

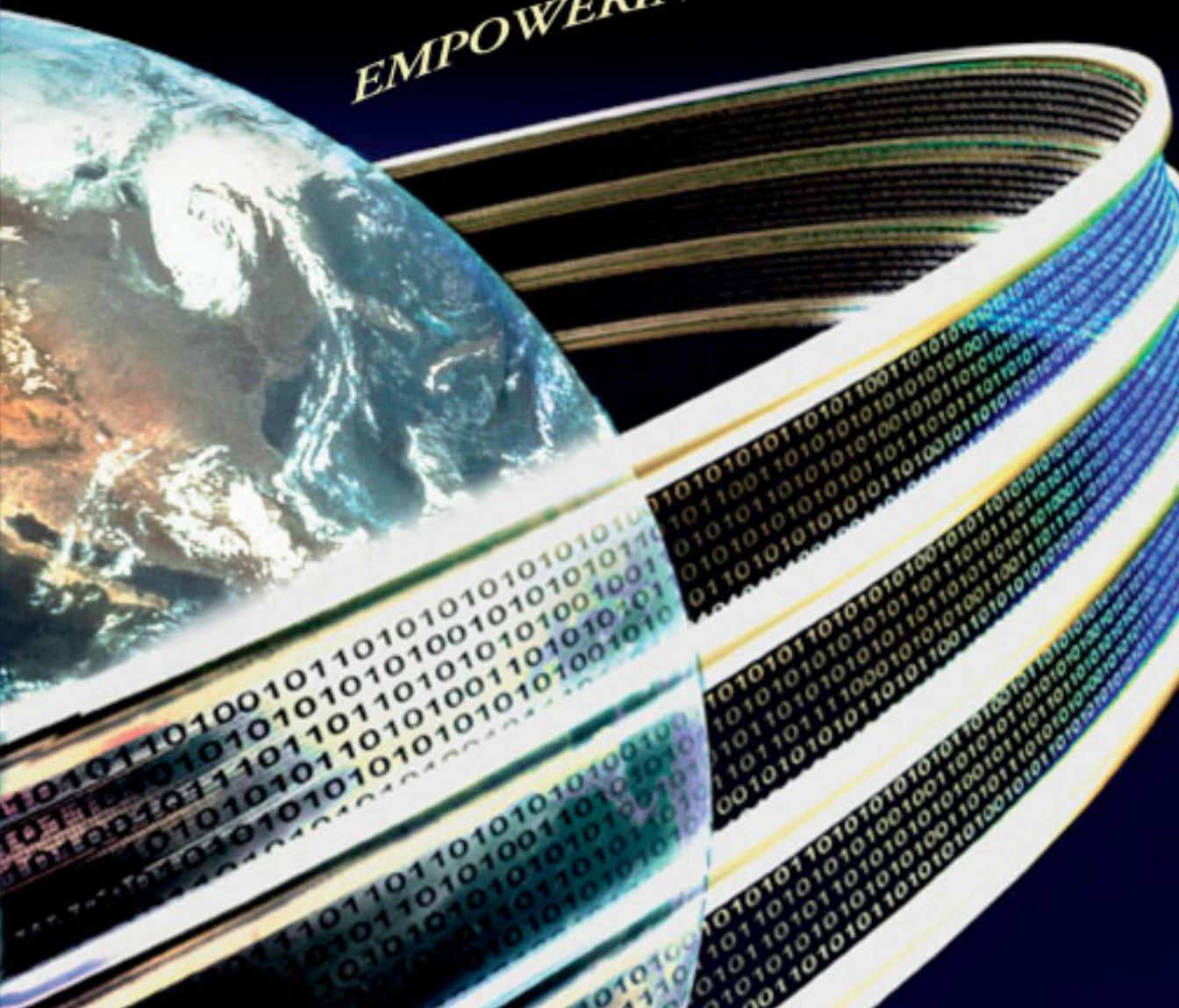
United States Department of State

IT STRATEGIC PLAN

Fiscal Years 2006–2010

Goals Paper

EMPOWERING DIPLOMACY



“The success of U.S. diplomacy in this new century depends in no small measure on whether we exploit the promise of the technology revolution.”

Secretary of State Colin L. Powell

This Goals Paper provides a high-level blueprint for using the Department’s modern information technology (IT) infrastructure to deliver knowledge resources and IT services to State’s diplomatic practitioners overseas and in the United States.

Strategic Theme:

From Infrastructure to Empowerment

The purpose of this Goals Paper is to stimulate broad-based discussion throughout the Department and with its external partners and customers to forge a consensus on the IT goals to be pursued between FY 2006 and 2010.

Table of Contents

Introduction	2
IT Vision	6
IT Goals	6
1. The Right Information: Knowledge Leadership for Diplomacy	7
2. Anytime/Anywhere Computing: Diplomats on the Move	10
3. External Partnership: Diplomacy Through Collaboration	13
4. Risk Management: Mission Effectiveness and Security	16
5. Work Practices and Workforce: Leading Change	19
Next Steps	21

Introduction

This *Information Technology (IT) Goals Paper* outlines a future-oriented technology program for the Department that directly supports U.S. foreign policy and diplomacy as articulated in the *FY 2004–2009 Department of State and USAID Strategic Plan*. The paper sets five key IT goals for FY 2006–2010. Several of these goals represent significant departures from the Department’s current ways of doing business and allocating IT resources. Accordingly, the Department will promote wide discussion of this paper among end users, management, and IT professionals to ensure that the goals are well understood, modified as appropriate, and embraced broadly before developing a new IT Strategic Plan. The new Plan will set the IT direction for the balance of this decade and form the basis for major decisions on IT investments and projects.

Current Status of IT in the Department

This paper builds on 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, through the period covered by this new plan, it will take the next step: putting in place tools and information resources that will aid the employees who carry out the Department’s international affairs mission.

The Department has made extraordinary progress under the current *IT Strategic Plan*. Much demonstrable success has been achieved in all five goal areas, and the results have changed the way the Department does its business. The enthusiastic support of the Secretary of State and senior management for rapid, continuous IT modernization in support of diplomacy has been, and will remain, critical to success. This support has led to improvements in IT governance processes, including broad representation in decision-making. It has also led to substantial increases in investment, enabling the Department to catch up rapidly in terms of basic infrastructure technology. Table 1 highlights the major accomplishments under the Plan.



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

ITSP Goal	Major Accomplishments
1. A Secure Global Network and Infrastructure	<ul style="list-style-type: none"> • Highly standardized, available, and reliable global IT infrastructure • Fully implemented defense-in-depth security – e.g., server, e-mail, and workstation anti-virus, network intrusion detection, and operational CERT and CIRT processes • Institutionalized Certification and Accreditation program • Modern, reliable classified and unclassified networks • Internet access and Virtual Private Network (VPN) capabilities • Centralized IT modernization and refresh worldwide through Global IT Modernization (GITM) program • Enterprise network management
2. Ready Access to International Affairs Applications and Information	<ul style="list-style-type: none"> • Continued improvement in 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
3. Integrated Messaging—A Modern Worldwide Approach	<ul style="list-style-type: none"> • Single, worldwide e-mail system 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 • Server consolidation through Enterprise Server Operations Center (ESOC) • Financial systems 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 current *IT Strategic Plan* has changed the way the Department does diplomacy:

- Remote posts are less isolated as a result of the global networks;
- Flexible e-mail has replaced rigidly formatted cables for much of the Department’s work;
- Department management and oversight agencies have confidence in the Department’s ability to deliver large-scale IT projects;
- The Web has become an important information resource and a vehicle for outreach; and
- Electronic commerce has become well established for on-line acquisition.

Strategic Mission and Business Goals

This paper is driven primarily by the *FY 2004–2009 Department of State and USAID Strategic Plan*, which describes the Department’s mission and strategic objectives and goals. As the lead U.S. foreign affairs agency, the Department’s mission is to:

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

The *Strategic Plan* identifies principal aims of the Department and USAID in support of this mission. These aims link diplomacy, development assistance, and defense. The Plan goes on to identify specific initiatives to be pursued in support of this 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 its mission, the Department consults and works 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.

This *IT Goals Paper* is also driven by input from end users, bureaus, and posts as documented in the Department’s recently published joint *State/USAID Enterprise Architecture*, interviews and overseas visits conducted by the IRM Bureau Planning Office, and a survey conducted by the Office of e-Diplomacy of more than 3,000 policy and management officers worldwide.

A third driver of this *IT Goals Paper* is the President’s Management Agenda (PMA) and related government-wide IT initiatives, especially e-Government (e-Gov). Through these initiatives, the State Department seeks to promote efficiency in the delivery of administrative services as well as increased coordination among agencies operating overseas.

The Strategic Plan, Enterprise Architecture, and e-Government initiatives all emphasize the value of information and information technology as key tools in diplomacy, foreign affairs, and operational excellence. The *Enterprise Architecture* calls for extensive communication, coordination, and collaboration within the Department and with external organizations. The objectives and initiatives in the *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 computing, sophisticated data integration and analysis, and geographic information systems are essential if State is to achieve its strategic objectives and goals and satisfy its customers and constituents, notably the White House, Congress, other government agencies, U.S. allies, and above all, the American people.

This *IT Goals Paper* explains how IT will be a significant force helping State pursue its mission over the balance of this decade. As the lead international affairs agency, State is committed to being a leader in exploiting IT to further U.S. diplomatic aims.

Key IT Trends

The goals and strategies presented in this paper derive first from the requirements of the foreign policy mission, and second from best practices in management and IT. The Department is committed to maintaining a high quality, global IT environment that can exploit advances in technology as well as government-wide initiatives such as the e-Government initiative. Research and interviews revealed the following key trends and best practices, which are highlighted throughout this paper. The left column in Table 2 identifies key trends that will affect IT for the balance of this decade.

Table 2: In-Out Table Showing Key Trends and Best Practices

IN	OUT
Enterprise-wide, Government-wide solutions	Single bureau, single agency approaches
Rapid technology change and adoption	Reluctance to innovate
Knowledge as Department asset, proactively shared	Knowledge belongs to individual bureaus and is not shared
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 computing and telecommuting	Tethered to the desk
Voice/data integration/voice over IP	Separate networks
Voice input and speech recognition	Keyboards
Leveraging partnerships	Isolation
Automated, real-time language translation services	Limited ability to get documents translated
“Out of the box” commercial off-the-shelf (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 as utility	Non-standard, isolated IT environments
Adaptable networks—self-configuring, dynamic	Hardwired static networks
Risk management	Risk aversion

Vision—Partnership of IT and Diplomacy

In past years the Department’s IT program has provided essential support for administrative and consular functions, but has not been able to offer similar support for core diplomatic activities. Advances in technology make increased support for diplomacy feasible, and new challenges and opportunities make it imperative. The vision for 2010 is one in which IT becomes a much more active partner than it has been with the Department’s organizations and employees most directly involved in our diplomatic activities.

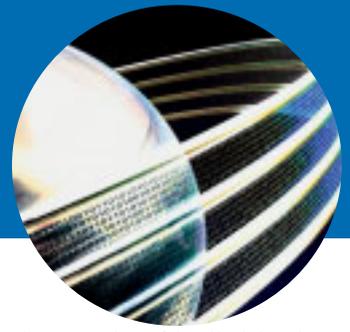
Vision
*Empowering diplomacy with tools
and information available anytime,
anywhere*

Five IT goals have been formulated to support this vision and the Department’s mission priorities:

1. ***The Right Information: Knowledge Leadership for Diplomacy*** – Superior diplomacy and decision-making facilitated by superior information.
2. ***Anytime/Anywhere Computing: Diplomats on the Move*** – Technology that makes the knowledge and communication resources of the Department available to personnel when and where they need them.
3. ***External Partnership: Diplomacy 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: Mission Effectiveness and Security*** – An approach that recognizes and balances the needs of diplomacy and security risks.
5. ***Work Practices and Workforce: Leading Change*** – IT professionals highly trained for mission support, and all non-IT staff trained to use technology effectively.

Descriptions of these five IT goals are set forth in the following pages. Tables 3 and 4, at the end of the paper, show how the five IT goals support the Department’s strategic objectives and goals and the Enterprise Architecture.

THE RIGHT INFORMATION: *Knowledge Leadership for Diplomacy*



1 Goal 1 will make available foreign affairs information tailored to the needs of individual officers, internal and external customers, and target audiences.

The Department of State is an information-producing machine whose annual output 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. In addition, Department personnel have access to the vast resources of the Internet and the networks of other government agencies. Yet much of this information fails to meet requirements because it is inaccessible, of questionable accuracy, out of context, not updated, or in the wrong format. As a result, our officers cannot easily find the information they need and are overloaded with marginally relevant information.

Knowledge Leadership is the Department's approach to improve knowledge sharing and collaboration within the Department and with our foreign affairs partners. The approach draws on State's deep subject matter knowledge of the foreign affairs environment, coupled with superior technology to empower personnel at all levels to make informed decisions and lead foreign policy formulation and implementation. Knowledge Leadership will help establish a knowledge sharing culture within the Department and the broader foreign affairs community. Engineering such a cultural change will require a significant initiative that focuses on four fronts: people, processes, organizations, and technologies.

Content Management Tools

- Taxonomy for classification, tagging, search and retrieval
- "Message" customized for the audience and purpose
- Data warehouse for integrated access to databases
- Intelligent, personalized search engines to retrieve the right knowledge and reduce information overload
- Customizable portals for organizing information
- Desktop publishing, contact management and desktop video
- User-friendly data management and analysis tools
- Document abstracting, cataloging, profiling
- Data mining and pattern analysis
- Knowledge management—expert locator, real-time question and answer
- Geographic Information Systems (GIS)

Department users will have access to an enterprise-wide content management service, staffed by researchers, information management specialists, and policy experts. This service will be responsible for managing the Department's substantive databases and content management tools and technologies, and assisting users with complex information management requirements.

Value-Added Logical Knowledge Bases

<u>Strategic Plan Area of Focus</u>	<u>Examples of Logical Knowledge Bases</u>
Regional Issues/Flashpoints	Israel and Palestine African refugees
Functional Issues	Economic data resources Arms control treaties
Interagency Coordination	Counter-terrorism Border security
International Influence	Biographical Info Public outreach and advocacy content

Users will draw on the following:

- Value-added **knowledge bases** containing pre-processed, high-quality information about high priority topics. See box above for examples.
- Intelligent **search and analysis** tools to help people overcome information overload and find exactly what they are looking for.
- **Collaboration tools** that support self-forming, self-managing professional networks and communities of practice and interest that overcome boundaries of geography, time and organization — both classified and unclassified. Collaboration tools will also include an expert locator.

Officers work on-line, using groupwear software, with counterparts from other countries and agencies to draft a NATO resolution

- Support for **outreach** through customer relationship management (CRM) systems that improve our ability to establish and sustain relationships with key contacts, support public diplomacy and advocacy, and strengthen content delivery to targeted audiences.

Public Diplomacy officers create “Blogs” that contain specialized content drawn from Department knowledge bases to target specific audiences

- An **enterprise portal** that gives Department users easy, desktop access to essential information and services, encouraging them to employ and share a full array of knowledge resources as part of their everyday work.

These practices and tools will position the Department to capitalize on the next wave of intelligent technologies and processes to strengthen the use of our knowledge resources —our databases and above all, our people—in the interest of foreign policy leadership. As discussed under Goal 5, these will also create a new, broader role for IT and Office Management Specialist (OMS) personnel as content managers and information consultants.



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.

ANYTIME/ANYWHERE COMPUTING: *Diplomats on the Move*



Goal 2 will provide an IT environment that allows full access to all needed knowledge and computing resources at anytime from anywhere in the world. The focus of this goal is to support **mobile computing** and to promote continuing and rapid technology innovation—absolute musts for modern diplomacy.

By its nature, diplomacy entails travel and mobility, as well as regular contact with people outside of State facilities. Effective diplomacy requires that our officers participate in policy discussions with the U.S. Government executive agencies and with Congress, meet with counterparts in foreign governments at executive leadership conferences, attend sessions of foreign parliaments and organizations, represent the U.S. before foreign and domestic organizations and publics and travel to other cities and countries. Our most effective diplomats 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 objectives. Much like others involved in advocacy or public relations, our diplomats spend a good deal of their time out of their offices in circumstances where effective access to State resources is essential.

Through this IT goal, the Department will provide technology to support the mobile employee. It will enable State's officers to use standard commercial personal digital assistants (PDAs), cell phones, laptops, and new devices as they emerge. These devices will deliver the knowledge resource products described under Goal 1, and will also allow full connectivity from home, while on travel, or at meetings. 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.



They will be easily able to consolidate and manipulate information from these multiple sources and formats. Voice input and output will be supported, and voice and data will be fully integrated. New and improving technologies, such as video conferencing and video mail, Geographic Information Systems (GIS), and language translation software will be made available as they are proven feasible.

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

- Always on—a global network as reliable 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 points to enable the mobile worker to access enterprise data, via “personal bandwidth,” to supplement enterprise bandwidth.
- Security—IT security solutions and updated Department policies will be required in order to exploit the full capabilities of mobile computing devices.
- 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 from multiple sources and paths.
- Global directory—a highly reliable directory is essential to enable people to access their data from anywhere, to identify experts, and to connect to other people. A government-wide international affairs directory, with entries for key NGO and foreign government staff, is necessary for the comprehensive connectivity requirements of modern diplomacy. The global directory will be extended beyond white, yellow, and blue pages to include green pages (information) and real-time information about users’ whereabouts, preferred delivery devices, and facility characteristics.

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.

As the political officer of the future leaves the embassy to call on the foreign ministry, his PDA is automatically reconfigured to continue to receive unclassified messages. In the car, he checks his unclassified e-mail via his PDA and sees that the Department wishes him to immediately deliver a new demarche to the host government.

The IT environment will function much as today’s electric and telephone utilities. End-users will be able to “plug in” to the network with any device regardless of location. The following strategies will contribute to the establishment of this ubiquitous computing environment:

- Centralization and standardization of servers and databases, building on successes such as the Enterprise Server Operations Center (ESOC)—allowing remote and

controlled access to and from anywhere, as well as critical infrastructure protection and business continuity planning.

- Expanding the centrally managed enterprise-wide Global IT modernization program (GITM) and further consolidating additional deployment and site visit activities.
- Labeling and “wrapping” all information—structured and unstructured—permitting complete and appropriate access to information from anywhere. Wrappers will be extended beyond security and retention and will include information necessary for rendering information on various device types and content adjustment or filtering based on the users’ current location. Labeling or tagging will be done for small units of information, enabling content to be assembled and reassembled in multiple ways for different purposes.
- Leveraging and promoting government-wide networks—for example, Secret Internet Protocol Routed Network (SIPRNET) and the Open Source Information System (OSIS), to maximize information sharing and minimize costs.
- Rapid and regular technology innovation—through an innovation laboratory, effective change management, and aggressive IT leadership supported enthusiastically by the Secretary of State and senior management. The innovation laboratory will include an integrated security engineering operation and will be explicitly charged with identifying and adopting leading-edge and secure COTS solutions that meet all mission requirements while clearly specifying any residual risk for management consideration.
- Rapid extension of technology innovations throughout the Department—we will improve our ability to move from proof of concept, to pilot and to full rollout more quickly. We will keep pace with the evolving open standards.
- Outsourcing the bulk of telecommunications and data services to take advantage of the global information infrastructure’s high availability and competitive price benefits. By leveraging highly secure, private network communications over commercial and satellite carriers, the Department will provide the necessary bandwidth to support new initiatives and expanded mobile diplomacy.
- Teaming with other agencies to leverage disaster recovery and business continuity capabilities by using consolidated IT and communication facilities around the world.
- Exploration of open source options to reduce dependence on a single vendor for critical operating system software and to reduce security risks.



EXTERNAL PARTNERSHIP: *Diplomacy Through Collaboration*



3 Under Goal 3 the Department will establish an IT environment that promotes external connectivity and information sharing. This goal draws on the concepts of the e-Government initiative, applying it both to diplomatic operations and administrative processes. Through this goal the Department will provide IT support to collaboration and coordination activities directly related to its diplomatic mission. It will also rely increasingly on and promote interagency processes and systems for administrative work. Implementation of this goal will reduce costs and improve productivity.

The Department works in concert with other U.S. Government agencies, Non-governmental Organizations (NGOs), and foreign governments in promoting the U.S. foreign policy agenda. The Department also offers services to U.S. citizens and businesses, such as travel assistance and support for international trade and exports.

IT has supported some level of intergovernmental information sharing through SIPRNET, OSIS, and Intelink. The *Department's Strategic Plan* calls for greater levels of collaboration over the next five years. In particular, it lays out the need for greater interconnections with:

- DoD and CIA in common efforts to ensure regional stability in various parts of the world;
- Homeland Security in screening foreigners who wish to visit the United States or immigrate to it;
- USAID, which is responsible for economic and social development, humanitarian relief, strengthening fragile states, mitigating transnational ills, and supporting U.S. strategic interests;
- Domestic and foreign press, domestic and foreign publics;
- Governments of friends and allies with whom we have common interests in global or regional affairs; and
- International organizations such as the United Nations, NATO, international development banks, and NGOs who are our partners in pursuing strategic objectives such as sustainable development and promotion of human rights.



The Department will expand services to U.S. citizens domestically and overseas by leveraging IT. Examples include adoption tracking, passport issuance, and access to travel information and advice.

In addition, the Department is committed to the President's Management Agenda and to OMB's efforts to consolidate the administrative systems that support government agencies. The Department will be an eager customer 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 200 locations around the world, the Department would benefit greatly from government-wide administrative services and systems that enabled streamlining of our overseas presence.

Four broad strategies will be pursued to achieve this goal:

- State will develop a joint IT strategic plan with USAID, followed closely by a program to institute shared networks and systems, and the development of collaborative tools to the maximum extent possible.
- The Department will work with OMB and GSA to seek to establish a government-wide IT infrastructure for all agencies involved in foreign affairs. Such an infrastructure will include a network and government-wide directory that connects all government employees working overseas, and will provide access by all authorized employees of any U.S. Government agency to foreign affairs knowledge bases and analytical tools including collaborative software.
- The Department will establish a secure extranet to promote information sharing between the U.S. foreign affairs community and external organizations, including foreign governments, NGOs, regional and global organizations, the public, and business.

Under a new Department program, bureaus and posts have been developing and maintaining classified web sites available on SIPRNet to promote interchange of important classified information. The lessons learned from this experience will be incorporated into future strategic efforts to centralize web site development to broaden and control access to vital information throughout the foreign affairs and intelligence communities. This will support a key Department function—publishing critical and timely information for its customers.

- The Department will streamline and reorganize its administrative operations to deliver only those services that cannot be delivered by government-wide systems and processes. In all cases, we will emphasize self-service and centralization of back-office functions and systems, reducing the numbers of administrative staff in the Department and especially overseas—increasing the “tooth-to-tail” ratio, and placing more emphasis on competence in the provision of administrative services.

To accomplish this goal, the Department will participate actively in and leverage government-wide initiatives, such as today's Quicksilver e-Government efforts, with the aim of freeing up resources that can be devoted to foreign affairs activities. By 2010, the Department expects to be using government-wide systems and services for all administrative activities, except those unique to overseas operations (e.g., arranging local hiring, housing, and purchasing).

This goal explicitly supports OMB’s goal of a U.S. government-wide IT Enterprise Architecture. It is also a logical extension of Goal 1, The Right Information, and Goal 2, Anytime/Anywhere Computing, throughout the U.S. Government in support of the President’s Management Agenda (PMA).



Our e-Government Vision

The Department will further the goals of e-Government to improve services and transactions for citizens and businesses through the organization, dissemination, and sharing of more and better information.

The *Department* advocates greater integration and sharing (collaboration) of mission critical information through the development of a single government network, a single government-wide directory, and shared virtual knowledge bases.

The Department is committed to moving its administrative support systems (e.g., Human Resources, Logistics, Financial, Budget, Payroll, Acquisitions, Travel) to centrally managed, government-wide solutions as soon as practicable.

RISK MANAGEMENT: *Mission Effectiveness and Security*



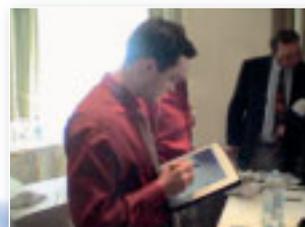
4 Under this goal, the Department will establish a strengthened IT security program based on risk management, critical infrastructure protection (CIP), the Federal Information Security Management Act (FISMA), and deployment of pre-approved security solutions. The intent is to enable rapid and secure introduction of new technologies. The risk management process will be engineered to support rapid management decision-making, yielding a decision normally within 90 days.

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.

In the past, the Department has been slow to adopt new technologies, in large part due to security processes that rely too heavily on security experts and not enough on managers, IT professionals, and end-users—that is, the employees carrying out the Department’s mission. Managers have been unwilling to make timely decisions, and security assessments have focused largely on the risks of security breaches, and not enough on the dangers of overly restricting access to required information. The introduction of new technologies must be business driven, not security restricted. It must also be timely to ensure that solutions are not bordering on obsolete when accepted.

Comprehensive security engineering has not received enough attention or resources, and it has not been conducted as a collaborative effort involving security, IT, and end-user experts. Security debates have been an “us and them” affair, with security expertise concentrated in the security organizations of the Bureau of Diplomatic Security and the IRM Bureau, and no one with authority representing the end-users and diplomats. Under this goal, the Department will change the process to establish effective risk management. The following list exemplifies the types of decisions that must be made now and in the future:

- Wireless laptops and networks, providing access from home and on travel
- Integration of voice mail and e-mail
- 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
- PDA access to classified networks



- Inclusion of Sensitive But Unclassified (SBU)/NOFORN on OpenNet
- Inclusion of EXDIS on ClassNet

The Department must explore with its national security partners the concept of integrating Confidential into the OpenNet environment, not unlike the architecture employed by the British Foreign Office. The Department must also position itself for the rapid implementation of full multi-level security when available.

Four key elements of IT security will demand attention under this goal. First, is the establishment of true risk management. Characteristics of an effective risk management process include:

- 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.
- 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 alone.
- 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.

In order to accomplish effective risk management, the Department will establish a user-led, business driven, risk management process staffed by end-users, IT and security experts. This process will be designed to support rapid evaluation and adoption of new solutions. It will be based on a thorough exploration of the risks of deploying or not deploying proposed technologies. If the Department is going to fulfill its responsibility of foreign affairs leadership, it must innovate to provide its employees with the knowledge they need. The Office of e-Diplomacy will continue to provide a strong foundation to lead this process.

The Department as an organization must manage and accept risks—
not place the burden on the individual user

Second, the IT security program will deliver improved technology and management solutions for increasing the *reliability and availability* of the IT infrastructure, and to ensure information integrity and proper authentication of information creators and users. To accomplish the goals of ubiquitous computing and make information available whenever and wherever needed, systems and networks will need high levels of fault-tolerance, redundancy, regular back-ups, and highly professional management. The Department will position itself to take advantage of the rapid advances in security technologies and best practices, such as advanced guard technology and multi-level security solutions for linking classification layers, business continuity planning, data encryption and centralization, thin client, and other approaches. The Department takes seriously the mandate from OMB to strengthen infrastructure and system security, and will use its IT Capital Planning process to promote security enhancements.

Third, we will clearly differentiate and set different *policies* and barriers for classified vs. unclassified systems, including those that handle SBU data. For unclassified systems (including SBU), we are committed to rapid adoption of new technologies that are commonplace in the commercial world. Other organizations, such as financial institutions, protect sensitive data, comparable to State's SBU, using the full capabilities of modern networks and systems, including remote access, wireless devices, and synchronization of systems. We must do the same if the Department is to remain competitive and effective. If necessary, we will improve the labeling of SBU information to prevent unauthorized access; however, the existence of SBU information will not be allowed to stymie the use of new technologies on unclassified systems that are important in enabling our diplomats to do their jobs.

Fourth, we will establish and document pre-approved (by the risk management office, the Enterprise Architecture and the Configuration Control Board) security solutions or modules that can be re-used throughout the Department without further review or approval. We will apply the emerging Certification and Accreditation processes to these solutions, ensuring that they provide the strong security required. Examples of security solutions to be deployed are:

- Digital signature
- Smart IDs and biometrics for authorization and authentication
- Guard technology for transferring data across security levels
- Use of firewalls, encryption, Secure Sockets Layer (SSL), and other technologies to provide intranet/extranet access to internal systems
- Configuration of PDAs and laptops for remote and wireless connectivity
- Password management for sensitive applications

When the U.S. established its new diplomatic presence in Kabul in 2002, State was unable to establish secure telecommunications and provide remote access to needed IT systems and data under the battlefield conditions faced by our diplomats. In the same environment, the Department of Defense was able to provide troops with laptop access to classified data and systems. DoD was able to set up this effective, secure, and mobile IT environment in a matter of days. State must be able to do so as well.

Renewed emphasis on these security solutions, along with a sensible risk management policy, promises to increase IT security and improve the ability of its workers to accomplish their goals without unnecessary security impediments.

MISSION IS JOB ONE!



WORK PRACTICES AND WORKFORCE:

Leading Change



5

Under IT Goal 5, the Department will improve and streamline its operations so it can support and fully exploit the IT environment to be put in place, and can adapt to the increasingly rapid changes likely to occur. This Goal will focus first on the work practices and personnel engaged in diplomacy, and then on aligning IT processes and staff to support the mission-related work and personnel. The Under Secretary for Political Affairs will take the lead on the processes of diplomacy, and the Bureau of IRM will lead the work to revamp the IT processes and workforce—all of this focused not just on information technology but the way that technology is used to further American foreign policy goals.

As technology becomes more pervasive, the Department's foreign affairs officers will become increasingly reliant on the use of sophisticated technology in their daily activities. Under this goal, the Department will ensure that foreign affairs officers 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 used, much as was done under the *FY 2001–2005 IT Strategic Plan*.

Training for Diplomacy

- Incorporate new technologies into FSI courses such as Political and Economic Tradecraft
- Create targeted user training for specific job categories/cones (e.g., B&F, OMS, Econ Officer)
- Use multiple training vehicles such as formal training, Computer-Based Training, one-on-one at people's desks
- Incorporate change management into training—use illustrations and focus training to inspire people to adopt new technologies and use them effectively

OMSs will be trained to develop into an organizational resource for embassies in IT areas, such as publishing content developed by policy officers on classified web sites, and formulating effective Internet and database searches.

The IRM Bureau and the IT workforce will change to mirror the new, broader focus on information resources: to help our personnel do their day-to-day 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. The IRM Bureau will focus on core information and user support activities, and will outsource non-core operations to the private sector or government-wide services. The end result will be an IRM Bureau organization re-tooled to provide knowledge leadership services, high-end consultative support to end-users, and technical support for the few unique Department applications.

The Department will revamp its IT workforce, building on its recent successes in recruitment, retention, and training. The new IT worker will be skilled as an information consultant, able to help Department personnel 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 will no longer worry about technical support for cranky hardware and applying software patches, tasks which consume far too much of their time today. Instead, they will become a valuable part of the Country Team, providing direct support for the post's strategic priorities. A new professional discipline will be identified. The "knowledge worker" will understand both the mission of the Department 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.

The success of this Goal and the entire strategic plan depends heavily on the Department's ability to promote innovation, absorb new technology, and make changes far more rapidly than it has done in the past. This will require effective change management and commitment at the highest levels of the organization. It will also require a systematic examination and clarification of the Department's work processes for mission and management related activities. This will enable a more effective IT program focused on 21st century diplomacy. It will also allow officers to make better use of the collaborative, decision support, and information sharing tools and transfer their expertise from post to post.

Beyond the \$3,000 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.

Next Steps

The immediate next steps to pursue the goals presented above are to develop a new IT Strategic Plan and complete the key projects that will take the Department to the starting point for the new plan (e.g., SMART, bandwidth).

The new *IT Strategic Plan* will flesh out the five goals and define a set of strategic initiatives to achieve them. The Plan will specify a timeline, major milestones, performance measures and resources needed for each initiative, as well as a consolidated critical-path-based plan for the entire IT program. The Plan will be coordinated with any changes in mission priorities and will support joint IT planning with USAID.

In parallel with the development of the new *IT Strategic Plan*, we will solicit guidance from the e-Government Program Board on needed pilot efforts to test and fine-tune specific strategies and approaches, especially those that represent a significant departure from the way things are done today. These pilot efforts should not only include exploration of new technologies, such as Customer Relations Management (CRM) software, data mining, tailoring and personalizing content, but also experimenting with organizational changes (outsourcing messaging, competitive sourcing, training IT staff as information consultants, setting up a risk management organization) to improve the delivery of new technologies. Personnel with different specialties will be consulted in pursuing these pilot efforts, so that IT solutions are focused on work processes and associated information requirements.

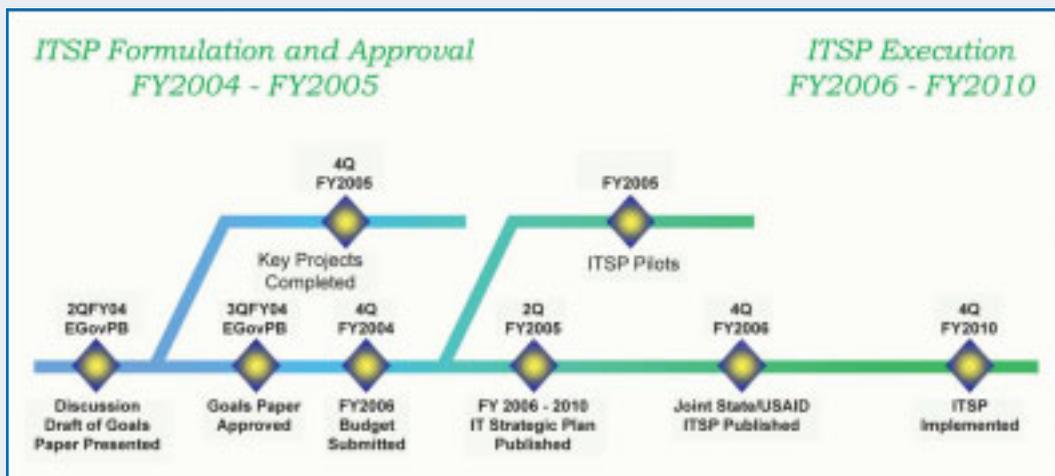


Table 3: Examples of IT Support for Department Goals and Objectives

Department Strategic Plan		IT GOALS				
Department Strategic Objective	Department Goals	1. The Right Information	2. Anytime/ Anywhere Computing	3. External Partnerships	4. Risk Management	5. IT Organization and Workforce
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 counter-terrorism) 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 diplomats 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 and 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
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 Programmatic 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

Table 4: ITSP Goals Support Enterprise Architecture

EA To-Be Technical Solutions		Right Information	Anytime/ Anywhere	External Connectivity	Risk Management	Organization & Workforce
1	Out-Of-Office Communications	S	P	S	S	S
2	Audio Conferencing	S	P	S	S	
3	Video Conferencing	S	P	S	S	
4	Message Management	P	S	S	S	S
5	Instant Messaging	S	P	S	S	
6	Collaborative Work Environment	P	S	P	S	
7	Enterprise Information Management	P	S	S	S	S
8	External Information Exchange	S	S	P	S	
9	Enterprise Identity Management	S	S	S	P	
10	Learning Management	S			S	P
11	Program Resource Management			S	S	P

 P = primary
 S = supporting

ACKNOWLEDGMENTS:

Bruce Morrison, Chief Information Officer would like to thank the IRM Planning Office for developing the FY 2006–2010 IT Goals Paper:

Kenneth R. Alms*	Donald C. Hunter
Michael A. Cesena	Karen Mummaw*
Janice J. Fedak*	Andy Tainter
Wally Francis	Andrew Winter
Barry Finkelstein	

The IRM Planning Office would like to thank the following Department of State individuals:

David E. Ames	E-gov Program Board	Frank E. Moss
Jay Anania	Travis Farris	Charlie Ries
Mark Boyett	Marc Grossman	Daniel P. Sheerin
Bruce G. Burton	John L. Hopkins	Richard J. Shinnick
Peter H. Chase	James H. Holmes	Stephen P. Shinnick
	Joe B. Johnson	

American Embassy Paris—Ambassador Leach, Mark Abbey, Bernie Abinader, Valerie Belon, Jean Francois Blondelet, Kasirat Choonit, Wilson Estell, Randall Grover, Richard Gunn, Michael Hoza, Kibby Jorgensen, Bob Kirk, Barbara Lankford, Jim Melville, Linda Safta, Kate Schertz, Kerry Weiner, Douglas Wells, Alex Wolff, Michael Zorick

American Embassy Prague—Rich Appleton, Robert Barr, Mark Canning, John Dockery, Scott Learmont, David Rowles

American Embassy Ouagadougou—Ambassador Holmes, Elizabeth Bailey, Eric Benjaminson, Todd Haskell, Reggie Hopson, Josetito Nakpil

We would also like to acknowledge those individuals and groups outside the Department of State:

Barry Fulton, George Washington University
J. Stapleton Roy, Kissinger Associates
Robert Gallucci, Georgetown University
Charles Schmitz, Retired FSO
Richard O’Neill, Highlands Forum
Alan C. Wade, CIO George Bush, Center for Intelligence
Gartner
META Group

We offer special thanks to A/RPS/MMS, in particular Sally Brennan and William Palmer for their outstanding contributions to the design and publication of this paper.

*If you have questions or comments concerning this paper, please contact the IRM/BPC staff indicated above.

