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

I.A. Overview

1. Date of Submission:	9/12/2006
2. Agency:	014
3. Bureau:	IRM/OPS Operations
4. Name of this Capital Asset:	Joint DoS/USAID IT Infrastructure Integration Program
5. Unique Project (Investment) Identifier: (For IT investment only, see section 53. For all other, use agency ID system.)	014-00-02-00-01-1671-00
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.)	Full Acquisition
7. What was the first budget year this investment was submitted to OMB?	FY2008

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:

To fully align foreign policy and development assistance to support the President's National Security Strategy and Management Agenda, the Department of State (DoS) and U.S. Agency for International Development (USAID) have begun integrating common management structures. This collaboration will help both organizations execute joint goals, such as providing employee support, increasing operational efficiencies, and reducing redundancies and costs for the taxpayer. To implement this initiative, a DoS / USAID Joint Management Council (JMC) was created. The JMC has established seven working groups to address issues surrounding specific management functions. In addition, the DoS and USAID Teams have analyzed the advantages of and the challenges in integrating the agencies' Sensitive But Unclassified (SBU) networks, AIDNet and OpenNet, to ensure a modernized, secure, and high-quality IT infrastructure. Working with the JMC and supporting the FY04-09 Joint Strategic Plan and FY07 Annual Performance Plan, a USAID Team developed an approach to explore an effective means to integrate the USAID and DoS IT infrastructures, policies, and organizations. The DoS and USAID Team will plan and execute the critical integration of AIDNet into the OpenNet environment in a 3-phase approach during FY08-10: 1) Project Ramp-up, 2) Piloting and Engineering, and 3) Worldwide Deployment and Engineering. Note that this business case assumes full funding for the integration in FY08-10. If funding is provided in FY07, the DoS and USAID Teams will expedite the integration, initiating the first phase in early FY07. Network integration provides several strategic benefits, including economies of scale, support of Transformational Diplomacy goals such as more robust remote access capabilities and servicing of American Presence Posts (APPs), and the opportunity to build an integrated environment for the Foreign Affairs community. Examples of other benefits include enhanced IT capabilities, communication, and space utilization at embassies; elimination of duplicate capabilities and systems; direct support of Regionalization/Rightsizing efforts by merging supporting systems and support personnel; and potential for future consolidation of management systems, e.g., HR, to improve accountability and organizational efficiency. This Exhibit 300 requests funding for DoS to support this joint goal and mirrors the Exhibit 300 that USAID is also submitting for FY07.

9. Did the Agency's Executive/Investment Committee approve this request?	Yes
a. If "yes," what was the date of this approval?	8/30/2006
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	Yes

computers)?	
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 support one of the PMA initiatives?	Yes
If "yes," check all that apply:	Financial Performance, Expanded E-Government, Right Sized Overseas Presence
13a. Briefly describe how this asset directly supports the identified initiative(s)?	The Joint IT Infrastructure Integration supports the PMA by providing stable and adequate, yet flexible infrastructure; gaining economies of scale; and providing more central/regional coordination.
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 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 identified as "high risk" on the Q4 - FY 2006 agency high risk report (per OMB's "high risk" memo)?	No
19. Is this a financial management system?	No
a. If "yes," does this investment address a FFMIA compliance area?	
1. If "yes," which compliance area:	
2. If "no," what does it address?	
b. If "yes," please identify the system name(s) and system acronym(s) as reported in the most recent financial systems inventory update required by Circular A-11 section 52	

20. What is the percentage breakout for the total FY2008 funding request for the following? (This should total 100%)	
Hardware	54
Software	8
Services	38
Other	
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?	Yes

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)

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

2008	Customer Results	Service Accessibility	Integration	Transition USAID domestic users to DoS OpenNet to improve performance and achieve efficiencies.	Less than 10% of domestic USAID users using OpenNet for primary computing.	100% of domestic USAID users transitioned from AIDNet to DoS OpenNet	
2008	Customer Results	Service Quality	Accuracy of Service or Product Delivered	USAID mission pilots accepted by USAID mission directors.	0% (no DoS OpenNet available)	100% acceptance of pilot implementations	
2008	Mission and Business Results	Information and Technology Management	IT Infrastructure Maintenance	4 USAID pilot sites transitioned from AIDNet to DoS OpenNet.	0% (no DoS OpenNet available)	4 USAID missions transitioned to OpenNet	
2008	Processes and Activities	Quality	Errors	Quality assessments conducted on pilot sites	0% (no DoS OpenNet available)	100% acceptance of pilot implementation by USAID mission directors	
2008	Technology	Effectiveness	IT Contribution to Process, Customer, or Mission	Shared Internet Service Provider (ISP) bandwidth between USAID and DoS	0% (no bandwidth sharing of ISPs overseas)	20% of collocated USAID missions and DoS embassies share ISP connections.	
2008	Technology	Efficiency	Interoperability	Shared Domestic Metropolitan Area Network (MAN) bandwidth between USAID and DoS	0% (no bandwidth sharing of MAN domestically)	Integrate MAN bandwidth resulting in one physical MAN.	
2008	Technology	Reliability and Availability	Reliability	Integrated Wide Area Network (WAN) aggregation points.	0% (no integated WAN aggregation points)	Integrate WAN aggregation points resulting in one synchronized shared WAN aggregation point.	
2009	Mission and Business Results	Information and Technology Management	IT Infrastructure Maintenance	16 USAID sites transitioned from AIDNet to DoS OpenNet	0% (no DoS OpenNet available)	20 total USAID missions transitioned to OpenNet	
2009	Technology	Effectiveness	IT Contribution to Process, Customer, or Mission	Shared Internet Service Provider (ISP) bandwidth between USAID and DoS	0% (no bandwidth sharing of ISPs overseas)	50% of collocated USAID missions and DoS embassies share ISP connections.	
2010	Mission and Business Results	Information and Technology Management	IT Infrastructure Maintenance	20 additional USAID sites transitioned from AIDNet to DoS OpenNet	0% (no DoS OpenNet available)	40 total USAID missions transitioned to OpenNet	
2010	Mission and Business Results	Information and Technology Management	IT Infrastructure Maintenance	Shared Internet Service Provider (ISP) bandwidth between USAID and DoS	0% (no bandwidth sharing of ISPs overseas)	75% of collocated USAID missions and DoS embassies share ISP connnections.	

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:	5
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?	Yes
a. If "yes," have those weaknesses been incorporated agency's plan of action and milestone process?	Yes
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?
OpenNet Transport 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.	Joint DoS/USAID IT Infrastructure

Integration Program

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
Configuration Management (New DoS Service)	Defines the set of capabilities that control the hardware and software environments, as well as documents of an organization.	Business Management Services	Management of Processes	Configuration Management			No Reuse	7
Program/Project Management (New DoS Service)	Defines the set of capabilities for the management and control of a particular effort of an organization.	Business Management Services	Management of Processes	Program / Project Management			No Reuse	27
Network Management (New DoS Service)	Defines the set of capabilities involved in monitoring and maintaining a communications network in order to diagnose problems, gather statistics, and provide general usage.	Business Management Services	Organizational Management	Network Management			No Reuse	4
Data Network Services	Executes, maintains, and supports the devices, facilities, and standards that provide the computing and networking within and between enterprises.	Support Services	Communication	NEW			No Reuse	38
Continuity of Operations	The execution of contingency plans for operations during crisis, unforeseen circumstances, or disruptions in normal day-to-day operations.	Support Services	Security Management	NEW			No Reuse	7
Remote Systems Control (New DoS Service)	Defines the set of capabilities that support the monitoring, administration, and usage of applications and enterprise systems from locations outside of the immediate system environment.	Support Services	Systems Management	Remote Systems Control			No Reuse	4
System Resource Monitoring (New DoS Service)	Defines the set of capabilities that support the balance and allocation of memory, usage, disk space, and performance on computers and their applications.	Support Services	Systems Management	System Resource Monitoring			No Reuse	13

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)
Network Management	Component Framework	Security	Certificates / Digital Signatures	Digital Certificate Authentication - Patriot Technologies RSA Secure
Network Management	Component Framework	Security	Certificates / Digital Signatures	Secure Sockets Layer (SSL) - Microsoft supported
System Resource Monitoring	Service Access and Delivery	Access Channels	Other Electronic Channels	Attachmate NetIQ Application Manager
Network Management	Service Access and Delivery	Delivery Channels	Intranet	Hewlett-Packard OpenView
Remote Systems Control	Service Access and Delivery	Service Requirements	Authentication / Single Sign-on	Cisco Access Control System (ACS)
Remote Systems Control	Service Access and Delivery	Service Requirements	Hosting	Microsoft Active Directory
Program / Project Management	Service Access and Delivery	Service Requirements	Legislative / Compliance	Business Engine Microframe Program Manager (MPM)
Program / Project Management	Service Access and Delivery	Service Requirements	Legislative / Compliance	Section 508 (all systems must comply)
Network Management	Service Access and Delivery	Service Transport	Service Transport	Internet Protocol (IP) v4 transitioning to v6 - Cisco, Microsoft supported
Network Management	Service Access and Delivery	Service Transport	Service Transport	IP Security (IPSec) - Cisco, Nortel supported
Network Management	Service Access and Delivery	Service Transport	Service Transport	Taave Software Co. PReView
Network Management	Service Access and Delivery	Service Transport	Supporting Network Services	Nortel 600, 1700, 2700 FIPS Type 2 encryption for SBU networks
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Cisco Routers, including 2621xm, 7206/8vxr
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Cisco Switches, including 2950, 3750, 6509
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Network Devices / Standards	Lucent Optical Switching, OC3, OC12, OC48
Remote Systems Control	Service Platform and Infrastructure	Hardware / Infrastructure	Servers / Computers	Hewlett-Packard Enterprise Servers, including DL380
Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Wide Area Network (WAN)	Marconi Asynchronous Transfer Mode (ATM) - ServiceOnData

Network Management	Service Platform and Infrastructure	Hardware / Infrastructure	Wide Area Network (WAN)	Niksun NetVCR
Configuration Management	Service Platform and Infrastructure	Hardware / Infrastructure	Wide Area Network (WAN)	Remedy Action Request System
Remote Systems Control	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Microsoft SMS Deployment Management
Configuration Management	Service Platform and Infrastructure	Software Engineering	Software Configuration Management	Opsware Network Automation System

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)?	Yes
a. If "yes," please describe.	
DoS and USAID will share service components of the SRM as a part of this investment. Both organizations plan to identify 'best-of-breed' technologies and service implementations. For example, the DoS Network Management component is considered world class by both partners, and will be used as the basis for an integrated network management system. Conversely, the USAID distributed firewall technologies have proven effective in providing mission critical protection directly to field operations, and will be a strong candidate for the integrated network.	
6. Does this investment provide the public with access to a government automated information system?	No
a. If "yes," does customer access require specific software (e.g., a specific web browser version)?	
1. If "yes," provide the specific product name(s) and version number(s) of the required software and the date when the public will be able to access this investment by any software (i.e. to ensure equitable and timely access of government information and services).	

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

II.A. Alternatives Analysis

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

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

1. Did you conduct an alternatives analysis for this project?	No

a. If "yes," provide the date the analysis was completed?	
b. If "no," what is the anticipated date this analysis will be completed?	9/30/2006

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

An alternatives analysis is underway and with an expected completion date of September 30, 2006. Once completed, the joint technical teams will provide DoS and USAID Senior Management with the results. DoS and USAID will work collaboratively to identify, validate and implement the most efficient and cost effective alternative.

4. What specific qualitative benefits will be realized?

The alternatives analysis is currently under development with an expected completion date of September 30, 2006. Qualitative benefits will be provided in the analysis, but are expected to include economies of scale and an integrated environment for the Foreign Affairs community. Examples of other benefits include enhanced IT capabilities, communication, and space utilization at embassies; elimination of duplicate capabilities and systems; direct support of Regionalization/Rightsizing efforts by merging supporting systems and support personnel; and potential for future consolidation of management systems, e.g., HR, to improve accountability and organizational efficiency.

II.B. Risk Management

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

1. Does the investment have a Risk Management Plan?	Yes
a. If "yes," what is the date of the plan?	7/30/2005
b. Has the Risk Management Plan been significantly changed since last year's submission to OMB?	Yes

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

In FY 2005, a USAID Team developed an appendix to the USAID PMO risk management plan that focused solely on the initial risks of collaboration, JEA alignment and the Foreign Affairs Infrastructure e-authentication and extranet concept. In late FY 2006, the team developed the USAID/DoS IT Infrastructure Integration (i3) Planning Concepts and Preliminary Approach document, which refined and further identified the high-level technical and policy risks associated with an IT integration. Continuing in FY 2007, DoS will engage with USAID to revalidate each risk, to identify additional risks, and to develop mitigation strategies for each risk to minimize the impact of the risk or the probability of its occurrence. This information will be governed by and contained in a formal risk management plan, which will be jointly developed by DoS and USAID technical saffs, responsible for risk management, monitoring, and evaluation moving forward and will update senior management regularly on these risks and their status.

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:

As part of the project management process, the i3 team has identified and analyzed risks during project planning. Risk analysis includes classifying the risks and assessing the risk probability, impact, immediacy, and controllability. These attributes help the program manager identify the greatest risks to the program and ensure they are appropriately mitigated. Following risk assessment, the risk probability was multiplied by the risk impact and incorporated into the cost and schedule estimates to account for risk. For example, a risk with an estimated $10,000 impact and 70% probability would cause the cost estimate to be increased by $7,000 ($10,000*70%). If a risk had an estimated two-month impact to the schedule and 50% probability, the schedule was increased by one month (2 months*50%). These schedule risks would also affect the cost estimates, since the cost of an additional month of work would need to be included. Although the original estimates were appropriately risk-adjusted, budget cuts have eliminated some of these adjustments and increased the program's cost risk. Programmatically, USAID and DoS will use an incremental approach that accomplishes the integration in three (3) successive

phases that build upon each other with each phase including several intermediate reviews (decision checkpoints) to allow the project team to react to changing conditions and provide executive management with the ability to evaluate progress before proceeding to the next phases. Technically, a carefully selected set of pilot missions will be used to validate requirements and validate and discover a full set of risks and issues before proceeding with a general worldwide deployment. In addition, during the integration, USAID will keep AIDNet operational until all issues and risks associated with the continuation of USAID business requirements, applications, and services have been adequately resolved and implemented in the OpenNet environment and/or a suitable alternative, e.g., alternate hosting environment, is provided.