

DRAFT Joint IT Strategic Plan

This version is subject to revision and does not represent the official position of either USAID or DoS

**Joint IT Strategic Plan
Empowering Diplomacy and Development**

November 2005



USAID
FROM THE AMERICAN PEOPLE



DRAFT Joint IT Strategic Plan

This version is subject to revision and does not represent the official position of either USAID or DoS

EXECUTIVE SUMMARY

Purpose

This Joint Information Technology Strategic Plan (JITSP) establishes a blueprint for how IT will support the US Department of State and US Agency for International Development (USAID) throughout the balance of this decade. The JITSP focuses on the policy and management goals and objectives of both organizations, and enables broad internal and external collaboration to further the joint mission of diplomacy, development, and disaster assistance.

**Strategic Theme:
Transformation
From Infrastructure to Empowerment**

The JITSP builds on the IT successes of both State and USAID, which have resulted in a robust, secure, global IT infrastructure in place at over 300 locations around the world. While building on past successes, this new JITSP will transform both agencies, positioning them to promote US foreign policy objectives around the world. By joining forces under this JITSP, State and USAID will take the next steps in bringing information to bear on the substantive international issues facing the United States today.

Vision

Information and information technology are increasingly vital tools in the pursuit of US foreign policy. The information technology environment envisioned in this Plan represents a significant departure from the IT of the past in that it focuses on supporting the substantive work of diplomacy and development, rather than IT infrastructure or administrative functions.

**Vision:
Empowering diplomacy and development
with information and tools available
anytime, anywhere**

The key elements of the JITSP are:

- Transforming information into actionable knowledge
- Supporting foreign policy priorities such as promotion of democracy
- Enabling "virtual teaming" among internal and external participants in development and diplomatic programs and initiatives
- Liberating State and USAID personnel through mobile computing
- Enabling rightsizing and other management initiatives

DRAFT Joint IT Strategic Plan

The lessons of the first years of the 21st century demonstrate the importance of information -- the need to deliver the right information to the right people when they need it. Reliable information is the enabler of effective decision-making which is at the heart of international diplomacy and development. This realization leads to the most important focus of this JITSP -- producing accurate information that supports decision-makers, and making that information available to those who need it, regardless of time or place. Information will be processed and organized to ensure accuracy and utility, and will be available at all times. Information will be maintained centrally in a virtual library, and will be accessible from anywhere around the world. This will enable "dataless" posts, enhancing information security and mission effectiveness.

Security and efficiency are paramount objectives that will be furthered through rightsizing, and through the use of interagency solutions sponsored under the e-Government initiative. Information technology will enable rightsizing by providing a robust network that supports centralization and regionalization of functions and service delivery. This will allow virtually all administrative services to be provided remotely, thus eliminating the need for administrative personnel at most posts and missions. Use of Government-wide solutions will increase efficiency, effectiveness, and consistency of administrative and substantive services, such as economic analysis.

Mission effectiveness in international affairs requires extensive collaboration, both internally among US Government personnel, and with external partners. This JITSP provides extensive support for collaboration, allowing people to form dynamic virtual teams to work together on issues, policy initiatives, and development programs, wherever they may be located. For example, a typical virtual team supporting a development program might include functional and geographic specialists, procurement/grants managers, budget and finance staff, contractors and NGOs, host nation and third country government staff, and locally hired employees. These people will all be able to share information, convene virtual meetings, and collaborate in real time as needed -- with all exchanges protected by suitable security mechanisms.

In summary, State and USAID will operate very differently as a result of the information and systems to be deployed under this plan. Among the key changes are:

- Enhanced collaboration to further US foreign policy objectives
- Easier and more rapid access to higher quality information leading to better policy decisions
- Strengthened outreach programs supported by multi-media information products, to serve US citizens and engage foreign officials and publics
- Freedom to carry out diplomatic and development initiatives while out of the office, teleworking, on travel, or on site responding to a disaster or other crisis
- Greater efficiency and responsiveness in supporting the front-line personnel carrying out US diplomacy, development, and disaster assistance

DRAFT Joint IT Strategic Plan

Goals and Objectives

Five goals and 16 objectives, presented in the following table, will be pursued to achieve this vision.

Goal	Objectives	Key Elements
Goal 1: The Right Information: Knowledge Leadership for Diplomacy and Development	1.1 Dynamic Information Environment	<ul style="list-style-type: none"> • Value-added knowledge bases • Central information service
	1.2 Specialized Tools And Systems	<ul style="list-style-type: none"> • Content management • Contact management • Search, retrieval, analysis, presentation
	1.3 Performance And Results	<ul style="list-style-type: none"> • Management and policy dashboard • Executive Information System
Goal 2: Anytime/ Anywhere Access: Foreign Affairs Professionals on the Move	2.1 Mobile Computing	<ul style="list-style-type: none"> • Modern end-user devices -- cell phones, laptops, PDAs • Remote access to liberate foreign affairs professionals
	2.2 Performance-Driven IT Infrastructure	<ul style="list-style-type: none"> • Universal 7X24 availability • Commercial-quality network
	2.3 Common Infrastructure	<ul style="list-style-type: none"> • Consolidated support for State and USAID • Life cycle refresh
Goal 3: External Partnership: Diplomacy and Development through Collaboration	3.1 External Collaboration	<ul style="list-style-type: none"> • Secure, flexible extranets • Collaboration with NGOs, other governments, and publics
	3.2 Unified Interagency Infrastructure	<ul style="list-style-type: none"> • Expansion of global infrastructure to all USG agencies operating overseas
	3.3 E-Government Lines Of Business Solutions	<ul style="list-style-type: none"> • Support for the PMA • Efficiency gains through interagency solutions
	3.4 Rightsizing	<ul style="list-style-type: none"> • IT as enabler of central service delivery
Goal 4: Risk Management: Balancing Security with Business Imperatives	4.1 Risk Management	<ul style="list-style-type: none"> • Rapid, secure introduction of IT • Business owner accountability for risk, per NIST guidance
	4.2 Consistent Security Infrastructure	<ul style="list-style-type: none"> • Security framework that accommodates State and USAID business requirements • Security solutions that support all five goals
	4.3 Business Continuity	<ul style="list-style-type: none"> • Robust, fully tested contingency plans for all operations and locations
Goal 5: Work Practices and Workforce: Leading Change	5.1 It Organizational Excellence and Accountability	<ul style="list-style-type: none"> • Accountability for service levels in IT support • IT innovation laboratory
	5.2 Strengthened It Skills	<ul style="list-style-type: none"> • Training and support for IT staff and end-users • Shift of IT role to focus on end-user needs
	5.3 Consistent It Governance	<ul style="list-style-type: none"> • Adoption of best practices from State and USAID • Central control over IT investments

Strategic IT Goals and Objectives

Implementation

Key management strategies and critical success factors will drive execution of the JITSP and accomplishment of the strategic goals and objectives. Key among these is a strategy for integration of State and USAID IT capabilities. The integration strategy will ensure that the IT environments of the two agencies are consolidated to the extent practical, achieving economies of scale and the benefits of information and technology sharing. The strategy also calls for ensuring that the mission and business requirements of the two agencies are accommodated without compromise. Best practices of each agency will be leveraged in the consolidated environment.

Critical success factors include the following:

- Active leadership commitment at the highest levels
- Focused application of IT investments and resources -- all consolidated under e-Governance
- Recognition of information as a US Government asset, not the property of individual posts, bureaus, or agencies
- Professional management to lead large-scale development and integration programs
- Accountability for achieving established customer service levels
- Commitment to continuous innovation and rapid introduction of new technologies
- Adoption of a cost-effective approach to IT security and risk management, one that ensures appropriate security without impeding vital operations

Although the JITSP will yield efficiency gains if executed properly, substantial investments will be needed, especially in the first two to three years. Savings produced through rightsizing and centralization of IT and other operations should be made available to pursue the JITSP.

Specific initiatives will be defined in a Tactical Plan that details the sequence of projects and investments required to implement the JITSP.

Table of Contents

1	Introduction.....	1	Deleted: 1
1.1	Overview.....	1	Deleted: 1
1.2	Current Status of IT at State and USAID.....	1	Deleted: 1
1.3	Stakeholder Participation in the Planning Process.....	4	Deleted: 4
2	IT Strategic Plan Drivers.....	6	Deleted: 6
2.1	Mission and Business of State and USAID.....	6	Deleted: 6
2.1.1	Department of State.....	6	Deleted: 9
2.1.2	USAID.....	7	Deleted: 9
2.1.3	Challenges.....	7	Deleted: 10
2.2	President’s Management Agenda and e-Government.....	9	Deleted: 12
2.3	Rightsizing.....	9	Deleted: 14
2.4	IT Best Practices and Trends.....	10	Deleted: 17
3	Vision—Empowering Diplomacy and Development with Information Technology.....	12	Deleted: 19
4	Goals and Objectives.....	14	Deleted: 20
4.1	Goal 1 - The Right Information.....	18	Deleted: 23
4.1.1	Dynamic Information Environment.....	20	Deleted: 27
4.1.2	Specialized Tools and Systems.....	21	Deleted: 29
4.1.3	IT Capabilities for Performance and Results.....	24	Deleted: 30
4.2	Goal 2 – Anytime/Anywhere Access.....	28	Deleted: 30
4.2.1	Mobile Computing.....	30	Deleted: 30
4.2.2	Performance-driven IT infrastructure.....	32	Deleted: 30
4.2.3	Common Infrastructure for State and USAID.....	34	Deleted: 30
4.3	Goal 3 - Supporting External Partnerships and Leveraging e-Government.....	38	Deleted: 30
4.3.1	External Collaboration.....	39	Deleted: 30
4.3.2	Unified Interagency Infrastructure.....	41	Deleted: 30
4.3.3	e-Government Lines of Business (LOB) Solutions.....	43	Deleted: 30
4.3.4	Rightsizing.....	45	Deleted: 30
4.4	Goal 4 – Risk Management – Balancing security with business imperatives.....	48	Deleted: 30
4.4.1	Risk Management.....	51	Deleted: 30
4.4.2	Consistent IT Security Infrastructure.....	54	Deleted: 30
4.4.3	Business Continuity.....	56	Deleted: 30
4.5	Goal 5: Work Practices and Workforce.....	59	Deleted: 30
4.5.1	Organizational Excellence and Accountability.....	60	Deleted: 30
4.5.2	Strengthened IT Skills.....	62	Deleted: 30
4.5.3	Consistent IT Governance.....	63	Deleted: 30
5	Management Strategies & Critical Success Factors.....	66	Deleted: 30
5.1	IT Integration Strategy.....	66	Deleted: 30
5.2	Critical Success Factors (CSFs).....	68	Deleted: 30
5.2.1	Leadership CSFs.....	68	Deleted: 30
5.2.2	Management CSFs.....	69	Deleted: 30
5.2.3	Technology CSFs.....	70	Deleted: 30
6	Implementation Strategy.....	71	Deleted: 30
			Deleted: 30

DRAFT Joint IT Strategic Plan

This version is subject to revision and does not represent the official position of either USAID or DoS

1 Introduction

1.1 Overview

This *Joint Information Technology (IT) Strategic Plan (JITSP)* outlines a future-oriented technology program that directly supports the core functions of U. S. foreign policy, diplomacy, development, and disaster relief as articulated in the *FY 2004–2009 Department of State and USAID Strategic Plan*. While IT is not a core function of State or USAID, it is essential in carrying out the core functions of both agencies. The JITSP reflects the joint requirements of the Department of State and the US Agency for International Development (USAID), and will support a significant level of integration of the IT environments and operations of the two agencies. It will also promote the establishment of an integrated platform for supporting the activities and information requirements of all US Government agencies operating overseas.

The Plan establishes five strategic IT goals and 16 objectives for FY 2006–2010. Several of these goals represent significant departures from the current ways of doing business and allocating IT resources. The Plan sets the IT direction for the balance of this decade and forms the basis for major decisions on IT investments and projects. The Plan provides linkage between the Joint State/USAID Strategic Plan and required technologies, information resources, and knowledge management practices. The JITSP will supply input to the joint State/USAID Enterprise Architecture (EA) currently under development, will drive the technical architecture, and will ensure that the EA supports the strategic direction of the two agencies.

Secretary of State Rice has said "This is a time of global transformation and it calls for transformational diplomacy....More than ever, we will need men and women who are able to communicate well to reach out to people in other lands and to work in partnership with them to build a freer and safer and better world."

The JITSP commits the Department and USAID to using IT to enable our people to communicate and share the information needed to accomplish the transformational diplomacy proposed by Sec Rice.

1.2 Current Status of IT at State and USAID

This Plan builds on the successes and strengths of both State and USAID in deploying and exploiting IT in support of international operations. For State, the Plan begins with the current *IT Strategic Plan* which covers the period FY 2001– 2005. Under the earlier plan, the Department successfully modernized its global IT infrastructure. Now, the Department will take the next step: putting in place tools and information resources that directly support the international affairs mission.

State has made excellent progress under its *IT Strategic Plan, FY 2001-2005*, achieving demonstrable success under five goals, and changing the way the Department does

DRAFT Joint IT Strategic Plan

business. The Department recently implemented improvements in its IT governance processes, to ensure continuing broad and effective representation by senior managers in decision-making. By demonstrating effective progress, the Department was able to justify substantial increases in IT investment, enabling rapid introduction of a modern, global technology infrastructure. The enthusiastic support and leadership of senior management, including the Secretary of State, proved critical in securing necessary resources and promoting ongoing IT modernization in support of diplomacy. The Department has also been pursuing a knowledge management strategy, called Knowledge Leadership, under which collaboration capabilities, portal technologies, and other innovative approaches have been put in place.

Table 1 highlights the major accomplishments under its FY 2001-2005 Plan.

Table 1: Accomplishments under FY 2001–2005 IT Strategic Plan

ITSP Goal	Major Accomplishments
<p>1. A Secure Global Network and Infrastructure</p>	<ul style="list-style-type: none"> • Highly standardized, available, and reliable global IT infrastructure with 99.5% network availability in FY2005 • Defense-in-depth security – e.g., server, e-mail, and workstation anti-virus, network intrusion detection, and operational CERT and CIRT processes • Certification and Accreditation program • Modern, reliable classified and unclassified networks • Desktop Internet access and Virtual Private Network (VPN) capabilities • Centralized IT modernization and refresh worldwide through Global IT Modernization (GITM) program • Enterprise network management
<p>2. Ready Access to International Affairs applications and Information</p>	<ul style="list-style-type: none"> • Continued improvement and centralization of border security systems • Public affairs and Public Diplomacy applications and Web sites • Specialized mission-support databases and applications (e.g., Treaties, Refugees, Contacts) • Connectivity to SIPRNET and OSIS, and establishment of a strong State knowledge-sharing program on SIPRNet • Collaboration capabilities supporting diplomacy, border security, and humanitarian information programs • Initial steps toward mobile communications

DRAFT Joint IT Strategic Plan

ITSP Goal	Major Accomplishments
3. Integrated Messaging— A Modern Worldwide Approach	<ul style="list-style-type: none"> • Single, worldwide e-mail systems for classified and unclassified traffic • Initiation of State Messaging and Archive Retrieval Toolset (SMART) program to deploy innovative worldwide, integrated messaging
4. Leveraging IT to Streamline Operations	<ul style="list-style-type: none"> • Significant progress in implementing Web-based administrative applications to improve efficiency • Server consolidation through Enterprise Server Operations Center (ESOC) • Financial systems for both State and USAID centralized in Charleston
5. Sustaining a Trained Productive Workforce	<ul style="list-style-type: none"> • Skilled IT workforce • Best Practice in recruitment and retention • Modern, effective training/certification programs

Information technology implemented under the earlier *IT Strategic Plan* changed the way the Department does diplomacy. A few examples are:

- Remote posts are less isolated as a result of the global networks;
- Fast, flexible e-mail replaced rigidly formatted cables for much of the Department's work;
- The global unclassified and classified networks created a platform that encourages information exchange;
- Desktop access to the Web is an important information resource and a vehicle for engagement and outreach; and
- Electronic commerce is well established for on-line acquisition.

This JITSP also builds on the progress USAID has made in exploiting IT to further the objectives of international development and disaster assistance, notably:

- Collaboration systems that enable teams to manage and share information and communicate with team members regardless of their location
- Mobile computing technology that provides remote access and support for rapid-response teams
- Joint strategy for knowledge management (KM) and an Executive Information System (EIS) that promotes information access and sharing, and monitoring of program performance and results
- Security risk management that focuses on effective decision-making and proper accountability for risk decisions

- An IT security framework that incorporates multiple security models appropriate for different sets of business and mission requirements

State and USAID have begun to integrate the IT capabilities of the two agencies. A Joint Management Council (JMC) coordinates integration activities at senior management and working levels. The unclassified intranets (OpenNet and AIDNet) are connected, although not fully integrated. The JMC is exploring the effort required to modernize USAID's IT infrastructure so it is compatible with State's. Work is underway toward integrating financial, procurement, and other administrative systems, although much work remains. A State/USAID Joint Enterprise Architecture (JEA) is under development. Both agencies are encouraged by the progress made to date, while remaining cognizant of the significant challenges we face as we look forward to implementing this JITSP.

1.3 Stakeholder Participation in the Planning Process

This *IT Strategic Plan* was developed by an IT planning team representing both State and USAID. The Plan is driven by customer requirements that reflect the strategic and tactical goals and priorities of both agencies. Key input to the plan includes the following:

- United States Department of State and United States Agency for International Development Joint Strategic Plan, Fiscal Years 2004 – 2009
- Department of State's Knowledge Leadership Strategy (2003)
- USAID's Knowledge for Development (KfD) Strategy for 2004-2008
- Interviews with USAID and State individuals (see Appendix A)
- Overseas visits to seven US embassies and two USAID missions, and conference calls with an additional four USAID missions. Overseas visits included meeting with external partners working with USAID
- Report of the Overseas Presence Advisory Panel (OPAP), 1999
- Input received from State's electronic discussion groups
- Data from a survey conducted by State's Office of e-Diplomacy of more than 3,000 State policy and management officers worldwide
- Congressional Testimony Of John Streufert, Acting Chief Information Officer, USAID, April 7, 2005

The following additional documents were used to help provide a context and broader set of requirements and drivers for this JITSP:

- President's Management Agenda
- AIDNet/OpenNet Convergence Document
- Federal Information Security Management Act (FISMA)
- US Foreign Aid, Meeting the Challenges of the Twenty-first Century ("White Paper"), January 2004

DRAFT Joint IT Strategic Plan

- Government Performance and Results Act
- Clinger-Cohen Act
- A Vision for Inter-Agency Foreign Affairs Connectivity, white paper on the Foreign Affairs Virtual Environment (FAVE)
- Joint and individual enterprise architectures (EAs)
- Business Requirements for Information Sharing within the U.S. Foreign Affairs Community, June 2005
- The Future of the Internet, January 9, 2005, PEW Internet & American Life Project
- National Security Strategy of the United States, September 2002

2 IT Strategic Plan Drivers

Four broad drivers are the basis for this plan:

- The mission, business needs, and strategic priorities of State and USAID
- The President's Management Agenda and e-Government
- Rightsizing
- Best practices in IT

2.1 Mission and Business of State and USAID

The *Joint Department of State and USAID Strategic Plan, FY 2004–2009* states that the mission of the two agencies is to:

Create a more secure, democratic, and prosperous world for the benefit of the American people and the international community.

The *Joint State/USAID Strategic Plan* identifies the principal aims of the Department and USAID in support of this mission. These aims link diplomacy, development assistance, disaster relief, and defense. This plan identifies specific initiatives to be pursued in support of the joint mission, including Arab-Israeli peace; stability, democracy, and economic freedom in Iraq, Afghanistan, and the Muslim world; reduction of the North Korean threat; reduction of regional tensions; HIV/AIDS prevention; drug eradication and democracy in the Andean region; strengthened alliances; and alignment of diplomacy and development assistance. In carrying out their mission, the Department and USAID consult and work with other U. S. Government agencies, foreign governments, Non-Governmental Organizations (NGOs) and international organizations, foreign and domestic press, and the foreign and domestic public.

2.1.1 Department of State

The Department of State is the primary cabinet department responsible for the foreign policy of the United States. In support of the President, the Department helps formulate and carry out the nation's foreign affairs agenda and promote its national interests around the world. As documented in the *Joint State/USAID Strategic Plan*, the Department focuses on and promotes a broad range of priority goals and objectives, such as democracy, counterterrorism, peace and prosperity, global economic growth and free trade, border security, international law enforcement, and drug interdiction.

The Department operates in over 165 countries around the world, maintaining embassies in virtually every nation. The overseas posts are supported by geographic and functional bureaus in Washington, as well as specialized regional facilities that provide services in

financial management, logistics and procurement, and information technology. The Department participates in international organizations, and conducts an active outreach program to explain and promote our nation's traditions and values around the world.

2.1.2 USAID

USAID is the principal U.S. agency that provides assistance to countries recovering from disaster, trying to escape poverty, or engaging in democratic reforms. USAID fosters long-term and equitable economic growth and advances U.S. foreign policy objectives. USAID operates in 100 countries and supports programs and activities in agriculture and trade, global health, democracy, conflict prevention, and humanitarian assistance. It operates within two lines of business: development assistance and disaster assistance.

According to the USAID White Paper on Foreign Assistance in the 21st Century, U. S. foreign assistance addresses five core operational goals:

- Promoting transformational development
- Strengthening fragile states
- Providing humanitarian relief
- Supporting U.S. geo-strategic interests
- Mitigating global and transnational ills

Appendix A contains the Business Capability Map (BCM) for USAID that provides an integrated view of USAID's programs and activities. The BCM is a tool used in the process of creating an enterprise architecture. It shows the business model in a one-page snapshot to facilitate examination of different elements of USAID's "business" from a common perspective.

2.1.3 Challenges

Because of their missions and overseas operations, both State and USAID face special challenges that affect requirements for information technology and potential for joint IT activities. These challenges include:

- **Global operations** -- the two agencies operate all over the world, and must adapt to diverse political, economic, security, and cultural conditions, as well as varying levels of quality and reliability in local telecommunications and infrastructure services.
- **Reliance on external partners** -- while both organizations rely on partnerships with NGOs, contractors, foreign government agencies, and other partners, USAID is especially dependent on external collaborators. The Agency's development programs are carried out by contractors, Private Voluntary Organizations (PVOs), and NGOs throughout the developing world. USAID depends on important management information from these external partners to address the reporting requirements of key stakeholders.

DRAFT Joint IT Strategic Plan

- **Reliance on Locally Employed Staff (LES)** -- both agencies use LESs, including non-Americans, for many jobs overseas. USAID relies more heavily than State on non-American local staff for vital IT support positions at overseas missions. In many locations, this reliance results in significantly lower costs, but also creates security and resource challenges for integration with State.
- **Security** -- overseas operations demand high levels of security to protect American lives, sensitive information, and critical assets. Security considerations affect the location, design, and construction of embassies and other facilities as well as the design and deployment of IT systems and capabilities.
- **Physical Separation** -- in some countries, State and USAID facilities are colocated in the embassy compound, thus facilitating consolidation of services. Where the agencies are not colocated, it will be a challenge to deliver responsive service and provide necessary IT security in a consolidated environment.
- **Performance and results** -- State and USAID are required by law and the President's Management Agenda (PMA) to track funding and demonstrate results. The two agencies face different challenges in this area: State's work is broad, varied, nuanced, and tends to be reactive to specific situations. Thus it is sometimes difficult to formulate meaningful goals and performance targets. USAID's needs focus on program management data to support return on investment and similar analysis of development and disaster assistance efforts. Given the dependence on outside parties to accomplish much of the work and USAID's highly decentralized organization, it is difficult to obtain standardized information that supports the needed analysis.

An overarching challenge addressed by this Plan is creating an integrated IT environment to support the two agencies. There are important advantages to doing this, namely:

- economies of scale in providing support to overseas locations,
- improved service to employees,
- enhanced potential for information sharing
- alignment of information with foreign affairs priorities, and
- a critical mass of expertise and resources, such as facilities that ensure continuity of operations in the event of a disaster.

The challenges to be addressed are formidable, and include: accommodating the business, security, and staffing models of the two agencies; satisfying both agencies' critical requirements in a unified management and technical IT environment; standardizing data and information management conventions and processes; and effecting the necessary change management to blend the cultures of the two agencies.

The approach to integration is specified in Section 5.1 of this joint plan. In general, the goal of this plan is to promote the maximum level of integration and consolidation consistent with meeting both agencies' requirements, while allowing the flexibility to adapt to changing circumstances. This goal will be accomplished through careful joint

tactical planning and analysis as an outgrowth of this JITSP. This work has already begun, under the JMC, as noted above. In addition the Applied JEA has identified agreed upon collaboration opportunities in the information security and telecommunications areas. The integration envisioned by this IT Strategic Plan will be based on adopting the best practices and strengths of both agencies, supplemented by input from other government agencies, IT research organizations, and the private sector. For this joint ITSP to be successful, it must ensure that neither organization suffers any degradation in service or capabilities as a result of integration.

2.2 President's Management Agenda and e-Government

A second key driver is the President's Management Agenda (PMA), its E-gov mandate and other related government-wide IT initiatives. Through these initiatives, State and USAID will promote efficient and effective service delivery to the public, business, other USG agencies, and other governments. These initiatives also focus on delivering excellent administrative services internally to employees, and increasing coordination among agencies operating overseas. Internally, the Department and USAID will pursue the key PMA objectives of improving the management of human capital, competitive sourcing, financial management, and budget and performance integration.

The *Joint State/USAID Strategic Plan* and JEA, which are key components of e-Government, emphasize the value of information, information technology, and knowledge management as key tools in diplomacy, foreign affairs, international development, and organizational excellence. The Joint Enterprise Architecture calls for extensive communication, coordination, and collaboration between the Department and USAID, and with external organizations. The objectives and initiatives in the Joint Strategic Plan depend heavily on high quality information that can be accessed and shared appropriately and securely from anywhere and at anytime. World-class IT tools, such as video conferencing, mobile access, sophisticated data analysis, and geographic information systems are essential for State and USAID to achieve their strategic objectives and goals, and to address the needs of their customers and constituents, notably the White House, Congress, other government agencies, U.S. allies, and above all, the American people.

2.3 Rightsizing

The Joint State/USAID Strategic Plan and the PMA both emphasize "rightsizing" the entire presence of US Government agencies and personnel overseas. Rightsizing promotes enhanced mission capabilities, cost-efficiency, and security. This IT Strategic Plan supports rightsizing by promoting interagency integration, delivery of services from regional and central locations, and self-service through modern IT solutions.

"Rightsize and Regionalize the U.S. Government's Overseas Presence. The Department and USAID will work together with OMB and other U.S. Government agencies to align the number and location of staff assigned overseas with foreign policy priorities, security, and other constraints." Joint Strategic Plan



This *JITSP* explains how IT will be a significant force helping State and USAID pursue their missions over the balance of this decade. As the lead international affairs and development agencies, State and USAID are committed to exploiting IT to further U. S. global objectives.

2.4 IT Best Practices and Trends

The Department and USAID are committed to maintaining a high quality, global IT environment that can exploit advances in technology and government-wide initiatives such as e-Government. Research and interviews revealed the following key trends and best practices, which are highlighted throughout this plan. The left column in Table 2 identifies key trends that will affect IT for State and USAID for the balance of this decade.

Table 2: "In-Out" Table: Key Trends & Best Practices for State and USAID

IN	OUT
Enterprise-wide, Government-wide solutions	Single bureau, single agency approaches
Rapid technology change and adoption	Reluctance to innovate
Social and community collaboration	Individual effort
Outsourcing of non-core activities	In-house for all functions
Wireless	Wired
Next generation data mining and search	Fragmented data sources accessible in restricted ways
Mobile	Tethered to the desk
Voice/data integration/voice over IP	Separate networks
Voice input and speech recognition	Keyboards
Voice-mail/email integration	Separate message stores
Leveraging partnerships	Isolation
Automated, real-time language translation services	Limited ability to get documents translated
"Out of the box" COTS	Highly customized solutions, including overly customized COTS
Web-based	Client-server
Multi-media for effective communication	Rigid formats, cables
Enterprise-wide business continuity planning	Ad-hoc approach to critical infrastructure protection
Computing and networking as utilities	Non-standard, isolated IT environments
Adaptable networks—Self-configuring, dynamic	Hardwired networks
Dockable laptops	Desktop computers
Risk Management	Risk Aversion
Dataless posts	Expensive and vulnerable distributed data model

3 Vision—Empowering Diplomacy and Development with Information Technology

The vision for 2010 is one in which IT is an active partner supporting the mission-oriented activities of the Department and USAID. By helping organize and provide access to critical information now scattered around the world, along with state-of-the-art systems, tools, and networks, both agencies will greatly increase the value of IT investments and empower US diplomacy and international development.

Vision
*Empowering diplomacy and development
with
information and tools available anytime,
anywhere*

By 2010, through this vision, both agencies will have achieved the following:

- Ready access to the vast stores of information needed for diplomacy and development -- getting the right information to the right people at the right time to enable the right decisions and actions
- A highly integrated IT environment supporting State, USAID, and other currently supported agencies, then expanding to provide a platform for all US Government activities overseas
- Consistent achievement of customer service levels, based on cost-efficiency and best practices across agencies, using centralized and regional support models
- A centrally managed, commercial-quality IT infrastructure, remotely accessible worldwide and operating like a utility at highly competitive prices
- Lowered administrative costs and rightsizing objectives through streamlining and reliance on E-gov interagency solutions and services, with State and USAID providing some services under a Foreign Affairs Line of Business (LoB)
- Rapid adoption of technology to support emerging business requirements
- An IRM organization and workforce that demonstrates best practices in service delivery and innovation
- Fully tested, consistent business continuity program that ensures that mission critical operations will not be disrupted

DRAFT Joint IT Strategic Plan

The following scenarios illustrate how this IT vision will enable great change in State and USAID:

- USAID's development activities will be radically different by 2010. During the formative stages of a project, the program director will call on expert planners scattered around the world who will collaborate electronically via the medium most conducive for the team. Various experts in public health, economics, host nation culture, and other pertinent fields will comprise a virtual team. The best experts can be included regardless of their physical location. Contracts and grants managers and budget and finance staff will participate from their regional or central facilities. Administrative services will be available via the web or telephone from a central service provider. Technology will enable the best expertise to be brought to bear without the security risks and expense of overseas travel. As the project is underway, the program manager and other USAID managers and staff will be able to access real-time video images of field activities as well as up-to-the-minute information on project progress. Results will be tracked, measured, and interpreted via easy to use dashboards.
- The diplomat of 2010 will have access to a broad range of useful information to help explain US positions and promote our national interests. Effective multi-media information products will be available on demand, customized to meet the needs of the situation and target audience. Best-of-breed content and customer relationship management software will enable the production of these targeted information products. The modern diplomat will be freed from his or her desk, able to travel around the host country, presenting a positive image of the United States, and address any questions about US policies. Remote access to the foreign affairs virtual library will be invaluable. Everyone will be able to choose their preferred device for mobile access -- whether it be a cell phone, laptop, Blackberry, or TV.
- Ambassadors and Chiefs of Mission will be able to focus more fully on US foreign policy imperatives and strategic interests in their host countries. Communication among members of the country team will be streamlined and highly automated, regardless of agency affiliation. Secure collaboration with external organizations will be available as well. Information needed to present US positions on key topics will be readily available in the most effective form. Administrative services will be fully centralized and standardized, requiring no concerted effort on the part of overseas posts and missions. Support for acquisitions, human resources, budget and finance, and IT will be delivered from central facilities a mere click or phone call away. Services will be delivered according to an established schedule of prices and terms.

4 Goals and Objectives

The five IT goals supporting this vision and mission priorities of State and USAID are:

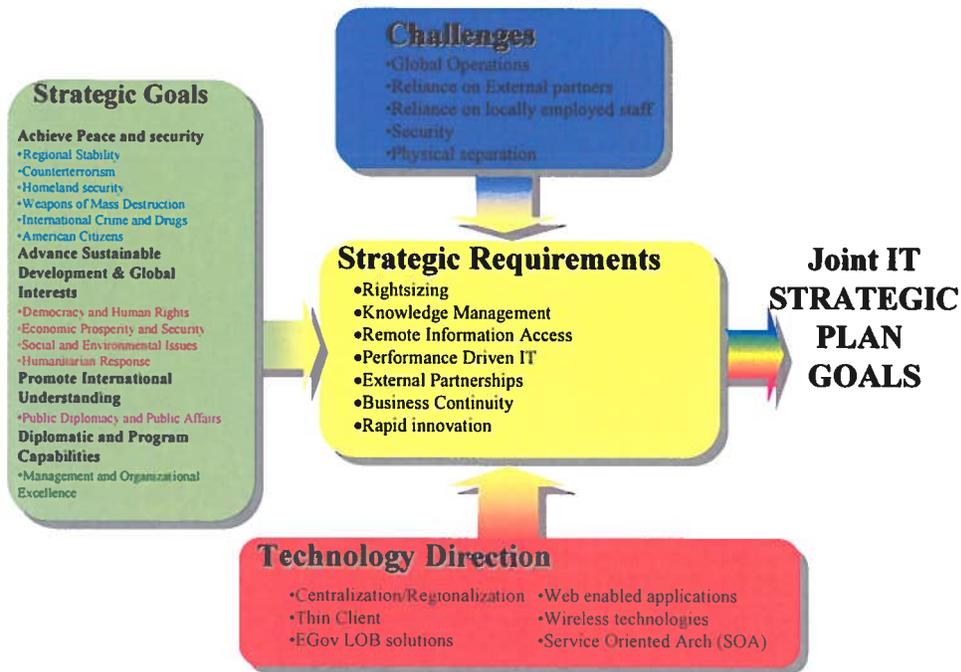
1. ***The Right Information: Knowledge Leadership for Diplomacy and Development*** – Superior diplomacy, decision-making, and management of development programs, all facilitated by readily accessible and superior information.
2. ***Anytime/Anywhere Access: Foreign Affairs Professionals on the Move*** – A well-managed IT infrastructure that makes knowledge and communication resources available to personnel when and where they need them.
3. ***External Partnership: Diplomacy and Development through Collaboration*** – Improved connectivity and collaboration with other U. S. Government agencies, nongovernmental organizations (NGOs), business, and the public — domestic and abroad.
4. ***Risk Management: Balancing Security with Business Imperatives*** – A life cycle approach to security that recognizes and balances mission needs and security risks, and ensures business continuity for all locations worldwide.
5. ***Work Practices and Workforce: Leading Change*** – IT professionals highly trained and organized for mission support and service delivery, and all non-IT staff trained to use technology effectively.

The JITSP goals focus on the strategic theme shown in the box below. Until now, investments have produced a global IT infrastructure connecting all overseas and domestic locations. With this new plan, the focus will shift to using the global infrastructure -- bolstered with enhanced capabilities and capacities -- to empower diplomacy and development.

**Strategic Theme:
Transformation
From Infrastructure to Empowerment**

Descriptions of these five IT goals are set forth in the following pages. The figure below shows how the Joint Strategic Plan leads to strategic requirements which in turn leads to the JITSP goals. Also influencing the JITSP are the challenges and technology drivers discussed above. Table 3 below maps the five goals to the Joint State/USAID Strategic Plan and indicates the impact of these IT goals on the foreign affairs mission.

DRAFT Joint IT Strategic Plan



DRAFT Joint IT Strategic Plan

This version is subject to revision and does not represent the official position of either USAID or DoS

Table 3: Examples of IT Support for Joint Strategic Plan Goals and Objectives

Joint Strategic Plan		IT GOALS				
Joint Goals	1. The Right Information					
Achieve Peace and security	<ul style="list-style-type: none"> Regional Stability Counterterrorism Homeland security Weapons of Mass Destruction International Crime and Drugs American Citizens 	<ul style="list-style-type: none"> Tailored knowledge bases on key issue areas (e.g., Middle East Peace Process) Improved linkage between related knowledge bases (e.g., WMD and counterterrorism) Intelligent search engines adapted to foreign affairs materials Production of personalized, multimedia materials on any topic 	<ul style="list-style-type: none"> Secure mobile access to classified and unclassified Portable devices contain important information needed for negotiations and persuasion “Office-in-a-box” for rapid deployments IT support for home as well as office, and support for telecommuting 	<ul style="list-style-type: none"> Integration of visa and other border security information with Department of Homeland Security. Upgraded interagency communication links and enhanced coordination for Crisis Management 	<ul style="list-style-type: none"> Flexible need-to-know policy allows wide access by foreign affairs professionals to information and analysis across issue areas and geographic regions 	<ul style="list-style-type: none"> IT workforce retrained in mission-related knowledge functions, multimedia techniques, and mobile support for diplomats
Advance Sustainable Development & Global Interests	<ul style="list-style-type: none"> Democracy and Human Rights Economic Prosperity and Security Social and Environmental Issues Humanitarian Response 	<ul style="list-style-type: none"> Integrated, global databases on USAID development projects, human rights conditions, environmental and economic issues Exploitation of Geographic Information Systems 	<ul style="list-style-type: none"> Rapid establishment of remote operations centers for first responders to humanitarian disasters 	<ul style="list-style-type: none"> Collaboration with USAID, and other U.S. Government agencies and NGOs on environmental, development, and human rights issues 	<ul style="list-style-type: none"> Rapid introduction of the best available mobile technology for field operations 	<ul style="list-style-type: none"> Integration of USAID and Department IT resources to improve support for mission-related activities of both organizations

DRAFT Joint IT Strategic Plan

Joint Strategic Plan		IT GOALS				
Promote International Understanding	<ul style="list-style-type: none"> Public Diplomacy and Public Affairs 	<ul style="list-style-type: none"> Use of Standard Customer Relationship Management tools, as developed by U.S. businesses to influence customers, but customized for the languages and unique cultural requirements of individual countries 	<ul style="list-style-type: none"> Video and Web casts for target audiences extended throughout the world Worldwide bandwidth needed for sophisticated multimedia operations 	<ul style="list-style-type: none"> Effective public relations materials that reflect benefits provided by all U.S. Government agencies (e.g., USAID development, Peace Corps projects, Social Security payments, educational grants) 	<ul style="list-style-type: none"> Unrestricted access to unclassified information and advanced Internet capabilities 	<ul style="list-style-type: none"> IT personnel retrained to create and manage content of web sites and to establish Web Logs (Blogs) for person-to-person communication with foreign publics
Diplomatic and Program Capabilities	<ul style="list-style-type: none"> Management and Organizational Excellence 	<ul style="list-style-type: none"> Recruitment and training/retraining of IT staffs to reflect balance needed between foreign affairs and technical skills 	<ul style="list-style-type: none"> Centralized IT infrastructure frees up most IT staff to serve as information consultants and advisers High levels of redundancy equals high availability and business continuity 	<ul style="list-style-type: none"> Cross-agency networks and systems 	<ul style="list-style-type: none"> Streamlined, responsive process for rapid analysis and approval of new technologies 	<ul style="list-style-type: none"> IT workforce elevated in skills and importance in foreign policy function Substantive staff skills enhanced to enable full use of IT

DRAFT Joint IT Strategic Plan

This version is subject to revision and does not represent the official position of either USAID or DoS

4.1 Goal 1 - The Right Information

"Right content, right format, right audience, right now" [Public Diplomacy Strategy]

Primary Business Objective:

- Mission effectiveness through knowledge creation, access and sharing, resulting in enhanced policy development, program planning and execution, and decision-making
- Enhanced outreach to people around the world to promote understanding of the United States and our foreign policy objectives

IT Objectives:

1.1 *Dynamic information environment* -- centrally managed, broadly accessible, secure infrastructure for value-added knowledge bases

1.2 *Specialized tools and systems* -- for document publishing and management, content management, search and retrieval, analysis and visualization

1.3 *Performance and results* -- executive information systems (EIS) and management dashboards for information aggregation and analysis to support program management and monitoring

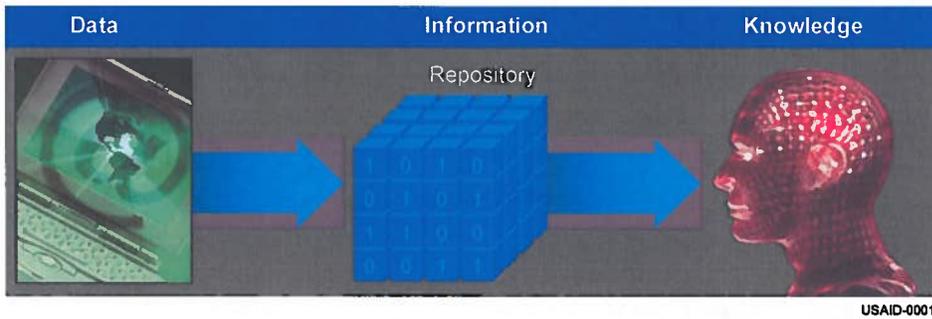
Target for Goal 1

The Department of State and USAID share a common need for knowledge management, and this Plan will leverage the experiences and meet the requirements of both. The annual output of the Department of State includes more than 1 million cables, 60 million e-mails, hundreds of thousands of indexed documents on thousands of Department web pages, and other reports, analyses and information. The information USAID requires to manage over \$16 billion in development and assistance programs is located in many disparate data stores, often under the control of partner organizations. Both agencies have access to the vast resources of the Internet, their Intranets and the networks of other government agencies. Yet, much of this information is inaccessible, of questionable accuracy, out of context, out of date, or in the wrong format. As a result, employees cannot easily find the information they need and are overloaded with marginally relevant information.

Both agencies also face equally important challenges related to results management. A key focus for USAID is improving the Agency's oversight of its programs, enabling it to inform stakeholders about how development and assistance funds are spent and what results are produced. State also must do a better job of measuring the success of US foreign policy goals, highlighting the impact of diplomatic efforts on transformation around the world, and the progress toward key strategic objectives such as promoting democracy.

Goal 1 will meet these challenges by following the approaches outlined in the Department's Knowledge Leadership and USAID's Knowledge for Development strategies. Both agencies will produce foreign affairs information tailored to the needs of individual officers, internal and external customers, and target audiences. This goal will deliver an evolving set of systems and tools for creating, discovering, managing, accessing, manipulating, sharing, and presenting information. The focus will be on adding value -- converting data into information and information into knowledge.

Modern concepts in knowledge management will provide access to implicit and tacit knowledge dispersed throughout State and USAID. Personnel will be encouraged and rewarded for sharing their expertise.



The Department of State's Acting CIO has said that State and USAID need a broad, unified policy that recognizes information as an enterprise-wide asset. This is in contrast to the current practice where the organization that gathers, compiles, or develops information treats that information as an organizational asset, sharing the information only upon specific request. This will require substantial culture change mandated from the top and reinforced through tangible incentives.

To accomplish this goal and provide top quality knowledge and information services for diplomacy, the Department will shift the balance among the competing demands for IT resources, tilting a greater share toward foreign policy requirements. This theme is discussed further under Goal 3, through which e-Government solutions will be employed to reduce the costs of administrative systems, thus freeing up resources for diplomacy.



Goal 1 Objectives

4.1.1 Dynamic Information Environment

Under this objective, State and USAID will establish an integrated environment that enables the foreign affairs professionals of both agencies to find the information they need. This environment will include:

- A *virtual repository* or *data warehouse* for internal information and selected externally generated information important enough to bring in-house. The repository will consist of structured and unstructured information in all forms. Currently unstructured information is captured in such formats as emails, cables, memoranda, reports, graphics, photos and audio and visual media. Structured information is captured in a variety of dedicated and specialized databases. In the future, these information products will be managed as an enterprise-wide corporate resource under the direction of a professional, dedicated staff of information experts. The bureaus will be able to use the repository to build value-added knowledge bases, addressing for example counterterrorism, democracy, and other strategic topics. There will be tools for collecting, culling, organizing, and adding value to raw data so that users can gain maximum benefit.

A repository, accessible from anywhere around the world, will provide up-to-the-minute official policy statements and talking points on hot issues of the day -- democracy, global warming, trade, labor, and terrorism. .

- An *indexing capability* (taxonomy) for classification, metadata, search and retrieval to enable people to find what they are looking for easily and quickly. The taxonomy will be useable for both internal and external information sources. We will leverage interagency metadata efforts (e.g., government-wide XML) being carried on by the intelligence community, GSA, and others.
- An *information service or virtual library*, staffed by professionals in library and information science, working with foreign policy and development experts, to assist in finding, accessing, and processing information. This service, which is based on State's proposed Diplomatic Research Service and USAID's Knowledge for Development Centers, will be responsible for managing substantive databases and content management tools, supporting and facilitating communities of practice, and assisting users with complex information management requirements.

Lessons learned and success stories will be readily accessible, capturing information on a world-wide, cross-agency basis. For example, USAID missions implementing agriculture development programs will be able to access best practices and successes obtained in other USAID missions around the world.

- **Central web site management** that aggregates all Intranet information in a secure common environment to give users easy, desktop access to essential information and services. Intranet websites will be managed by a central content management service that will make it easy for users to post current information and share knowledge as part of their everyday work. Web publishing will be centrally funded and supported.

In the future, a central organization will manage all web site development and information publishing, recognizing that the information being posted is a core enterprise-wide asset. This organization will also manage the dissemination function, focused on customers and stakeholders. Posts and bureaus will continue to provide content, but the responsibility for web-based presentation will be centralized.

- **Collaboration environment** that supports self-forming, self-managing professional networks and communities of practice and interest to overcome boundaries of geography, time and organization — both classified and unclassified. This collaborative environment will encourage teamwork and spark creativity. Collaboration tools will allow users to establish virtual teams focused on specific issues, geographic areas, or business functions. The members of the virtual teams can be based in different geographic locations, and can work together in real-time and off-line. The collaboration environment will also include an expert locator and the ability to locate expertise in both agencies.

Messaging will evolve to a web-based environment in which today's emails, cables, and memoranda will be centrally stored, managed, indexed, and retrievable in multi-media formats via an enterprise-wide database, accessible from anywhere at any time.

4.1.2 Specialized Tools and Systems

The state of the art in information management tools is evolving rapidly. By 2010, highly sophisticated capabilities will be readily available, in such areas as voice recognition, intelligent search and retrieval, tools that learn and adapt to the needs of individual users, foreign language translation, visualization, and publishing and presentation tools. The key to success in this area will be the ability to incorporate new tools into the environment quickly and enable users to benefit from them rapidly. This will require:

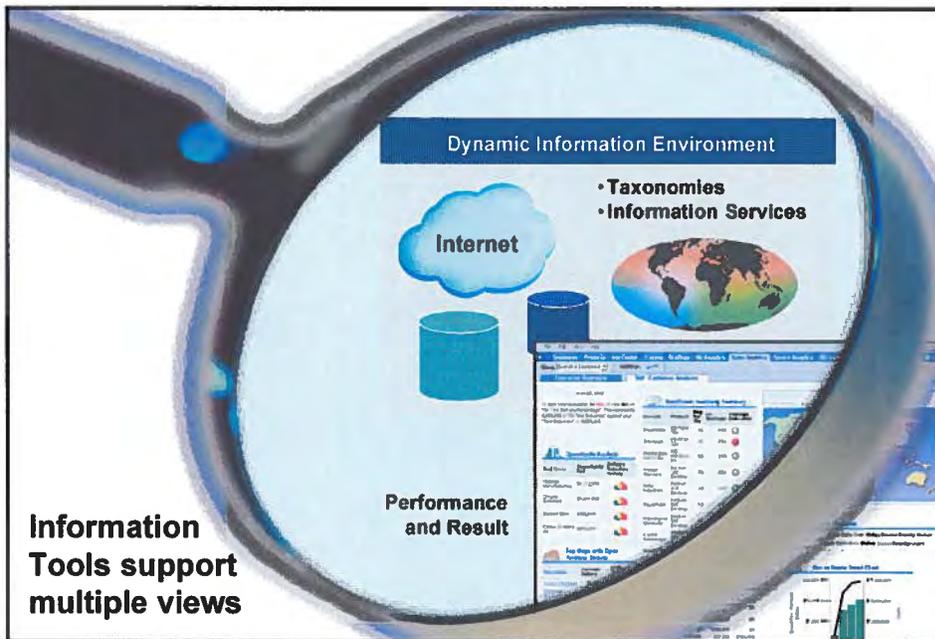
- a nimble decision-making and risk management structure, wherein business managers consider risk factors at every decision point;
- highly skilled technical staff who understand business requirements and use that understanding to identify, analyze, implement, and integrate tools and systems rapidly; and

- excellent training and change management support to ensure that end-users can exploit the capabilities productively

Army embraces COTS and rapid support for the field -- The Army has embedded acquisition specialists among combat units in the field to work with commanders to understand requirements, acquire COTS solutions, and deploy them rapidly to further mission objectives.

An illustrative set of tools is listed in the figure below. The paragraphs which follow describe examples of particularly important tools, along with their potential value for State and USAID.

Development and Diplomacy

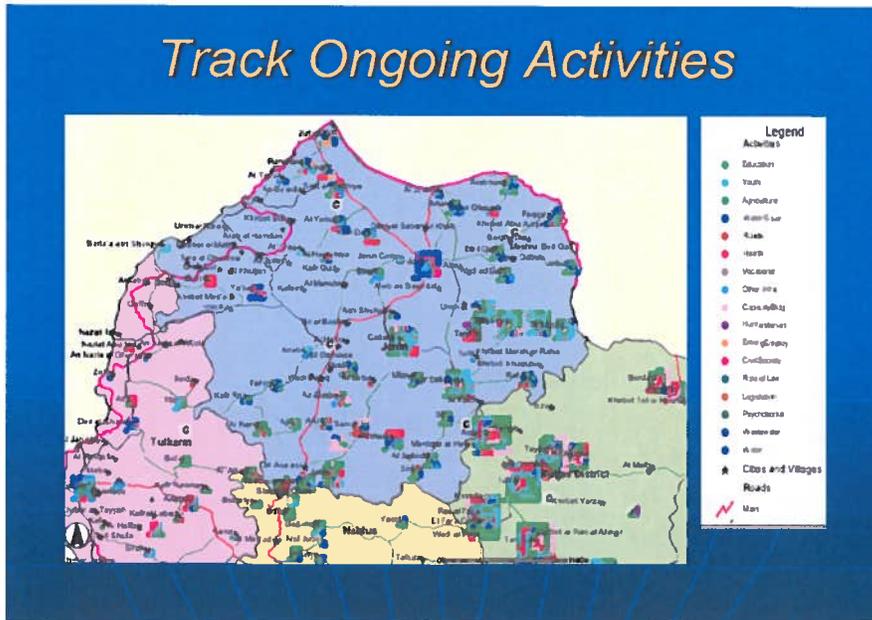


USAID-0004

A Customer Relationship Management (CRM) system and process will be provided for capturing and sharing relevant information regarding foreign and domestic customers and other contacts, customers' needs and priorities, and preferred communication channels. This capability will increase the effectiveness of customer/contact engagements and enable staff to share contact-related information across the enterprise. This is an essential tool for Public Diplomacy, for tracking embassy and domestic contacts, and coordinating with partners in development programs.

Content Management (CM) will be supported by a system for organizing and publishing information to web sites and other output media. It will include capabilities to draft or import material, route drafts through a dynamic workflow process, and publish content for multi-media access.

Portal Technology will be implemented to allow end-users to customize their virtual work environments for easy access to material of most interest to them. Specific capabilities, such as news, messaging, bookmarked web sites, and search tools will be accessible via the portal.



Knowledge and Information Management Tools:

- Contact/customer relationship management (CRM)
- Content management
- Customizable portals for organizing information and windows
- Collaboration
- Instant Messaging (IM)
- Customized multi-media information products and presentation
- Intelligent, personalized, adaptable search engines
- Geographic Information Systems (GIS)
- Visualization for presentation and analysis of information
- User-friendly data management and analysis tools
- Document abstracting, cataloging, and profiling
- Data mining and pattern analysis
- Dashboard for program monitoring and results
- Knowledge Management—expert locator, real-time question and answer
- Media search and capture technologies
- Interactive web tools, such as Wikis (interactive encyclopedias) and Blogs (on-line journals) and other emerging technologies

Some USAID contractors and NGOs use sophisticated capabilities for program management and reporting to USAID missions and Washington. They have remote access to web applications, databases, GIS, and interactive portals. State and USAID will implement these types of capabilities under this objective.

4.1.3 IT Capabilities for Performance and Results

An important priority for both agencies is to improve management information and oversight of programs and activities. For the Department, there will be increasing requirements from oversight groups and the American public to demonstrate tangible results in pursuing strategic priorities such as promoting democracy and counterterrorism. For USAID, a key priority is to improve program management and oversight of its development activities and funds management. USAID's objective is twofold: (1) to provide ready access to accurate information that will enable management to direct how foreign aid funds are spent and ensure that they are being spent according to plan and priorities; and (2) to monitor the results produced as a result of the development assistance that the US provides. Both agencies have begun to address these challenges through Executive Information Systems (EIS) and dashboard capabilities.

USAID's EIS will provide a mechanism for aggregating information from multiple internal and external sources on how funds are allocated and spent. It will also provide a means to establish metrics for desired program results, and then to compare actual results with these metrics. It will tie together information on program budgets, procurement, funds actually spent, status of program execution and delivery, and results achieved. In

addition, the EIS will be used to track internal management and administrative activities of both State and USAID, enabling informed decisions about investments and ensuring that results are being achieved.

State's Strategic Planning Office (RM/SPP) is developing a Global Affairs Dashboard capability to track programs and activities. The electronic Global Affairs Dashboard (e-GAD) is a web-based tool that will provide integrated visibility, analytical capabilities, and decision-making insight into planning, performance, and resource information by bureau/office, mission, and strategic goal of integrated performance and budget data. The tool will enable both the Department and USAID to meet the President's Management Agenda Item of Budget and Performance Integration.

Goal 1 Strategies

Table 4-1 highlights the key strategies needed to accomplish the Goal 1 objectives.

Table 4-1: Goal 1 Strategies

Strategy	Key Components	Performance Indicators
Information/Data Architecture Framework	<ul style="list-style-type: none"> • Categorization schema – developing a standardized vocabulary • Thematic Communities of Practice – centered around shared information needs • Linkage of Business Processes to supporting Information 	<ul style="list-style-type: none"> • Increased information sharing opportunities across organizations • Controlled redundancy and increased consistency in information • Increased ease in finding, analyzing and managing information
Knowledge Management	<ul style="list-style-type: none"> • Knowledge-sharing culture and leadership • Information-sharing architecture and collaboration tools 	<ul style="list-style-type: none"> • Number of people participating in knowledge sharing
Integrated data management strategy	<ul style="list-style-type: none"> • Data stewardship policies • Baseline data architecture inventory • Data exchange and integration standards • Data security policies • Data storage/warehouse • Enterprise-wide database administration (DBA) function 	<ul style="list-style-type: none"> • Growth in volume of data in central repository(ies) • Increased data quality • Increased number of queries to central databases and data warehouse • Increased connections among databases • All official documents, including emails, included in searchable archive
Information service, virtual library	<ul style="list-style-type: none"> • Organizational/staffing approach -- combination of virtual and physical • Scope of services and service delivery metrics • Service delivery and pricing 	<ul style="list-style-type: none"> • Growth in use of and demand for services from internal and external users • Quality of information products • Responsiveness to customer demand

DRAFT Joint IT Strategic Plan

Strategy	Key Components	Performance Indicators
Dashboard/EIS	<ul style="list-style-type: none"> • Initial capability for USAID • Standards for data reporting, mandatory for contractors, NGOs • Expanded capability for State oversight and reporting • Support & training for data entry by external partners 	<ul style="list-style-type: none"> • Ability to satisfy stakeholder queries • Extent of use by USAID and State executives, and external stakeholders
Evolving suite of innovative and collaborative tools	<ul style="list-style-type: none"> • Baseline suite of tools • Capability to integrate new tools rapidly 	<ul style="list-style-type: none"> • Time to implement new user capabilities • Effectiveness in meeting user needs for information management • Extent of user participation in collaborative workspaces

4.2 Goal 2 – Anytime/Anywhere Access

"The Department and USAID have the ability to make great progress in IT coordination and integration, not simply because of shared goals, but because of shared global locations."

Primary Business Objectives:

- Mission effectiveness through (1) ubiquitous access to information and systems for telework and out-of-the-office activities; and (2) a continually refreshed infrastructure with the capacity and service levels to support diplomacy and development
- Economies of scale through network and systems integration with USAID

IT Objectives:

2.1 *Mobile Computing* -- full support for end-user devices and services, such as laptops, PDAs, cell phones, blackberries, wifi, wireless networks, and newer innovations

2.2 *Performance-driven IT infrastructure* -- worldwide 7x24 end-to-end availability, adaptability, reliability, and capacity to meet dynamic global requirements and service levels

2.3 *Common Infrastructure* -- flexible, secure infrastructure to support State and USAID

Target for IT Infrastructure and Anytime/Anywhere Computing

Goal 2 will provide an IT environment -- infrastructure and end-user devices-- that allows full access to all needed knowledge and computing resources at anytime from anywhere in the world. This goal will also extend the infrastructure to USAID, along with the necessary security, architectural, and policy elements needed for integration.



USAID-0008

The end result will be a common global IT infrastructure that supports State and USAID. The common infrastructure addresses the telecommunications services of telephones, wireless access devices, radios, video telecommunications, data networks, messaging, and communications acquisition. This joint infrastructure will be centrally managed and governed by rigorous service and performance standards. The infrastructure will be dynamic and function much like a utility, providing base services for all with market-based pricing for add-ons, and allowing organizations and individuals to plug into it with a diverse set of end-user devices. The infrastructure will be based on commercial and government standards, so that it can easily accommodate new devices and capabilities as they become available on the market. The joint IT infrastructure will be adaptable, scalable, and "self-healing", that is with the capability to recover quickly from any disruption so that it is always available.

The joint infrastructure will comprise both classified and unclassified networks, linked by guard technology that enables users to move information back and forth securely. A single unclassified network will be in place, supporting multiple levels of access to accommodate the security requirements of both agencies. This common infrastructure will form the basis for eventual extension as a platform to support all agencies that operate overseas.

Many USAID contractors and NGOs have fully mobile computing capabilities that include laptops, Internet service, satellite links, GPS, imaging, VOIP, IM – all from very remote area providing full 24x7 access to their systems and databases. USAID field technicians require the same level of support.

The IT environment of 2010 will be characterized by:

- Standardized, centrally managed global infrastructure at all State and USAID locations
- Always on, available everywhere, responsive to customer needs
- Mobile access to all information resources from an evolving set of end user devices
- Base services for all with market-based pricing for add-ons
- High levels of information security and integrity, with no loss of functionality and customer convenience, through effective controls (e.g., PKI, single-sign-on)
- Services based on end-to-end performance standards and metrics
- Reliance on commercial products and services, without customization
- "Plug-in" utility-like capability

Goal 2 Objectives

4.2.1 Mobile Computing

By its nature, the work of State and USAID entails extensive travel and mobility, as well as regular contact with people outside of US Government facilities. The Information Access objective will provide technology to support the mobile employee. It will enable State and USAID personnel to use standard commercial wireless personal digital assistants (PDAs), cell phones, laptops, and a wide range of new devices as they emerge. These devices will deliver the knowledge resource products described under Goal 1, and will allow full connectivity from home, while on travel, or at meetings.

The networks and end-user devices of the future will have embedded intelligence to recognize and react to varying conditions, tailoring their configurations and security features appropriately. The following scenario illustrates how this will work: as the political officer of the future leaves the embassy to call on the foreign ministry, his PDA/cell phone is automatically reconfigured to continue to receive only unclassified messages while out of the secure embassy facility. In the car, the officer checks e-mail via phone and learns of an urgent requirement to deliver a new demarche to the host government.

Personnel will be able to telecommute and have access to all necessary information including their classified and unclassified e-mail, documents, files, voice mail, contact information, and will be able to participate in secure video and audio conferencing—all while at home or on the move. Should natural disaster or security threats occur at the work place, these innovations also will be a key enabler for continuity of operations as employees can continue to work off-site (as discussed in Goal 4).

By 2010, a substantial portion of the workforce, in the US and overseas, will telework at least part of the time. They will have easy-to-use, robust IT tools -- Internet-based access to OpenNet, dockable laptops, cell phones, PDAs -- all of which give them full access to the information and systems they need from wherever they are. Unlike today's environment, both agencies will rely exclusively on out-of-the-box commercial end-user devices, with all required security and configuration management built into an intelligent central environment.

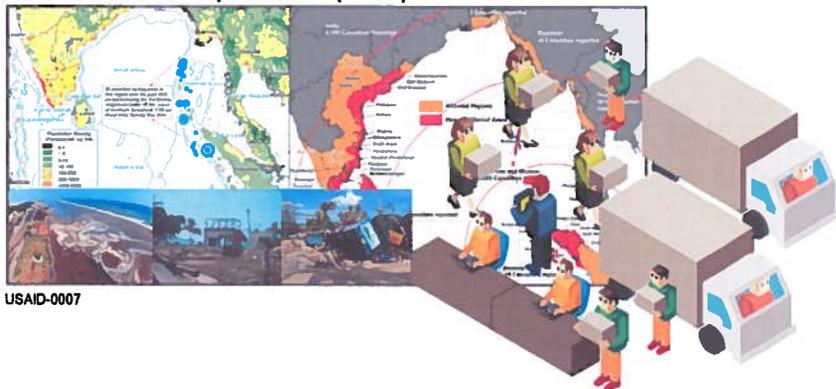
Effective diplomacy and development require the following kinds of activities conducted outside of Government offices:

- participation in policy discussions with home office and other U.S. Government executive agencies and with Congress,
- meetings with counterparts in foreign governments and non-Governmental organizations overseas,
- participation in conferences,
- attendance at sessions of foreign parliaments and other organizations,
- representing the U.S. before foreign and domestic organizations and publics, and
- traveling to other cities and countries for official visits, information gathering, and other temporary duty assignments.

Our most effective State and USAID personnel cultivate relationships with foreign officials, parliamentarians and citizens, using these relationships to acquire expertise about the host country, to understand developments that affect U.S. national interests, to implement programs and to promote U.S. foreign policy and development objectives. Much like others involved in advocacy or public relations, our personnel spend a good deal of their time out of their offices in circumstances where effective access to IT systems and information is essential.

Much of USAID's work is done in remote locations overseas, and effective program oversight requires meetings and site visits, necessitating frequent work outside the office. USAID has been increasingly involved in disaster relief, responding to such events as the recent tsunamis and earthquakes in Southeast Asia. Key to emergency assistance are Disaster Assistance Response Teams (DARTs), rapid response task forces that can be mobilized very quickly, as needed anywhere in the world. To be effective, these teams need remote access to IT systems and information; they have some capabilities today, but will need much more in the future.

Disaster Assistance Response Teams (DARTs)



When the USAID DART sets up operations in a remote part of the world, it is fully equipped with the latest in mobile and collaborative technology and with full access to all applications and data needed to support its vital disaster relief mission. NGOs, contractors, Headquarters and mission staff are all "kept in the loop" automatically as much as they want and need to be.

4.2.2 Performance-driven IT infrastructure

This objective will create and maintain the next generation global IT infrastructure -- one that functions like an electric or telephone utility. The infrastructure will be ever-present and always available, ready and waiting for end-users to plug in and connect. Much as we plug our personal electrical appliances into outlets just about anywhere, so too will we be able to connect our laptops, cell phones, ultra-thin client computers (i.e., those with no data and very little software) and all of the other devices not yet conceived. This is done today in thousands of coffee shops around the world, and all elements of the necessary technology are in place. The key to this objective is a strategic concept of how to engineer, configure, secure, deploy, operate, refresh, and pay for such an infrastructure.

The global infrastructure of the future will be based on an architecture that mirrors the evolving business model of the Department and USAID -- that is, it will support regionalization and centralization, meshed communication channels that facilitate flexible information flows, and ability to scale capacity to meet changing demand.

This objective will permit the department and USAID to centralize most information and processing power, leading to "dataless" posts and missions. The benefits of dataless posts are:

- Enhanced information security, as sensitive information need not be stored in hundreds of locations around the world;
- Enhanced personnel security, as most administrative services and personnel need not be located at risky overseas locations; and
- Increased efficiency and performance, as service delivery is managed as a central resource with professional oversight, service level targets, and competitive sourcing to ensure cost-effectiveness

The Department and USAID will outsource the bulk of telecommunications and data services to take advantage of the high availability networks and competitive price benefits in the global marketplace. Commercial carriers will provide the necessary network capacity and performance to support new initiatives and expanded mobile diplomacy and development through highly secure, private network communications facilities.

Both agencies will explore the use of open source options to reduce dependence on a single vendor for critical operating system software and to reduce security risks.

Five elements must be in place to enable "anytime, anywhere" connectivity:

- **Always on**—a global, meshed network as reliable and adaptable as today's telephone and electric utilities. The future network will provide sufficient redundancy and fault-tolerance to ensure that it is always available.
- **Everywhere**—the future Global Network Infrastructure will provide secure access via the Internet to enable the mobile worker to access enterprise data, via "personal or commercial bandwidth," to supplement enterprise bandwidth.
- **Security**—IT security solutions and updated policies will be required in order to exploit the full capabilities of mobile computing devices. Security will be built into the backend processors, enabling expanded use of off-the-shelf products without today's heavy customization.
- **Bandwidth**—substantial network capacity will be needed to meet the goals of mobile diplomacy, and the Department will establish plans for delivering bandwidth on demand using multiple sources and paths, including paths that support regionalization and centralization.

- **Global directory**—a highly reliable government-wide international affairs directory, with entries for key NGO and foreign government staff, is necessary for the comprehensive connectivity requirements of modern diplomacy and development. The global directory will be extended beyond white, yellow, and blue pages to include green pages (information) and real-time information about users' whereabouts and preferred delivery devices.

We will provide "end-to-end" performance management, no longer thinking that connectivity stops at the entrance to the embassy or mission. We will ensure adequate performance and reliability to the end-user device whether it is located in the embassy compound, at warehouse facilities, or other locations where users work.

4.2.3 Common Infrastructure for State and USAID

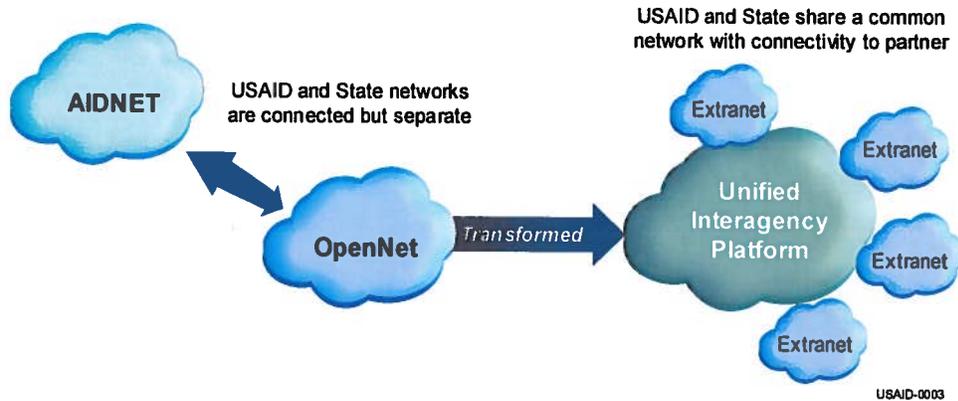
The global IT infrastructure of the two agencies will be consolidated during the first two years of this plan. The consolidated environment will be capable of supporting all of USAID's requirements, including connectivity with a broad range of external partners via secure extranets as discussed under Goal 3. The integrated environment will be a product of the strengths of each agency's network and support environment, capitalizing on the following best practices:

- Extension of State's Global Information Technology Modernization (GITM) to all components of the global infrastructure
- Extension of the Enterprise Server Operations Center (ESOC) to all State Bureaus and USAID
- Consolidation of the security models of both agencies to ensure a flexible, robust, secure platform for anytime, anywhere access
- Development of a service oriented end to end management approach

The consolidated environment will be based on policies and architectural elements that support the requirements of both agencies. The following common elements will be blended as this objective is pursued:

- Management policies
- Network and systems architecture
- Network and systems administration
- Remote management
- Technology replacement and modernization

DRAFT Joint IT Strategic Plan



Several issues will be addressed to integrate the two agencies' networks. One is that USAID permits remote access by system administrators to diagnose and, if possible, repair network and system problems. This is especially efficient for ensuring around the clock coverage by administrators. State's network policies do not currently permit such access, but will be modified to do so in the future. A second is that USAID's infrastructure has not been refreshed to the level of modernization comparable to State's. This Joint ITSP would bring a fully modernized infrastructure to USAID employees through an expansion of GITM. However, significant resource shortfalls must be addressed to allow substantial network integration. A recent study indicated that USAID would need \$180 million to bring its network up to State's standard.

Goal 2 Strategies

Table 4-2 highlights the key strategies needed to accomplish the Goal 2 objectives.

Table 4-2: Goal 2 Strategies

Strategy	Key Components	Performance Indicators
<p>Mobile computing/end-user device program</p>	<ul style="list-style-type: none"> • Full user capabilities from mobile devices -- eliminate restrictions and customization • Virtual organization and telework, providing personnel flexibility to vary their hours and work locations 	<ul style="list-style-type: none"> • Range of mobile devices connecting via the Internet or permitted on network • Comprehensiveness of capabilities available via remote devices • Numbers of users with OpenNet Everywhere (ONE) or other mobile devices • Numbers of teleworkers and time spent teleworking
<p>Consolidation, integration, and standardization</p>	<ul style="list-style-type: none"> • Enterprise server operations centers • Global networks and processing centers to meet user needs • Central remote management of all components to reduce costs and improve security • Identify and build on best practices • Expand use of thin client model to reduce costs and improve security 	<ul style="list-style-type: none"> • Single unclassified network • Number of distributed processing facilities eliminated • Volume of information processed and residing centrally/regionally • Measurable reduction in burden on posts for technical administration (e.g., patch management)
<p>Replacement and Modernization</p>	<ul style="list-style-type: none"> • Expand GITM to cover entire infrastructure and USAID • Implement adaptable deployment methodologies • Implement flexible deployment configurations 	<ul style="list-style-type: none"> • Percentage of replacement and modernization activities under GITM

DRAFT Joint IT Strategic Plan

Strategy	Key Components	Performance Indicators
Networking strategy	<ul style="list-style-type: none"> • Outside global network assessment/reengineering • Integrated network model for State and USAID • Latest Internet Protocol standards (IPv6) • Voice Over IP (VOIP) • Partner with Internet2 and Next Generation Internet (NGI) initiatives 	<ul style="list-style-type: none"> • Reduction in worldwide costs for telephone service • "Connectedness" -- multiple links to ensure always connected • Network problems no longer cited as impediment to progress
Competitive Service Delivery	<ul style="list-style-type: none"> • Desktop services managed as a utility • COTS with no customization • Innovative contracting, outsourcing, competitive sourcing, and other privatization options • Fee for service to ensure that services respond to demand and are cost-competitive • Loosely coupled, highly cohesive business modules providing services • Established Service Level Agreements (SLAs) with agreed-upon performance standards and metrics 	<ul style="list-style-type: none"> • Performance that meets SLAs • Elimination of duplicative systems • User satisfaction

4.3 Goal 3 - Supporting External Partnerships and Leveraging e-Government

"We will strengthen our administrative systems and pursue collaborative solutions to Web-base, centralize and integrate our IT systems."

Primary Business Objectives:

- Mission effectiveness through external collaboration and information sharing, promoting homeland security, border security, and rightsizing US overseas presence
- Management efficiency through e-Government solutions, streamlining, and rightsizing
- Enhanced service to US citizens in areas such as passport issuance, travel information, contracting and purchasing, and grants management

IT Objectives:

3.1 *External Collaboration* -- secure extranets and e-commerce for interchange with external, non-governmental partners and the public

3.2 *Unified interagency infrastructure* -- expansion of the State/USAID infrastructure to include the entire foreign affairs and homeland security community

3.3 *e-Government Lines of Business Solutions* -- pursuit of the PMA and reliance on government-wide administrative applications and services

3.4 *Rightsizing* -- IT as an enabler of centralization and regionalization

Target for External Partnerships

Under Goal 3, the Department and USAID will extend the information assets and infrastructure created in Goals 1 and 2 to include other Government agencies and external partners. The utility-like IT infrastructure will be expanded using components of eGovernment initiatives to enable flexible and secure connectivity and information sharing, allowing controlled access for authorized people both within and outside the US Government. By 2010, a global electronic community will be in place connecting all participants in US diplomacy and development programs. Layers of access will be supported to balance information security and access requirements, based on logical and physical controls.

This goal draws on the concepts of e-Government to streamline and consolidate lines of business, leveraging government-wide solutions and best practices. Shared systems and databases for all administrative processing will be the norm by 2010. The key to achieving these objectives is a comprehensive Joint Enterprise Architecture (JEA) addressing the needs of State and USAID, and providing a platform for expansion to all agencies operating overseas.



USAID has developed expertise as an overseas procurement and grants management organization. The Agency knows how to engage the private and non-profit sectors around the globe to carry out development and disaster assistance programs rapidly. To support this expertise, the Agency is focused on systems that draw data from multiple sources to support program execution and oversight and results tracking. Procurement, grants management, financial management, human resources, and program management systems must be engineered to produce consistent and reliable management information. This goal supports this initiative by:

- *Providing connectivity with partners who are major data suppliers*
- *Leveraging best of breed e-government solutions*
- *Streamlining and reengineering business processes*
- *Integrating current stovepipes of information and automation*

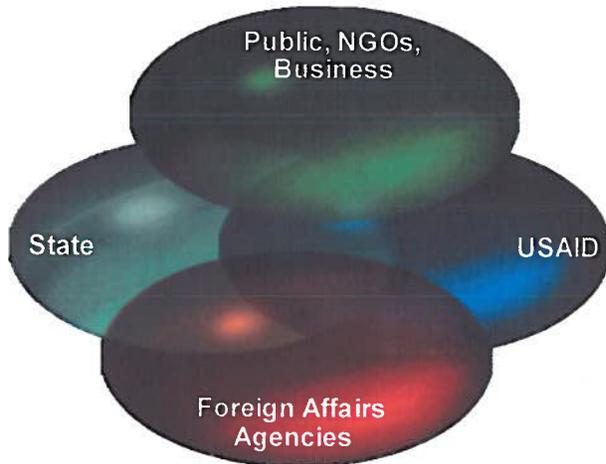
A unified environment for interagency collaboration at overseas posts will further strategic goals in the areas of homeland security, rightsizing, and e-Government lines of business. The Foreign Affairs Virtual Environment (FAVE) is a starting point for moving toward this interagency network. The unified environment will support the establishment of virtual teams, assembled dynamically with participants from multiple agencies as needed to address specific issues.

Goal 3 Objectives

4.3.1 External Collaboration

The Department and USAID work in concert with other US Government agencies, Non-Governmental Organizations (NGOs), Private Voluntary Organizations (PVOs), contractors, the public, the media, and foreign governments in promoting the U. S. foreign policy agenda. They also offer services to U.S. citizens and businesses, such as travel assistance and support for international trade and exports.

DRAFT Joint IT Strategic Plan



USAID-0002

USAID has a requirement to provide system and information access to partners based on a risk profile different from State's. Use of logical and physical controls, such as e-authentication and compartmentalizing of data stores, will permit both agencies to meet business requirements on a shared, virtual network. This approach will provide a basis for expansion to other agencies as well.

This objective will provide the IT support to enable State and USAID to work collaboratively with their non-governmental partners. The focus will be on the following:

- ***Flexible, secure extranets***-- extending the internal networks to allow external partners controlled access to information and systems, and to supply data needed for program oversight. These extranets will be accessed via secure portals that support diverse security profiles to enable authorization and authentication of non-Government personnel without compromising system and data integrity. Access will be provided via the Internet and US Government networks.

USAID's OFDANet is an example of a successful extranet. The Office of Disaster Assistance maintains a portal and collaboration facilities using e-Room to enable disaster response teams to post and share information and coordinate activities. Each team sets up and administers its own workspace with appropriate security profiles within corporate security and administrative policies and guidelines. Access controls operate at the level of individual documents, data fields, and individuals. Sensitive information can be restricted while other information can be broadly accessible.

- **Collaboration** -- exploiting advances in technology to provide cost-effective methods for working collaboratively with external personnel. An array of technologies will be available to suit different requirements and working styles. Included will be electronic meetings, information repositories, video and audio teleconferencing, electronic decision-making tools, etc.
- **Public diplomacy** -- using technology, such as interactive web sites, for Public Affairs Officers to stay connected with their sources, to produce and deliver customized, multi-media information products, and to monitor the global media and publics for reactions to US policies and actions.

Virtual Presence Posts (VPPs) will take advantage of technology advances and provide expanded services to communicate with overseas publics.

4.3.2 Unified Interagency Infrastructure

"The United States currently lacks a nationally focused effort to generate a truly collaborative information environment by coordinating the resolution of legal, policy and technical issues across all agencies and all levels of government," Congressional Testimony of Dr. Linton Wells II, Acting Assistant Secretary Of Defense (Networks And Information Integration) and Chief Information Officer, October 26, 2005.

The need for a single, integrated platform and network supporting all overseas US Government operations has never been greater or more apparent. Interagency collaboration and exchange of information are vital to our nation's security and the promotion of US interests around the world. This need will be addressed through a Unified Interagency Platform established under this objective. This objective will be achieved by the end of this decade and will provide secure connectivity with all US Government agencies, building on e-Gov initiatives such as HSPD 12 for e-authentication. Any US Government employee will have access to information from any other agency, subject only to appropriate authorization. This will require a consistent security posture across the entire foreign affairs community, a component of Goal 4.

Interagency collaboration requires adoption of consistent approaches to information security, exchange, and management across the Government. Today, agencies differ in the extent to which they classify data and in their use of classified and unclassified networks. State officers overseas tend to use the classified network extensively even for unclassified traffic. USAID and other agencies with minimal access to the classified environment are left out of these conversations. Process changes and technology will be used to address these issues and promote effective collaboration. Thin clients and remote access devices will provide broader access for USAID, PAOs, and consular officers to classified information while outside the embassy and CAA.

The report of the Overseas Presence Advisory Panel (OPAP) in 1999 made a strong case for such a network as a way to promote better information sharing and coordination across agencies at overseas posts and missions, and as a step in rightsizing the overseas facilities. The tragedy of September 11, 2001, and the many threats against embassies and personnel have magnified the need for greater coordination as well as the need to reduce our overseas presence dramatically.

Dozens of US agencies operate distinct networks and systems overseas, inhibiting information sharing and increasing overall costs. A common platform supporting overseas operations will promote efficiency and interagency connectivity.

The FAVE initiative will be refined to support the planning for a Government-wide foreign affairs network. The network will provide seamless communications across agencies at overseas posts and missions. This will, for example, better enable the Bureau of Consular Affairs at State and the Department of Homeland Security to coordinate the screening of foreign visitors and prospective immigrants. The single platform and network will permit instantaneous access to critical information regardless of which agency initially collects and maintains it. It will enable experts from multiple agencies to coordinate on issues, and will ensure that the US Government presents a united and effective front around the world. In pursuing this objective, both agencies will exploit the experiences and lessons learned from current government-wide networks such as SIPRNet and OSIS.

The core outcome will be a single government-wide foreign affairs network. All overseas personnel will have access to everything they need through this integrated environment. This will include government-wide and home-agency systems. Web-based data and applications, which will predominate in the future, will be accessible directly, much as one accesses the Internet. Other agency-specific applications will be made accessible in various ways. The management of this network will require an interagency configuration control board (CCB) and trusted end-user authentication among agencies.

This objective explicitly supports OMB's goal of a U.S. Government-wide Enterprise Architecture -- focused on the foreign affairs community. The integrated network will require a consistent, Government-wide approach to the following:

- User authorization and authentication, relying on the e-Gov solutions for identity management such as e-Authentication and other methods for personal identity verification mandated by Homeland Security Presidential Directive (HSPD)-12
- A consolidated global directory of users from all affected agencies
- Service Oriented Architectures (SOA) and Enterprise Application Integration (EAI) to share data, services and business processes with internal and external partners
- A governance process through which all agencies participate in ensuring that evolving requirements are met and policies are continually adjusted to reflect new developments
- Conformance to the Joint Enterprise Architecture (JEA), including network standards, to ensure consistency and enable interagency operations.

4.3.3 e-Government Lines of Business (LOB) Solutions

The Department and USAID are committed to the President's Management Agenda and are eager to participate in government-wide initiatives, such as today's e-Government efforts based on Lines of Business (LoBs). Both agencies look forward to scaling back their internal administrative operations as a result, thus freeing up resources that can be devoted to foreign affairs activities. By 2010, they expect to be using government-wide systems and services for many administrative activities, and to provide services to other agencies through a Foreign Affairs LoB for functions unique to overseas operations (e.g., arranging local hiring, housing, and purchasing).

The Department and USAID will be eager customers of government-wide services when available for Human Resources, Payroll, Finance and Accounting, Logistics, and Inventory and Asset Management. Given the need to support administrative operations at more than 300 locations around the world, both agencies will benefit greatly from government-wide services and systems that enable streamlining of our overseas presence. State and USAID will similarly provide such services in the Foreign Affairs sphere, freeing up resources from other agencies now devoted to sustaining overseas operations. As LoBs are expanded to cover substantive areas such as health, environmental affairs, or trade, State and USAID will participate in these as well.

State and USAID will reengineer business processes and application systems to gain efficiencies in the short term and support transition to government-wide solutions in the longer term.

State and USAID Participation in 24 Quicksilver e-Government Initiatives

<p>Government to Citizen</p> <p>Recreation One-Stop GovBenefit.gov E-Loans USA Services IRS Free File</p> <p style="text-align: right;"><i>Interior Labor Education GSA Treasury/IRS</i></p>	<p>Government to Business</p> <p>E-Rulemaking Expanding Electronic Tax Products for Businesses Federal Asset Sales International Trade Process Streamlining Business Gateway Consolidated Health Informatics</p> <p style="text-align: right;"><i>Transportation Treasury/IRS GSA Commerce SBA HHS</i></p>
<p>Cross Cutting = E-Authentication GSA</p>	
<p>Government to Government</p> <p>Geospatial One-Stop Grants.gov Disaster Management SAFECOM E-Vital</p> <p style="text-align: right;"><i>DOI HHS FEMA Treasury SSA</i></p>	<p>Increased Efficiency and Effectiveness</p> <p>E-Training Recruitment One-Stop E-Payroll E-Travel Integrated Acquisition Environment E-Records Management E-Clearance Enterprise HR Integration</p> <p style="text-align: right;"><i>OPM OPM OPM GSA GSA NARA OPM OPM</i></p>

Blue indicates current participation

The Department and USAID will expand services to U. S. citizens and businesses domestically and overseas by leveraging IT. Citizens will use interactive web sites and other online capabilities to conduct business with State regarding adoption tracking, passport issuance, and access to travel information and advice. USAID partners with businesses and Non-governmental organizations (NGOs) through the Global Development Alliance to improve economic conditions overseas. These partners will be able to conduct business with USAID electronically.

A top priority is effective exchange of information with people all over the world about US foreign policy and successes in development and disaster relief. The Department and USAID are committed to using IT as a vehicle for promoting US interests and informing people around the world about our country and our policies, through:

- *interactive web sites for working with partners, foreign ministries, the public*
- *creative use of multimedia, kiosks and other dissemination vehicles accessible by the public*
- *interactive systems that engage people in the US and overseas in the foreign policy debate*
- *IT support for exchange programs*

4.3.4 Rightsizing

An important priority for the Federal Government is rightsizing its facilities around the world to minimize unnecessary overseas presence. Rightsizing, which has been a goal for many years, will reduce security risks and costs. Business process redesign will support rightsizing by promoting standard solutions delivered centrally or regionally for virtually all business processes. The goal is to permit most administrative work, such as HR, finance, IT technical support, and procurement, to be done from regional and central locations with a critical mass of expertise supported by state-of-the-art information systems. Fewer support staff will provide higher quality support to overseas posts and missions, while working from safer regional or central locations.

Both State and USAID have been providing some services on a regionalized basis. For example, the mission in Tegucigalpa provides contract officer services to Managua. Other specialized services are provided from other locations. However, systems and networks have not been similarly reengineered to support this business model, thus requiring work-arounds and re-entry of data.

Information technology is a key enabler of rightsizing. The collaboration capabilities described in Goal 1 will enable people to work together as virtual teams, exchanging information and coordinating project activities regardless of location. Virtual teaming will allow consolidation of functions, such as procurement and human resources, at regional centers, with experts in these functions participating on the virtual teams. Rightsizing will also be supported by centralized applications and services that support global administrative functions. Industry models involving consolidated customer service centers and supporting systems will be explored for their potential applicability. Under such a model, personnel at posts would be able to place orders for services to be processed and fulfilled from these remote centers. As this concept is expanded, it may be possible to deliver virtually all administrative services with no need for administrative personnel at posts or missions.

Specific improvements to be instituted are:

- Web-enablement -- allowing full access to core IT applications of all foreign affairs agencies for end-users and technicians using a standard browser. This will enable remote access as discussed under Goal 2, as well as access via the networks of all foreign affairs agencies.
- Continuing shift to self-service -- building on successes like the Thrift Savings Plan, enable employees to perform much of their work without the assistance of intermediaries.

DRAFT Joint IT Strategic Plan

- Centralizing data and applications -- supporting rightsizing, reducing the need for maintenance of sensitive data in vulnerable overseas locations, and facilitating disaster management and continuity of operations.
- Employing e-forms and e-signatures to enable electronic exchange of data across locations, across agencies, thus eliminating the need for paper records and cumbersome processes for records disposition.
- Re-tooling application systems and databases to produce required data and eliminate today's multiple and ineffective data calls -- for example:
 - refine financial and logistics systems to institute program budgeting and tracking to allow for accurate reporting and oversight of IT expenditures;
 - strengthen USAID's Field Support System so it delivers the data needed for effective oversight of program activities; and
 - integrate systems and data to support comprehensive analysis and management reporting.

Goal 3 Strategies

Table 4-3 highlights the key strategies needed to accomplish the Goal 3 objectives.

Table 4-3: Goal 3 Strategies

Strategy	Key Components	Performance Indicators
Joint Enterprise Architecture	<ul style="list-style-type: none"> • "To be" model for common interagency platform • Information sharing model • Shared services model 	<ul style="list-style-type: none"> • Seamless communication among agencies overseas
Foreign Affairs extranet program	<ul style="list-style-type: none"> • Foreign affairs agency portals accessible via the Internet and/or USG networks • User authorization and authentication policies • Network architecture and security model 	<ul style="list-style-type: none"> • Volume of use and numbers of users of extranets

DRAFT Joint IT Strategic Plan

Strategy	Key Components	Performance Indicators
<p>Business process and application streamlining</p>	<ul style="list-style-type: none"> • Reengineer processes to support rightsizing of overseas locations and cost-efficiency of domestic operations 	<ul style="list-style-type: none"> • Specific performance targets for process efficiencies (e.g., increases in number of transactions per day, reduced lag times) • Meeting rightsizing targets -- fewer people, servers, data, and applications at posts • Meeting targets for domestic bureau streamlining -- fewer IT staff and distributed servers, applications, and data.
<p>E-Gov Solutions</p>	<ul style="list-style-type: none"> • Develop and carry out transition plans for moving to Government-wide, LoB-based solutions 	<ul style="list-style-type: none"> • Adoption of transition plan by e-Gov Program Board • Resources shifted to e-Gov solutions
<p>Government-wide overseas network</p>	<ul style="list-style-type: none"> • Work with OMB to develop a concept, network architecture, and funding approach • Assess existing initiatives (e.g., FAVE) and environments and develop and carry out transition plan 	<ul style="list-style-type: none"> • Plan and budget adopted by at least 70% of overseas agencies; plan funded • Elimination of agency networks at posts
<p>Application architecture - - web-enablement - self-service</p>	<ul style="list-style-type: none"> • Middleware (SOA, EAI) for promoting interchange of information with other agencies and partners 	<ul style="list-style-type: none"> • Measurable shift to web-based processing • Functions available for self service and extent of use • Volume of use of multiple, integrated databases

4.4 Goal 4 – Risk Management – Balancing security with business imperatives

“Ensuring the security of most agency information and systems is not the sole responsibility of the agency CIO” Also from KE: IT security is a shared responsibility and holding just one official accountable potentially weakens an agency’s ability to properly safeguard its entire collection of IT investments. [Karen Evans – placeholder]

Ronald Ross, a senior computer scientist and information security researcher at NIST, said people are spending too much time and money to protect low-risk systems and not enough on high-risk systems.

Primary Business Objectives:

Mission effectiveness through:

- (1) information access and sharing, balancing security with information needs
- (2) a comprehensive 100% reliable business continuity program
- (3) rapid introduction of new technologies that support modern diplomacy and development

IT Objectives:

4.1 **Risk management** -- disciplined management process for making risk-based decisions for business operations and information systems lifecycles rapidly and effectively

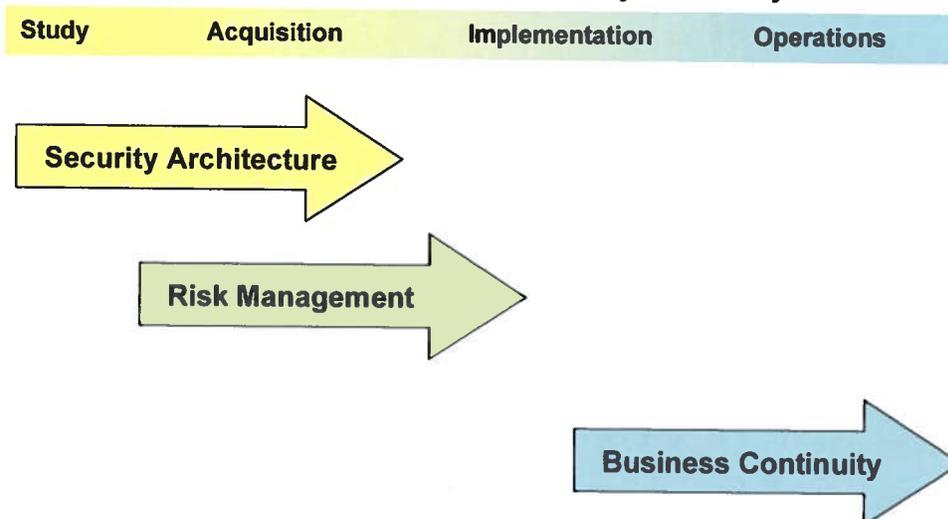
4.2 **Consistent security infrastructure**-- global approach to information security management consistent with the business and mission needs of State and USAID

4.3 **Business continuity** -- a robust and fully tested plan and facilities for contingency operations for all State and USAID locations

Goal 4 Target Environment

Under this goal, the Department and USAID will adopt a comprehensive and unified approach to all aspects of IT security. Such a joint IT security program is essential for accomplishing the other joint goals in this joint ITSP. The intent is to enable broad access to information and systems, secure internal and external collaboration, rapid and secure introduction of new technologies, and comprehensive business continuity plans.

Balancing Security Across Project Lifecycle



Through joint planning and execution, State and USAID will apply the best practices of each agency, as well as industry and government innovations in IT security. Business owners will be responsible for making risk-based decisions about deploying information systems. These decisions will be based on a security risk assessment produced through a partnership model, in which system owners, IT professionals, and security experts collaborate to make identify and quantify potential risks and probabilities. Security will be designed and built into all IT projects and programs from the earliest stages. Innovative security approaches, such as biometrics, will be in place to monitor and control user access to IT systems and information, thus enabling anytime, anywhere access, and secure extranets for internal and external collaboration. The Department and USAID will invest in the research and development of new security technologies in partnership with the private sector.

Every dollar spent on security is a dollar not spent on mission

This goal will position the Department and USAID to take advantage of the rapid advances in security technologies and best practices likely to occur over the rest of this decade. These include:

- Advanced guard technology and multi-level security solutions for linking classification layers
- Remote access to increasingly sensitive and classified data
- Business continuity planning
- Data encryption and centralization
- Thin client
- Advanced identity management

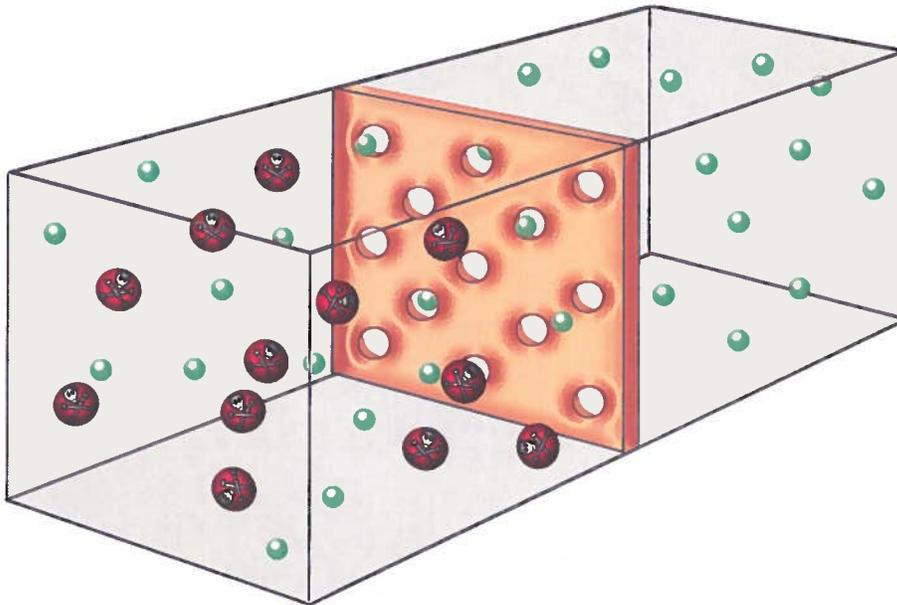
DRAFT Joint IT Strategic Plan

To accomplish the above, the Department and USAID will address the following:

- Joint IT Security Policies and Procedures
- Risk Management Program and Joint Processes
- Joint Security Management Plan

The Department and USAID take seriously the mandate from OMB to strengthen infrastructure and system security, and will use their IT Capital Planning processes to promote and finance security enhancements.

Like the semi-permeable membrane drawing shown below, information resources will be managed to prevent unauthorized flow of information, while allowing authorized users to access whatever they need to do their jobs.



4.4.1 Risk Management

"Don't be a scapegoat. The question of "How much risk?" is one that the IT department shouldn't answer. The assumption of business risk belongs to the business unit process owner." Gartner, October 2005

State and USAID have developed different approaches to security risk management. Traditionally, State has applied a posture of high security to its entire IT environment, including unclassified systems and networks. While this protects IT assets from unauthorized access and intrusions, it inhibits adoption of new technologies and hampers the ability of employees to do their jobs. While State is adopting a more balanced risk management approach, change has been difficult, and the Department is still too slow to make risk decisions.

The Honorable Karen Evans, Administrator for Electronic Government and Information Technology, OMB, noted the following to Congress: "...agency program officials must engage and be held accountable for ensuring that the systems that support their programs and operations are secure. Ensuring the security of most agency information and systems is not the sole responsibility of the agency CIO. IT security is a shared responsibility and holding just one official responsible potentially weakens an agency's to properly safeguard its entire collection of IT investments."

USAID, in contrast, has adopted a risk management approach that allows for rapid decision-making. One key to USAID's success is the establishment of a true partnership between IT and security professionals, and system owners. Under USAID's model, which has been highly praised and mirrors the practices of many other agencies, the system owner makes the final decisions regarding acceptance of risk. This aligns security and mission responsibility and increases the likelihood of balanced, effective, and rapid decisions. As a result USAID has been identified as a "center of excellence" for security [need to check this out].

Managing security risk entails assessing tradeoffs among the following security objectives, in the context of mission and business requirements:

- Availability—the IT resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses.
- Confidentiality—the information requires protection from unauthorized disclosure.
- Integrity—the information must be protected from unauthorized, unanticipated, or unintentional modification, or be modified only in approved ways by approved users or processes.

Risk management demands a level-headed payback analysis across the portfolio.

Mission is Job One!



Part of the role of the Information Systems Security Officer is to make sure that the business system owners understand all the identified risks and the resource requirements associated with implementing the planned mitigation strategies. System accreditation is the responsibility of the business system owner. Who better understands the business requirements, what risks may be acceptable, or whether it is more cost effective to mitigate a risk with a manual control than the business owner supporting the investment? In our experience, business owners, when they understand the risks, apply their resources to effectively mitigate and manage the identified risks. [Congressional Testimony of USAID's Acting CIO, John Streufert, April 7, 2005.]

The two agencies will adopt a model whereby the CIO retains responsibility for system certification, and the senior LoB manager is responsible for system accreditation. For example, the Director General will accredit human resource applications. The CIO will accredit all shared infrastructure activities and operations. As discussed under Goal 5, State will also clarify organizational responsibilities for IT security, re-aligning roles to fit this model. Currently, these responsibilities are split between IRM and The Bureau of Diplomatic Security (DS), with system owners having no decision authority.

Risk management will be applied to make decisions on:

- Wireless laptops and networks, providing full capabilities from home and on travel
- Integration of voice mail and e-mail
- Remote access to voice mail overseas
- Extranets to allow collaboration with external partners
- Cell phone access to e-mail
- Re-examination of data classification policies and practices to ensure that information is as accessible as possible
- Instant Messaging
- PDA access to unclassified networks for e-mail and document browsing
- Laptop access to classified and unclassified networks with full capabilities
- PDA access to classified networks
- Inclusion of Sensitive But Unclassified (SBU)/NOFORN on OpenNet
- Integrating Confidential into the OpenNet environment (in concert with other national security agencies), similar to the model used by the British Foreign Office

Characteristics of the risk management program to be put in place are:

- Thorough, yet rapid, exploration and analysis of the risks and costs of implementing or not implementing a given technology—one lesson of September 11, 2001, is that restricting access to information poses serious risks, often outweighing the impact of potential unauthorized disclosure.

The risk management process will be engineered to support rapid management decision-making, normally yielding a decision within 90 days.

- Risk assessment based on quantified probabilities -- management must have good information about the probability that a potential risk will cause harm. The envisioned risk management process will provide such data in a standard, non-technical format.

Good risk management practices lead to effective security controls commensurate with risks. They strengthen security by eliminating the need for vulnerable workarounds, permitting appropriate access to mission-critical data, and ensuring consistent security solutions.

- Management accountability for security decisions—whether to implement a new technology is a policy and management decision and cannot be left to technologists or security experts. System owners will have primary responsibility for making risk decisions. They will also be provided with good metrics and reports. USAID has

established a monitoring and reporting program under which system owners are given reports and grades on the security postures of their systems. This process will be extended to the joint State/USAID environment.

- Consideration of a diversity of views and opinions—security decisions must be based on rigorous debate of pros and cons by all stakeholders: end-users, security specialists and IT experts.

It took approximately one year for the Bureau of Consular Affairs (CA) to obtain approval for a web site through which US citizens can check the status of their passport applications.

4.4.2 Consistent IT Security Infrastructure

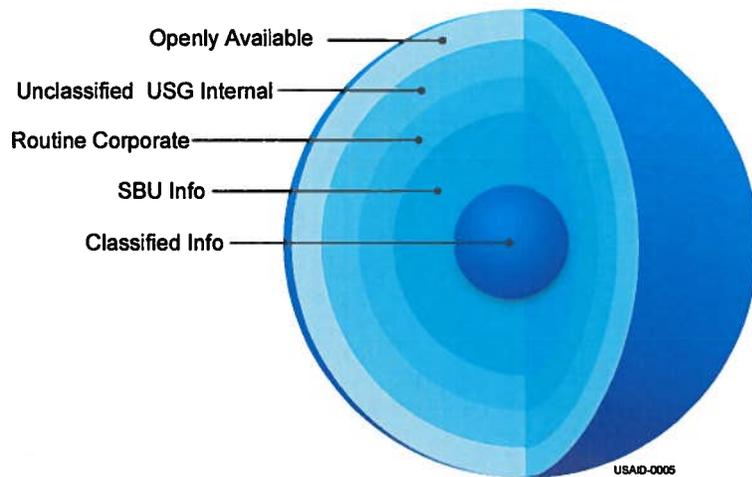
State and USAID will develop a comprehensive IT security architecture that will enable IT integration across the two agencies and will support the other goals in this plan. The architecture will be driven by the mission and business requirements of the two agencies. Currently, the two agencies operate multiple global environments or enclaves, each with its own security posture and implicit performance targets. To achieve integration, both agencies will assess these enclaves, define explicit performance goals and metrics, and design an environment that meets requirements as economically as possible.

Today, State and USAID each operates at least two unclassified global networks: State's OpenNet and PACE; USAID's AIDNet and OFDANet. Other smaller networks, e.g., Dedicated Internet Networks (DINs), are also in place to address specialized needs. These networks have been put in place to respond to different risk models (per the security objectives described in Section 4.4.1 above) and functional requirements. Moreover, there is constant pressure to create ever more networks to support emerging user demand. Unfortunately, maintaining these separate networks is expensive, inhibits broad information sharing, and may increase security risks by providing incentives for work-arounds through the various networks.

Accordingly, the two agencies will pursue a primary, global unclassified network to meet all shared needs. The consolidated infrastructure will permit secure connectivity between the unclassified and classified enclaves; and with external partners via secure extranets. The infrastructure will be designed and engineered to position use of multi-level security (MLS) should it become practical during the planning horizon. As the figure below indicates, State and USAID handle information that ranges in sensitivity, with the bulk of the information minimally sensitive or broadly accessible. Only a small percentage is classified or SBU.

Comment [P1]: Is guard technology the only potential solution?

DRAFT Joint IT Strategic Plan



Policy and culture changes will also be pursued to promote use of the correct network for each function and activity. Currently, because it is convenient, many political officers overseas use the classified network exclusively, whether the work they are doing is classified or not. This inhibits collaboration opportunities and artificially enlarges the expensive classified infrastructure. The future environment will be engineered so it is easy, perhaps automatic, for users to switch between environments and thus be able to use the correct infrastructure for each task.

The accomplishment of this objective will require the following:

- An **effective management process** for rapidly assessing proposed new requirements and determining how to address them within the context of the single network
- Clear business-driven security requirements and **performance metrics** for all general support systems and major applications.
- A process for **segregating sensitive data** and applications within the network, thus ensuring:
 - Proper protection of highly sensitive but unclassified information
 - Elimination of the need for multiple unclassified networks
 - Elimination of the unnecessary burden of protecting all information on the network at the highest level
- An architectural, enterprise-wide approach to **managing the boundaries** between networks, components, enclaves, and internal and external environments -- focusing on defined trust levels and patterns of connectivity that incorporate adequate security relative to the risk profile of each trust level.

- Assessing the shared *business needs and security models* of State and USAID to ensure that all requirements can be addressed in a single environment, promoting cost-effectiveness and broad information sharing. It will also identify any rare situations where a separate network might be required for special needs, for example OFDANet.
- Engineering the infrastructure to *minimize the need for expensive classified environments*, especially overseas -- pursue regionalization and centralization of classified data, use of thin clients, and other approaches to reduce the need for classified operations and data storage overseas. This is critical as decentralized classified environments are costly and pose security risks.

This architectural approach and joint Certification and Accreditation process will provide pre-approved security solutions that can be re-used with expedited review and approval.

Examples of security solutions to be deployed are:

- *Digital signature*
- *Smart IDs and biometrics for authorization and authentication to enable single sign-on*
- *Guard technology for transferring data across security levels*
- *Firewalls, intrusion detection, encryption, Secure Socket Layer (SSL), and other technologies to provide extranet access to internal systems*
- *Configuration of back-end servers to allow out-of-the-box use of PDAs and laptops for remote and wireless connectivity*
- *Identity management, based on HSPD 12 for e-Authentication, in conjunction with FIPS 201 and the government-wide Public Key Infrastructure (PKI) badge to govern access to all information systems.*

Comment [P2]: There will still be a requirement to validate the solution was actually applied correctly. These would be implemented very similar to a type accreditation. The test and evaluation would be simple, uniform and easy to quickly perform – accreditation packages and approval letters would be templates designed for quick processing.

4.4.3 Business Continuity

The focus of this objective is ensuring effective IT support for a comprehensive business continuity plan for State and USAID. This is a key element of risk management, which enables State and USAID to define the critical infrastructure needed for priority mission objectives and operations. The business continuity plan will in turn drive the creation of enterprise-wide Continuity of Operations (COOP) and IT contingency plans, supported by consolidated services and facilities.

This objective will enable operations to continue in the event of a localized or regional disaster which renders it impossible for staff to access State or USAID facilities. It will be comprehensive, addressing facilities, business processes, IT, personnel training, and testing.

DRAFT Joint IT Strategic Plan

Individual bureaus, offices, and posts/missions have begun disaster and business continuity planning, and this objective will bring these efforts together in a consolidated, consistent initiative under a single entity. While State and USAID provide guidance to posts and bureaus regarding business continuity, an enterprise-wide solution is lacking and will be put in place under this Plan. This action will ensure that all bureaus and posts have sufficient coverage and that business continuity resources are applied cost-effectively.

The business continuity plan will be driven by management priorities using a risk-based analysis, to specify the level of service that must be in place on a contingency basis. These priorities will be translated into clear goals and performance targets, specifying:

- Assumptions about the nature and scope of the disasters to be planned for
- The mission critical functions that must be operational at all times
- A ranking of all other functions, along with performance goals and measures for their acceptable level of operability during a disaster
- The personnel who require access during various disaster scenarios
- How rapidly alternative facilities and operations must be on-line following a disaster

Once senior management has addressed the broad outlines of a strategy, a comprehensive and detailed plan will be developed to conform to the strategic decisions made. The plan will identify resources needed to be invested in advance and in the event of a disaster. It will provide for alternative facilities to be in place in advance and will detail the activities needed to make the alternative facilities operational. It will also address the other elements noted above - such as initial and ongoing employee training and testing. Finally, the plan will address what must be done each year to ensure complete readiness at all State and USAID locations.

Bureaus will adhere to standards for IT applications and databases to ensure built-in redundancy and use of central facilities for business continuity. Standards will promote web-based design and central servers and data repositories.

In parallel with setting the policy and performance objectives, State and USAID will consolidate existing facilities to create a joint, enterprise-wide COOP program. This program will leverage existing State and USAID facilities around the country, e.g., Charleston, Portsmouth, Miami, and Kentucky, in an integrated network environment that ensures availability during regional disasters.

Goal 4 Strategies

Table 4-4: Goal 4 Strategies

Strategy	Key Components	Performance Indicators
Consolidated security architectures of State and USAID	<ul style="list-style-type: none"> • Establish security standards, metrics, and monitoring • Consolidate infrastructure security models 	<ul style="list-style-type: none"> • Single network for each security enclave • Demonstrated ability to meet requirements of both agencies
New technology assessment	<ul style="list-style-type: none"> • Joint process for assessing and approving new technologies • Clarify organizational roles and responsibilities • Establish system owner as accrediting official 	<ul style="list-style-type: none"> • 90-day decisions
Identity management	<ul style="list-style-type: none"> • Government standards -- HSPD 12, PKI, e-Authentication, FIPS 201 	<ul style="list-style-type: none"> • Common access controls for other agencies and external partners
Business continuity	<ul style="list-style-type: none"> • Oversight by a single entity • Objectives and metrics • Comprehensive plan, schedule, and resource needs • Enterprise business continuity services, e.g., shared COOP facilities, backup and recovery • Execution of advance activities • Comprehensive training • Comprehensive annual testing 	<ul style="list-style-type: none"> • Test results indicate full readiness, approved by executive management in both agencies

4.5 Goal 5: Work Practices and Workforce

Primary Business Objectives:

- Mission effectiveness through better use and adoption of technology and change management
- Efficiency gains through rightsizing and performance management resulting in excellent service to end-users, especially front-line, substantive personnel overseas

IT Objectives:

- 5.1 *Organizational Excellence and Accountability* -- achieve established service levels and innovate
- 5.2 *Strengthened IT Skills* -- ensure that end-users and IT specialists are properly trained
- 5.3 *Consistent IT Governance* -- establish best practices across both agencies

Target for Goal 5

The Department and USAID will organize their combined workforces and IT organizations to support the achievement of the other four goals in this Plan, and to enable continuous adaptation to the increasingly rapid changes likely to occur, both in requirements and technology. Technical support operations will be regionalized or centralized, whichever is most cost-effective, to promote rightsizing at posts and missions, and to create centers of excellence at consolidated locations. Such consolidation will ensure that IT staff are positioned to deliver exceptional customer service to end-users to help them maximize the value of information and systems.

The focus of Washington-based and regional organizations will be to support the direct diplomatic and development work carried out in the field. The central IRM organization will focus on delivering solutions to the embassies and USAID missions. Innovations in technology will be configured, pilot-tested, and deployed first to field locations.

The Department must embrace the value of information and create a knowledge sharing culture. People use only a small fraction of the capabilities available to them through modern IT. To expand the value of technology, this JITSP takes a holistic approach focusing on process reengineering, training, change management, as well as technology innovation.

This Goal will focus first on the work practices and personnel engaged in diplomacy and development, and then on aligning IT processes and staff to support the mission

related work and personnel. The Under Secretary for Political Affairs and the Deputy Director of USAID will take the lead on the substantive processes of diplomacy and development. The two CIOs will lead the effort to revamp the IT processes and workforce—all of this focused not just on information technology but on the ways that technology can be used to further US foreign policy goals. The intent is an integrated IT organization supporting both agencies and the entire foreign affairs community. This new organization will be customer-oriented and driven by service standards and performance metrics.

The IT governance processes of State and USAID will be consolidated to ensure that IT resources are allocated in accordance with the joint strategic plan and evolving priorities.

Goal 5 Objectives

4.5.1 Organizational Excellence and Accountability

The IT organization and workforce will be transformed to mirror the new, broader focus on information resources to help personnel do their work, which itself is changing. IT staff, especially those overseas, will spend more time helping end-users get the most value from IT systems and knowledge resources, and less time maintaining hardware and networks. IT professionals will assist officers in identifying IT tools that meet their needs, helping them overcome the technical hurdles so they are able to embrace change and exploit the technology effectively. The IT organization will focus on core information and user support activities, and will outsource non-core operations to the private sector or government-wide service providers. The end result will be an IT organization that provides knowledge leadership services, high-end consultative support to end-users, and technical support for the few unique applications.

Organizational planning will distinguish between two categories of IT professionals: those with in-depth technical and IT management skills, and those whose focus is on working with end-users to exploit technology for diplomacy and development. Positions requiring expertise will be staffed by civil service employees and contractors to ensure continuity and expertise.

Service level management will be a key ingredient of the re-tooled IT support environment. Service levels will be established for all key services, and service metrics will be collected and published on a monthly basis. Examples include:

- Network availability and performance for each location
- Help desk responsiveness -- problem resolution within parameters
- Process execution -- e.g., ITCCB and Risk Management decisions within established performance parameters (e.g., time), Federal Reporting Requirements accomplished effectively -- e.g., CPIC, EVMS.
- IT Infrastructure refresh performance
- Effective program management -- meeting milestones, quality standards, and budgets

Both State and USAID will revamp their joint IT workforce, building on recent successes such as skills incentive pay. The new IT worker will be trained as an information consultant, able to help people make the most of the available knowledge bases and analytical tools and suggesting new technology solutions to meet business needs. IT staff at overseas posts and missions will no longer worry about technical support for cranky hardware and application of software patches, tasks which consume far too much of their time today. Instead, they will become a valuable part of the Country Team, providing information consulting and direct end user for the post's strategic priorities.

A new professional discipline will be identified: The "knowledge worker" will understand both mission imperatives and the intricacies of IT. Some technical staff will continue to support the IT infrastructure and technology, but there will be a shift in emphasis toward information consulting and end-user support.

Achievement of this goal and the success of the joint IT Strategic Plan depend heavily on State and USAID's ability to promote innovation, adopt new technology, and make changes far more rapidly than has been the case in the past. Realization of this goal will require effective change management and commitment at the highest levels of both organizations. It will also require a systematic examination and clarification of work processes for mission and management related activities. These changes will enable a more effective IT program focused on 21st century diplomacy and development. They will allow officers to make better use of the collaborative decision support and information sharing tools, transfer their expertise from post to post, and share it with IT specialists, general Foreign Service Officers, and USAID professionals.

The IT organizations of State and USAID will establish a joint technology innovation laboratory to explore new technologies and generate new ideas and solutions. Non-IT personnel will be strongly encouraged to offer suggestions and to work with the lab to identify and prototype solutions. The laboratory will maintain a clearinghouse of ideas, requirements, and potential solutions. Both agencies will also continue working with other government and private incubators of new technologies, such as In-Q-Tel. Change management processes will ensure that technologies and systems are implemented out of the box, adapting business processes to the solutions, not re-paving the cow-path.

IT support operations will be more competitive and performance-driven, applying the following mechanisms:

- Fee-for-service for new technologies and add-ons, ensuring that IT products are responsive to customer demand.
- Use of alternative sourcing options to promote a competitive and cost-sensitive environment, exploring competitive sourcing, out-sourcing, and multiple-award contracts.

4.5.2 Strengthened IT Skills

As technology becomes more pervasive, personnel will become increasingly reliant on the use of sophisticated systems and data sources in their daily activities. The Department and USAID will ensure that their personnel have the necessary skills to exploit new and evolving IT solutions. Building on the success of programs such as the Foreign Service Institute's "Training Continuum," innovative training programs and technologies will be provided to both State and USAID employees, much as was done for State personnel under the *FY 2001–2005 IT Strategic Plan*.

Beyond the \$1,500 Typewriter

People use only a small fraction of the capabilities available to them through modern IT. To expand the value of technology, this Plan takes a holistic approach focusing on process reengineering, training, change management, as well as technology innovation. The Department must embrace the value of information and create a knowledge sharing culture.

FSI will expand the technology component of all courses, including those in substantive areas such as political and economic tradecraft. These courses will cover the information repositories and specialized tools applicable to the subject matter under study. Students will be given an opportunity to use these tools as part of their training in research, analysis, reporting, and other areas pertinent to development and diplomacy.

Students learning about political reporting and analysis will use the Department's advanced portal and search capabilities, language translation software, and visualization programs to create innovative multi-media reports. Personnel studying disaster response will learn how to set up their mobile IT kits and set up multiple levels of system and data access for all team members. Training in transformational diplomacy will cover use of mobile computing to help monitor elections and web casting of election events and speeches in remote locations.

The following additional training initiatives will be pursued:

- Apply multiple training vehicles to reinforce material -- formal classroom training, computer-based training, one-on-one at the desktop, distance learning, videoconferencing seminars, and informal brown bag lunch sessions
- Incorporate change management into tradecraft and technology training — use illustrations and focus training to inspire people to adopt new technologies and use them effectively

- Train Office Management Specialists (OMS) to serve as key information support resources for embassies and USAID missions, to build skills such as web and document publishing, desktop applications, conducting effective Internet and database searches, mapping and visualization tools.
- Expand use of regional training to increase numbers trained, decrease time away from posts, and reduce costs of training.

4.5.3 Consistent IT Governance

State and USAID will consolidate the e-Governance processes of the two agencies, and establish a standard set of processes for life cycle project management. Both agencies will provide comprehensive financial and management oversight of all IT investments, enabling management to ensure that IT investments and projects are aligned with mission and business priorities, while effectively meeting statutory requirements. Effective project oversight and control will ensure that IT systems satisfy business and user requirements and are delivered on time and within budget.

In consolidating the e-Governance process, the two agencies will revise their respective governance boards and committees and clarify roles and decision points. State's Under Secretary for Management, who oversees the Department's e-Gov process, has directed the CIO to refine, streamline, and clarify the process, strengthening oversight of the IT portfolio and ensuring that projects stay on track and produce expected business results. The enhanced process will serve as a starting point for consolidating the e-Gov processes of the two agencies.

The consolidated e-Gov process will oversee all IT spending for both agencies. Program budgeting and execution will be instituted to enable accurate budgeting and monitoring of all IT spending. Procurement processes will be modified as needed to ensure that IT purchases are tracked against IT budgets. The IT organization will be accountable for managing all IT funding, providing oversight to all projects, and achieving service and performance standards.

State and USAID will agree on a common life cycle process for IT project management, which will identify the stages of a project along with key control gates and decision points. This process will produce reports on project performance at key decision points and will enable management to take appropriate corrective action as necessary. Both agencies will benefit from more aggressive project oversight, focused on ensuring that projects are performing as planned and delivering excellent products and services.

Goal 5 Strategies

Table 4-5 highlights the key strategies needed to accomplish the Goal 1 objectives.

Table 4-5: Goal 5 Strategies

Strategy	Key Components	Performance Indicators
Innovative end-user training	<ul style="list-style-type: none"> • Expand IT component of substantive training • Explore ways to make courses more accessible to USAID personnel • Offer multiple training delivery mechanisms • Require IT training for all personnel • Change management 	<ul style="list-style-type: none"> • Greater volume of IT-enhanced work products (e.g., multi-media, visualization tools) • Measured skill levels of end-users and IT staff • Attendance of end-users, include USAID personnel • Greater use of IT tools in substantive business activities
Performance management for IT service delivery	<ul style="list-style-type: none"> • Reorganize both IT support organizations for service delivery and customer orientation • Establish steering committee of customers, including field/overseas users, and IT • Develop service level standards and performance metrics • Institute measurement and reporting 	<ul style="list-style-type: none"> • Achievement of service metrics • Corrective actions taken
Revamp IT Organization	<ul style="list-style-type: none"> • Assess needs for consolidated IT support for both agencies, domestic and overseas • Develop concept and structure for revamped IT organization 	<ul style="list-style-type: none"> • Elimination of duplications • Efficiencies due to economies of scale • Adoption of new organization

DRAFT Joint IT Strategic Plan

Strategy	Key Components	Performance Indicators
Technology innovation	<ul style="list-style-type: none"> • Establish joint IT laboratory for innovation • Promote idea generation from multiple sources • Open Standards • Open Source 	<ul style="list-style-type: none"> • User satisfaction with introduction of new technologies to meet business needs • Elapsed time between identified requirement and adoption • Reduced dependence on single vendors for critical technology such as operating system software
Centralization/Regionalization	<ul style="list-style-type: none"> • Assess IT needs at posts, regions, and HQ • Develop rightsizing plan for regionalizing and centralizing • Adopt and manage service levels for centrally delivered service • Explore alternative sourcing and pricing options • Expand regional training and use local external training suppliers 	<ul style="list-style-type: none"> • Achievement of rightsizing targets for IT and other personnel • Customer satisfaction • Availability of alternative sources and prices
Consolidate governance	<ul style="list-style-type: none"> • Joint e-Gov process • Clarify decision-making authority of various groups • Central management of all IT funds • Adopt common life cycle management process for both agencies 	<ul style="list-style-type: none"> • Effective oversight as indicated by rapid decisions and corrective action • Priority projects completed on time and within budget

5 Management Strategies & Critical Success Factors

5.1 IT Integration Strategy

As discussed above, by 2010 State and USAID IT operations and administration will be largely integrated. Commonalities across agencies will have been exploited through shared organizations and systems; those operations not inherent to either agency will have been outsourced to e-Gov service providers; and each agency will have shifted its primary IT focus to mission specific applications. State/USAID integration will provide a foundation for broader development of a unified IT infrastructure for all agencies operating overseas.

During FY2006, State and USAID will develop a tactical plan for full integration of their IT operations. The execution of the plan will be coordinated by the JMC. The plan will expand on the ideas presented in this joint ITSP and identify the specific levels of IT integration to be accomplished over the next five years. The tactical plan will identify cost reductions and cost avoidance resulting from IT integration, and will indicate how any savings should be reprioritized to support the goals of this Joint IT Strategic Plan. The following outlines guiding principles to be reflected in the tactical plan:

- **Consolidate IT activities within each agency** – Centralization and regionalization of each agency's IT activities will be invaluable in the interagency integration process. For example, it probably will be easier to integrate State and USAID firewall management processes if these processes are first centralized within each agency. However, in some cases, it will be advantageous to centralize or regionalize as part of the interagency consolidation effort. The key point is to determine the most expeditious approach for consolidating and centralizing/regionalizing.
- **Develop models for consolidating functions and locations** -- The Department and USAID will develop models for performing and staffing selected core and administrative functions, indicating where functions will be performed and by what types of staff. The agencies will then create organizational models for overseas locations based on such characteristics as size and threat level. These models will be the basis of planning and designing comprehensive IT support that can be applied globally.
- **Fully exploit common IT functions while accommodating unique requirements** – State and USAID will consolidate all common IT functions between the two agencies. Common functions include not only the IT infrastructure and administrative systems, but also mission-oriented activities such as knowledge management. Also included will be consolidation of the IT organizations that operate the integrated systems. As similar activities across

both agencies are analyzed, business processes in each agency may need to be adjusted to allow full integration. In addition, organizational elements across agencies will be restructured to eliminate redundancy. However, unique requirements will not be abandoned in order to “force” a common solution.

- **Leverage best practices** – IT integration of the two agencies must be a full partnership focused on achieving the IT strategic goals presented in this Joint ITSP – jointness cannot be viewed as the “assimilation” of USAID into State. Each partner’s strengths will be leveraged to the benefit of both agencies. Each common area will be analyzed to determine which agency is best suited to serve as lead. Recognizing that “matrix management” structures will likely be dysfunctional, activities will primarily be modularized and assigned to a specific agency.
- **Establish trust model** – In the target IT environment, State and USAID will share a common infrastructure and administrative systems. Each agency will assume responsibility for different activities based on best practices. Each agency will also be responsible for its own unique mission specific applications and systems that share the common infrastructure. Establishing the joint IT environment will require that both agencies adopt a comprehensive trust model – a security posture, architecture, and processes – to enable rapid technology decisions that support both agencies fully.

The tactical plan will detail the specific levels of integration to be achieved. The following will serve as a starting point for considering integration plans:

- **IT Infrastructure integration** – State and USAID will share a common IT infrastructure which encompasses the desktop processing environment (Common Operating Environment or COE), enterprise network, processing facilities, extranets, help desks, messaging, and enterprise software licenses. OpenNet and ClassNet will be extended to all USAID missions as required. The existing State networks – OpenNet and ClassNet – will be adopted as the worldwide foreign affairs network and will support all US Government agencies overseas. This will require that these networks adjust their services and risk management posture to accommodate all requirements. The level and quality of centrally provided services will be established and monitored via Service Level Agreements (SLAs). Each agency will provide specific infrastructure services to the other agency based on its experience, criticality of the function, and best practices. For example, USAID will manage extranets given its strong dependence on external partnerships and need for external collaboration. State will manage desktop/infrastructure modernization, building on the successful GITM program.
- **Administrative operations and software** – By 2010 most administrative operations will be supported by government-wide solutions. All funding associated with these activities will have been captured and redirected towards

the goals outlined in this plan. Any remaining administrative systems and activities will be shared to the maximum extent possible, building on current JMC efforts to develop common applications for financial management and logistics. For these shared applications, the goal is to develop fully common systems that use the identical software, common database platforms, and uniform data coding and integration.

- **IT governance and support** – the target is for the two agencies to adopt a common e-governance and project management processes as outlined under Goal 5.
- **Knowledge management** -- State and USAID will proceed jointly to apply best practices in knowledge and information management. They will work together to implement Goal 1, focusing on value-added knowledge bases, data warehouse technology, innovative tools for information analysis and presentation, web publishing and content management.

5.2 Critical Success Factors (CSFs)

Critical success factors are the underlying activities and processes that are essential to achieve large scale change. To make this plan work, both agencies will have to adopt the leadership, management, and technical practices and principles outlined below:

5.2.1 Leadership CSFs

- **Leadership Commitment** -- Senior executives, up to and including the Under Secretaries and Secretary, must embrace this Plan and actively promote its adoption and use. The Plan will guide IT investments and govern how information is applied to promote mission and business goals and priorities.
- **Focused Resources** – The joint E-gov Program Board and the JMC must ensure that resources and management attention are primarily focused on existing and new activities needed to achieve the goals of this plan.
- **Identification of Enterprise IT Funds** – In order for both agencies to decide what is cost effective in analyzing possible areas of jointness, it is essential to share complete and accurate funding data on all IT activities. Furthermore, each agency's IT capital planning process must be able to identify and control all of its IT dollars.
- **Information Sharing** – Management at all levels of both agencies must regard information as a corporate asset which is owned and shared throughout the enterprise. In addition, both agencies must achieve greater two-way information sharing and communication with partner agencies, the public, business and other governments.

- **Information stewardship** -- Managers must be given explicit responsibility and held accountable for ensuring the accuracy, reliability, and availability of information. There are several components to this CSF -- (1) there must be a single authoritative source for each element of information to avoid duplications and inconsistencies; (2) personnel evaluations and ratings will reflect management of data and information.
- **Change Management** – Effective change management will be required by both agencies to achieve this plan. Change management will focus on identifying the obstacles to change and techniques for overcoming those obstacles. It will include defining new roles and responsibilities and providing the necessary training and assistance for employees involved. In some instances, it will require realigning, centralizing, and combining various organizations.
- **Best Practices** – Each agency’s expertise and best practices will be retained and leveraged. Either agency may be designated the lead for any area where they have demonstrated highest levels of success.
- **Service Provider Selection** – Outside service providers will be selected for those functions where they provide the most economical and effective solution.

5.2.2 Management CSFs

- **Gap Analysis** – State and USAID must immediately undertake an analysis of existing IT programs, projects and activities to identify voids, duplications and inconsistencies between what is being done now and what needs to be accomplished to achieve this plan. Financial and personnel resources must be acquired and/or redirected accordingly.
- **Delivery of Service** - In order to obtain the trust and support of users for more centralized IT solutions, both agencies must deliver rapid and reliable service. Levels of service and measures of performance must be agreed upon by all parties and they must be carefully monitored so that those responsible are held accountable for the effective delivery.
- **Human Resource Plan** – To transition smoothly to the IT workforce that both agencies will require in the future, a five year IT human resource plan will be created. With all of the activity that will be required to achieve this plan, both agencies’ current IT workforces will be needed, but will have to be trained and reorganized extensively.

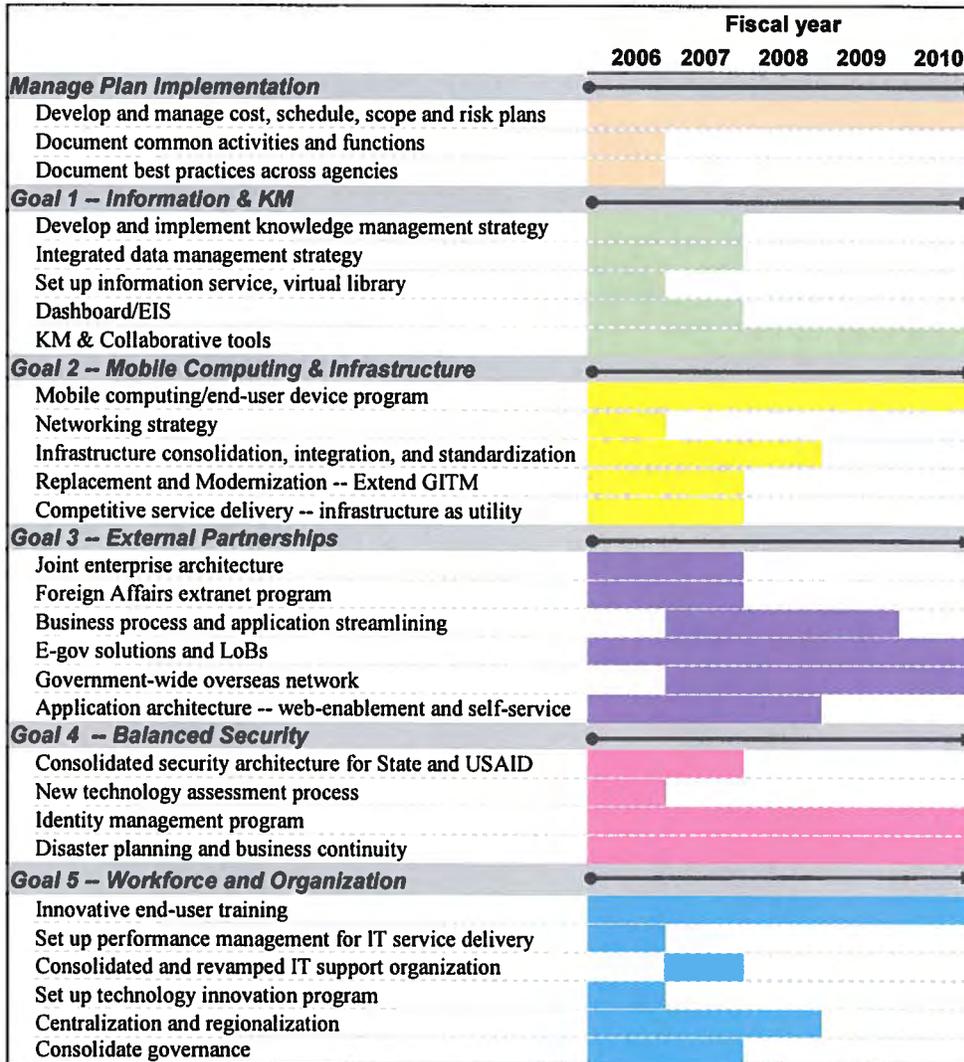
- **Performance Management** – Both agencies will need to refine, and then monitor with appropriate metrics (at the E-gov Board/JMC level), the completion of the strategies, key components and performance indicators listed for each objective in this plan. In addition, a standard performance management process and system will be put in place to support broad and effective performance management.
- **Project Management** – Both agencies must adopt a single standard project management discipline and provide the necessary training and certification programs to enable managers to carry it out.

5.2.3 Technology CSFs

- **Adoption of New Technology** – Both agencies must improve the rate at which they adopt new technology if they are to remain as competitive and relevant as possible. The keys will be to: (a) establish an office/laboratory to explore new technology solutions and; (b) accelerate the rate at which security approvals are obtained for new solutions by using the strategies set forth in Goal 4.
- **Development of New Solutions** – New solutions must be developed with the active participation of both domestic and overseas users. Where applicable, these solutions must reflect local, regional and central views of data as well as geographic, project, functional and temporal views.
- **Standards Based Environment** – A preeminent goal for both agencies is information sharing and collaboration. Both agencies must employ service-oriented architecture (SOA) and enterprise application integration (EAI) approaches to achieve interoperability and facilitate communication among multiple organizations, contractors and partners.
- **Quality Management** – Quality management is an important ingredient in delivering consistent, customer-driven IT services. State and USAID must adopt a quality management program such as ISO 9000 or the Capability Maturity Model.

6 Implementation Strategy

Figure 6-1 shows a high level schedule for carrying out this JITSP over the next five years. The figure shows the major activities needed to pursue each goal, mapped against fiscal years.



DRAFT Joint IT Strategic Plan

Implementation of this JITSP will require investments focused on the five goals and supporting strategies. To some degree investment funds will be obtained by shifting resources to new programs, and some resources will be freed up by efficiencies gained through rightsizing, competitive sourcing, and similar initiatives. But clearly, additional resources will be needed in the first two years of the plan to create momentum for such critical efforts as knowledge management, reengineering the global network, and enterprise-wide business continuity.

Table 6-1 provides a high level view of the resources required for each goal.

Goal	Implementation Considerations and Resource Needs
1. The Right Information	Investments will be required to establish central services and tools for knowledge management and performance management. Initial investments will focus on pilots to demonstrate success and build momentum.
2. Anytime/Anywhere Access	This goal will yield cost savings through centralization and consolidation. These savings will be reinvested to provide end-user devices and support for mobile access.
3. External Partnership	Savings resulting from rightsizing will be invested in secure external collaboration capabilities. Cost-sharing strategies will be established for interagency infrastructure. Additional savings may result from use of government-wide solutions.
4. Risk Management	Business continuity will require substantial investments. Once the processes are re-engineered properly, risk management will be accomplished within existing resource levels.
5. Work Practices and Workforce	The focus of this goal is to improve service without increasing costs. Consolidation of the State and USAID IT organizations may result in savings that can be reinvested in training and organizational development.

Table 6-1: Resource Requirements

Over the next six months, a tactical plan will be produced identifying the specific projects needed to carry out this Plan. The tactical planning process will provide additional detail about schedule, funding requirements, and timing of investments.

APPENDIX A

The Business Capability Map

USAID Enterprise Architecture, Agency Conceptual Level Overview, Volumes 1 and 2, March 4, 2005, USAID – More detail

The Business Capability Map (BCM) is a tool for developing USAID’s Enterprise Architecture. The objective of the BCM is to depict USAID’s business model in a one-page snapshot to facilitate examination of different elements of USAID’s “business” from a common perspective.

The map is the key framework used to identify areas of potential improvement/opportunity for short, medium, and long-term investment. It is divided into three sections: Value Added Services, Management Levels, and Business Capabilities:

- Value Added Service (across the top of the map). These are the services that must be provided and executed well to successfully fulfill USAID’s mission of development and humanitarian assistance. Each one of the Value Added Services is aligned to one of the 8 Agency business requirements.
- Management Levels (the left axis of the map). The phase of the business cycle in which capabilities are most appropriately utilized and placed. There are three management levels – Plan, Control, and Execute. There must be at least one capability in each management level to deliver the value-added service.
- Business Capabilities (the internal boxes in the map). A measurable business function that enables USAID to provide one or more of its value added services (e.g., Contextual Analysis, or Knowledge Lifecycle Management). Each capability is comprised of definable processes, technologies, skills, and information required to successfully enable that capability.

