be in "Operation and Maintenance" (Steady State) in FY 2008, i.e., selected the "Operation and Maintenance" choice 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.

Answer the following questions to describe how you are managing investment risks.

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?