

**U.S. Department of State
Information Technology Tactical Plan
(ITTP)
Fiscal Years 2011-2013**





Table of Contents

INTRODUCTION	3
Plan Purpose and Scope	3
Planning Methodology	3
Goal 1: Digital Diplomacy	6
Goal 1.1 – Social media to promote diplomatic initiatives	6
Goal 1.2 – Creation and management of knowledge in support of diplomacy	8
Goal 1.3 – Integration of management systems	10
Goal 2: Cloud Computing	13
Goal 2.1 – Cloud-based application and processing environment	15
Goal 2.2 – Redesigned and consolidated network	20
Goal 2.3 – An evolving suite of user-driven mobile technology and end-user services	23
Goal 2.4 – Enhanced risk management, cyber security, and reduction of sensitive holdings	26
Goal 2.5 – Green computing	29
Goal 3: State's IT Leadership	30
Goal 3.1 – Governance	30
Goal 3.2 – Performance Management	32
Goal 3.3 – Workforce Management and Training	33
NEXT STEPS	35
Acronyms	36

INTRODUCTION

Plan Purpose and Scope

This Information Technology Tactical Plan (ITTP) specifies the activities, milestones, deliverables, roles and responsibilities to implement the [FY 2011-2013 Information Technology Strategic Plan \(ITSP\)](#). The Tactical Plan is enterprise wide, covering all IT projects and investments, and all bureaus and posts.

Planning Methodology

The Tactical Plan is being developed collaboratively with project sponsors and managers. The Bureau of Information Resource Management (IRM) is responsible for plan development and for managing and monitoring Plan progress on behalf of the Chief Information Officer (CIO). This initial version reflects the vision and priorities of the ITSP and provides a high level road map of key projects and initiatives. As depicted in Figure 1, IRM is working with partners in the bureaus and offices responsible for specific projects to refine and finalize the ITTP. The Quadrennial Diplomacy and Development Review (QDDR) establishes policy and direction for the implementation of the Department’s strategic goals, and will provide a basis for refining the ITTP as it is implemented.



Figure 1 Implementing the IT Strategic Plan

IRM established a rigorous methodology to develop and manage the Plan, reflecting its importance in accomplishing the Department's strategic IT goals and objectives. Highlights of the methodology are as follows, with additional discussion below:

- ***Collaborative implementation*** – in each of the 11 strategic sub-goals projects will be developed in conjunction with partners, who are encouraged to engage other offices to work in collaboration and supply needed expertise.
- ***Transparency through dashboards*** – IRM will track progress of project managers with management dashboards, using green, yellow, and red indicators to provide a simple, unambiguous real time status. The CIO and eGov Program Board will receive quarterly reports and regular progress briefings.
- ***Gap analysis and transition of existing IT investments and projects*** – transitioning from the status quo to the future envisioned by the ITSP will be accomplished via a series of coordinated projects. For the purposes of this plan, a project is a set of activities with a well-defined scope and objectives, a clear beginning and end, and assigned resources that deliver a tangible product.

Some of these projects already exist, although they may require adjustment, and others will be established. IRM will conduct a detailed analysis of the Department's existing IT portfolio of investments and projects to determine the extent to which they can fulfill the requirements of the ITTP and if so, to identify any refinements needed. This analysis will reflect the Federal CIO's "Cloud First" policy, and will be reviewed with investment and project sponsors and technical managers prior to publication.

- ***Pilot projects to involve key stakeholders and identify viable IT solutions*** – the Plan calls for engagement of interested bureaus and offices to serve as champions to pilot test new technologies and approaches, analyze the results, and help formulate and engineer production projects and solutions.
- ***Services oriented operations*** – there will be a menu of IT service offerings with predefined service levels and pricing documented in service level agreements (SLAs). IT operations will be structured around these services.
- ***Quadrennial Diplomacy and Development Review*** – begins by assessing the world as it is today and the changes expected in the years ahead. It will drive U.S. diplomatic and development objectives for the foreseeable future. The tactical plan will provide the IT resources to support these objectives.



- ***Resource adjustments*** – the transition planning will specify any needed shifts in resources. These activities will be carried out as planned and within currently available resource levels. Project managers have wide latitude to shift resources from other, lower priority activities as necessary to ensure that these strategic priorities are addressed. IRM will work with project managers on resource planning and management.
- ***The Plan as a living document*** – the Tactical Plan will be published as an electronic document and updated at least twice a year.

Plans will include quarterly tangible milestones to demonstrate progress, and project managers will be held accountable for staying on schedule. More detail will be provided for FY 2011, less for the out years.

As work proceeds, the plan will be updated, and progress will be reported on dashboards. Acceptable milestones are completed activities or measurable results; works in progress are too ill-defined to be clear indicators and will not be accepted. The major activities are spelled out below, along with the key characteristics and performance measures. Service levels will be developed collaboratively between customers and service providers.

Goal 1: Digital Diplomacy

This goal focuses on information and applications that support the Department's global mission. This includes collaboration with inside and outside partners including the public. It promotes innovative use of modern cloud-based technologies, such as social media, wiki, and collaboration, along with enhanced capabilities for database and application management and integration. It includes three sub-goals.

Goal 1.1 – Social media to promote diplomatic initiatives

Scope of Work:

This sub-goal will create and sustain a shared environment for social media tools, promoting expanded use of cloud computing services such as Facebook™, Twitter™, and LinkedIn™ for diplomacy. This sub-goal also builds on the Department's experience with the in-house services such as Communities@State, an internal blogging program developed by IRM's office of eDiplomacy, that extends the internal social media experience to a broader, shared environment for both internal and external service, unclassified and classified.

A key role for IRM is to create a technical environment that facilitates access to an evolving set of tools, both for secure internal use and for engaging with external partners and overseas and domestic publics. International Information Programs (IIP) will continue to work with the Foreign Service Institute (FSI) to incorporate use of social media tools in training programs developed under Goal 3.3 for both IT and non-IT personnel.

Key performance indicators for Goal 1.1 are:

- Demonstrated increasing demand for and use of social media throughout the Department, including at overseas posts, as evidenced by usage trends.
- Effectiveness of engagement with foreign publics as evidenced by participation levels and survey results.

Table 1 Goal 1.1 Major Projects

Projects	Description
Social Media Requirements Analysis	<ul style="list-style-type: none"> • Gather and validate requirements for unclassified and classified environments • Engage champions/partners for social media projects • Include collaboration tools for online document development and virtual meetings
Social Media Business Model	<ul style="list-style-type: none"> • Customer demand will be the key driver • Specifications and road map for a shared social media environment • Outsourced to enforce service guarantees • Promote social media program for foreign outreach at overseas posts, phasing in over the next 2 years
Social Media IT Environment	<ul style="list-style-type: none"> • Levels of service, distinction between base offerings vs. fee for service • High level of flexibility in order to react swiftly to evolving events • Communication plan showing service offerings, pricing, service levels, etc. • Customer oversight process • Specify and implement measures for dashboard display



Goal 1.2 – Creation and management of knowledge in support of diplomacy

Scope of Work:

Goal 1.2 focuses on organizing tailored information for specific audiences, and making it available through modern web tools. It includes expansion of existing capabilities like Diplopedia, as well as ongoing implementation of innovations in knowledge management; virtual media libraries with video, audio and graphics; search engines; geospatial technology and language translation.

The IT innovation fund will be incorporated into this sub-goal, providing seed money to encourage research, experimentation, and pilot testing of new information-based IT initiatives. Bureaus and posts will be encouraged to apply for innovation fund grants and to explore a wide range of ideas for applying knowledge-based IT to the conduct of diplomacy. Other agencies and private sector organizations known for their IT innovations will be consulted to generate ideas.

Key performance indicators for Goal 1.2 are:

- Demonstrated value of information products to core customers (U.S. diplomats, other U.S. agencies, U.S. and foreign publics, other key stakeholders), where value is measured by volume of use, degree of active participation in collaborative efforts like Diplopedia, and stakeholder feedback.
- Interest in the innovation fund as measured by number and quality of proposals; and success of converting innovation fund projects to operational solutions with broad user community.

Table 2 Goal 1.2 Major Projects

Projects	Description
Next Generation Messaging System	<ul style="list-style-type: none"> • Cloud-based • New perspective, independent of existing messaging operations, drawing on best practices in industry and government
IT Innovation Fund	<ul style="list-style-type: none"> • Requires guidance and criteria for choosing projects, including scope and scale of desired projects • Proposals must include a plan for life cycle operations and costs, and for frequent updating of content • Process for tracking awards and success in transitioning to production solutions • Lessons learned to be documented and used to refine grant process • Encourages well-conceived, high-impact innovations through the use of existing or the development of new technologies or processes • High-level panel of IRM section representatives will review and approve submissions based on strict criteria
Enterprise-wide Content Management Capability	<ul style="list-style-type: none"> • Content management process for dating and tracking information • Web analytics to measure and report relevance and importance • Automatically timestamp published information
OpenGov	<ul style="list-style-type: none"> • Consider extended capabilities and information of interest to the public (e.g., tips on foreign cultures of use to business and leisure travelers) • Plan for steady publication of data on OpenGov and the internet • Plan for engaging outside experts to enhance Diplopedia content
Innovative tools for diplomacy	<ul style="list-style-type: none"> • Plan for such tools as pattern analysis, language translation, mapping, etc. • Enhanced search and web-crawling



Goal 1.3 – Integration of management systems

Scope of Work:

This sub-goal will engage the major functional bureaus in the Department in a coordinated effort to standardize and integrate key information to support management decision-making and business process efficiency. It will pursue dramatic expansion and enhancement of technologies just beginning to be deployed at State, notably the Enterprise Service Bus (ESB) for linking multiple systems and the Enterprise Data Warehouse (EDW) for consolidating critical data subsets to support management dashboards, analysis, and reporting. This sub-goal also entails more self-service and streamlining workflow for management systems.

Accomplishment of this goal requires focused data architecture, including a data model, an approach to normalizing data among the bureaus and major management systems, and standardization of key data elements. While data architecture work has proven difficult in the Department, because of a highly decentralized data ownership environment, it is possible to make substantial progress in this area.

The following are keys to success:

- Developing the data products incrementally, taking small steps until progress has been demonstrated.
- Scoping the subset of information included in the initial efforts to be manageable and of clear importance and value. Attempting too big a project will be unsuccessful.
- Engaging one or more committed partner/sponsors projects from among the functional bureaus.
- Pilot-testing the ESB and EDW for one or two projects that are visible and for which data integration has clear value. For example, we may work with M/PRI to integrate data from all of the major management systems in support of post planning and rightsizing efforts. The goal of the pilot is to build momentum and confidence that this is the right path.

This sub-goal also includes enhancing existing management applications to ensure they are ready to run on iPhones and other mobile devices, and to take full advantage of web and cloud capabilities, including transition to IPv6, using standard identity management and other application and platform services.



Key performance indicators for Goal 1.3 are:

- Demonstrated success in normalizing data across two or more major corporate systems, identifying authoritative source for each key data element and eliminating redundancy.
- Increased number of systems in the EDW, and increasing volume of usage of EDW business analytics and reporting products.
- Demonstrated success implementing an interface between two or more systems using the ESB, and development of data to indicate the cost-effectiveness of the ESB vs. conventional interface development.

Table 3 Goal 1.3 Major Projects

Projects	Description
Enterprise Data Architecture	<ul style="list-style-type: none"> • Prioritized set of core management systems and data elements, along with authoritative source for each • Focus on information that needs to be shared • Consider IPMS/ICAM as the partner for data modeling and normalization • Normalization pilot using IPMS/ICAM data • Analysis of pilot and plan for extending to the remaining management systems
Enterprise Service Bus	<ul style="list-style-type: none"> • Schedule for ESB production deployment with quarterly milestones • Explore a suitable pilot project and partner • All interfaces to be developed using the ESB -- no more investment in point-to-point connections
Enterprise Data Warehouse	<ul style="list-style-type: none"> • Lessons learned analysis drives refinement to EDW • Introduction and promotion of enhanced business intelligence tools and training to ensure EDW value • Phased plan with quarterly progress reports via the dashboard • Consider M/PRI as partner for rightsizing initiative using EDW
Concierge	<ul style="list-style-type: none"> • Key initiative for demonstrating cloud computing based solution • IRM's initial Software as a Service (SaaS) offering
Transition of Management Systems to ITSP Services	<ul style="list-style-type: none"> • Make management systems "mobile ready", "cloud ready", "ICAM ready" technologies • Long-term program to extend applications to the cloud and mobile devices • Coordinated and compliant with the cloud computing application architecture

Goal 2: Cloud Computing

This goal focuses on global access to Department information and services via a robust, worldwide, web-based infrastructure. Under this goal, State will build multiple information environments to serve different user groups, including Department personnel, U.S. agencies operating overseas under the authority of the Chief of Mission, Non-Governmental Organizations (NGOs) and businesses and the public. It includes five sub-goals.

Table 4 presents a set of characteristics of cloud computing defined by the National Institute of Standards and Technology (NIST).

Characteristic	Discussion
On-demand self-service	Consumer can unilaterally and automatically provision computing capabilities (i.e., server time and network storage) as needed, without requiring human interaction with service's provider.
Broad network access	Capabilities are available over the network and accessed through standard mechanisms through heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
Resource pooling	Computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).
Rapid elasticity	Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale up or down. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource monitoring provides transparency for both the provider and consumer.

Table 4: NIST Characteristics of Cloud Computing



The Department of State's strategy is to tailor the concepts and characteristics of cloud computing to provide cost-effective IT services in support of the foreign affairs mission. Benefits will include enhanced mission effectiveness, improvement in management services, and advances in the distribution and use of IT resources. State's objectives for cloud computing are:

- **Mission support** – delivering anytime, anywhere computing, and tailored application and web services to support State's global mission of diplomacy and development, including internal and external collaboration, dynamic delivery of new capabilities and solutions, and ready access to information.
- **Efficiency** – resulting from standardizing and virtualizing services, reducing the need for IT technical support personnel physically located around the world, and re-use of modular components for multiple purposes.
- **Security** – storing and accessing data from the cloud will eliminate the need for data storage at overseas locations, thus reducing security risks associated with information protection and increasing the speed with which a post could be evacuated in the event of a crisis, thereby increasing personnel and physical security.
- **Business continuity** – providing high levels of redundancy and automatic backup of all data and applications.
- **Scalable capacity** – delivering scalable network, server, and platform capacity wherever and whenever needed.

The Department has established the following guiding principles in pursuing cloud computing:

- Build on current initiatives, refining them as needed to realize the functional benefits of cloud computing.
- Proceed incrementally, implementing initial capabilities rapidly, then refining and expanding.
- Be customer-driven, providing mechanisms for listening to senior diplomats, executives, and end-users, and responding to their priorities and requirements.
- Minimize private and local data and processing, consolidating everything in the common, multi-provider, cloud environment.
- Use General Services Administration (GSA), public, and commercially available services when security conditions permit.
- Reuse components across applications.
- Security challenges are present in all computing environments, and cloud computing is no exception, requiring a close examination of the risks.



Goal 2.1 – Cloud-based application and processing environment

Scope of Work:

Goal 2.1 will establish a processing environment that supports cloud computing for internal and external customers. It will reduce infrastructure complexity and cost, increase systems security, enable centralization of critical information stores and the associated applications needed to access, process, and share information. Included will be two distinct cloud environments which are also depicted in Figure 2:

- Public or external/community cloud(s) to foster collaboration with State's partners, foreign governments, and U.S. and foreign publics. Services would include platform and software as a service.
- Internal or private cloud to support State and other U.S. Government agencies using the Foreign Affairs Network (FAN). The internal cloud will include classified and unclassified processing and data. The internal cloud will make use of Virtual Private Cloud services for expansion and unclassified processing.

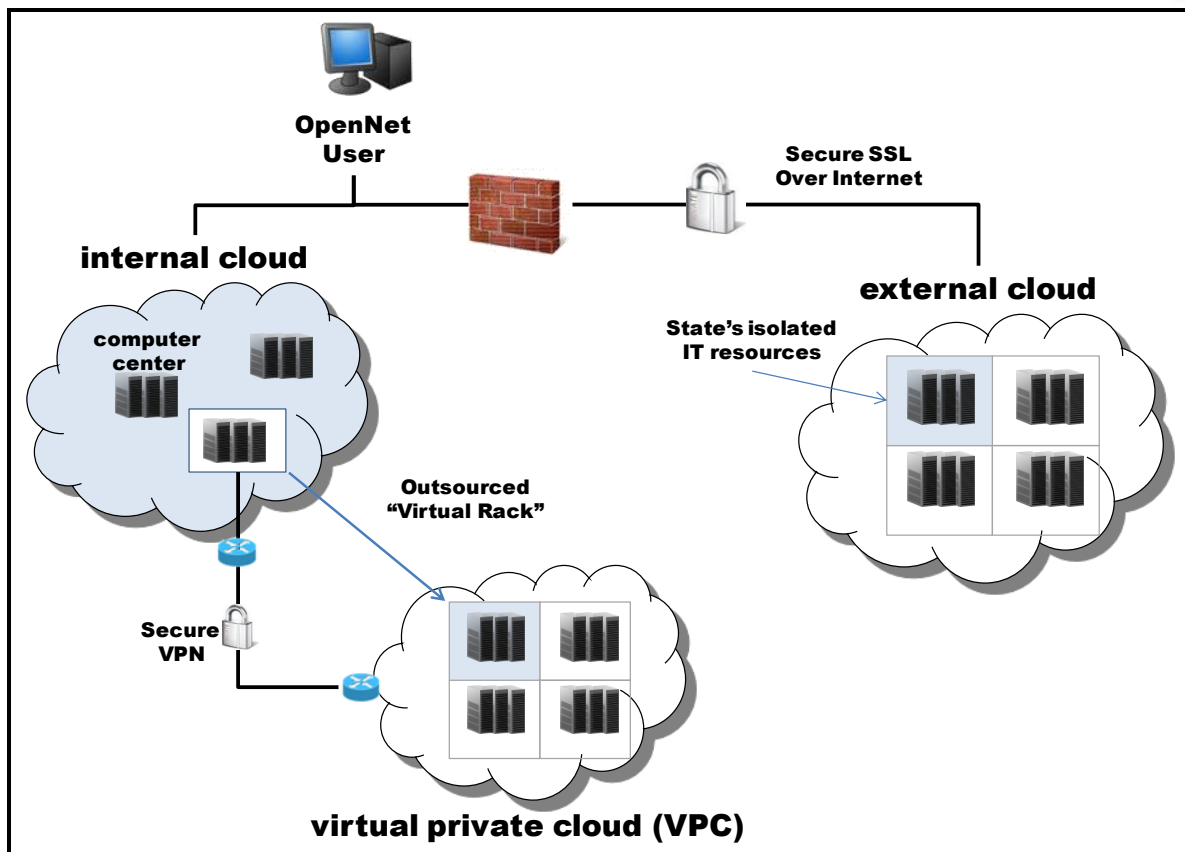


Figure 2 State's Cloud Computing Environment

Goal 2.1 must accomplish the following critical objectives of cloud computing:

- Ability to expand or contract capacity rapidly, to respond to business customer needs and to ensure that all performance requirements are met.
- Cost-effectiveness in delivering capacity.
- Flexibility and rapid response in delivering functionality and responsiveness needed by internal and external business customers.
- Provide core enterprise services that business customers can leverage to improve performance and lower risk.



To accomplish these objectives, IRM will establish a commercial-quality business enterprise with a standard menu of service offerings, service level agreements, and pricing, with performance standards set in service level agreements (SLAs). For example, adding substantial capacity to accommodate a new database or major expansion might require “X” days, while increased capacity to support a new collaboration web site with the public might be delivered within two hours. Cloud services will be delivered via a hybrid environment, in which capacity is provided by in-house resources at the Enterprise Server Operations Centers (ESOCs), and outsourced resources delivered via the private sector. The ESOCs will be the focal point for cloud services, providing virtual processing centers with dynamic workload balancing and a full set of standard, menu-driven application and platform services. Outsourced services will enable rapid, cost-effective expansion and contraction of capacity with minimal capital investment by the Department. Outsourced services will also ensure that State’s cloud environment keeps current with best practices and technology innovations. As ESOC equipment needs replacement, the first preference will be to outsource the required services, consistent with the Federal “Cloud First” policy.

State also will refine its approach to risk management by using, whenever possible, government wide programs such the Federal Risk and Authorization Management Program (FedRAMP) in order to take full advantage of cloud computing. While the CIO is the Department of State’s Designated Approving Officer for information security and assurance, the CIO will delegate to system owners and data sponsors the primary responsibility for determining level of acceptable risk for their data. IRM will be available to provide analyses and recommendations as well as enterprise services (such as single sign-on, portal hosting) under the SLAs that mitigate some of the system sponsors’ performance and security risks, but system sponsors will perform the risk management and risk decision making in order to determine the proper tradeoff among security vulnerability, cost, access requirements, and functional capabilities to be delivered via the cloud.

To move rapidly to establish a customer-focused cloud environment, IRM will engage a major system sponsor to serve as a pilot and champion for cloud computing. IRM, in consultation with customers, will determine realistic cloud computing requirements and a business model for delivering cost-effective cloud-based services. IRM recommends that ILMS be approached to serve as the champion. ILMS is a mature system initiative with global reach, and ILMS management has proven flexible in exploring innovative technologies. If cloud computing can work effectively for ILMS, we can then proceed to explore its applicability to other corporate systems.

Key performance indicators for Goal 2.1 are:

- Proven ability to expand and contract processing and data storage capacity on demand according to SLAs, based on pre-established service levels, such as providing additional virtual storage within “X” hours as noted above.
- Demonstrated cost savings due to use of virtual cloud services.
- Internal and external business customer use of and satisfaction with cloud services, performance, and risk mitigation in accordance with established SLAs.
- Increasing volume of information of various types stored in cloud vs. locally.

Table 5 Goal 2.1 Major Projects

Projects	Description
Cloud Computing Requirements Analysis	<ul style="list-style-type: none"> • Must provide a customer-focused specification of services to be delivered and performance requirements to be met • Include menu options, security capabilities, technical architecture, and capacity scalability • Approach ILMS to be the partner to define requirements, services, and customer oversight process
Cloud Computing Business Model	<ul style="list-style-type: none"> • Based on complete business plan for delivering cloud services to customers • Must include menu of service offerings, SLAs, pricing, and performance monitoring • Must include a customer engagement and support plan – addressing signing up new customers, communicating with existing customers, resolving problems, etc. • Must include an “exit plan” – addressing the transfer to a new vendor in case of contract expiration, loss of needed service levels, or best value to government.

Projects	Description
Cloud Initial Operational Capability (IOC)	<ul style="list-style-type: none"> • Complete ESOC development and virtualization • Initial group of major system sponsors operational on the ESOC • All domestic sites using cloud services • Full COOP service offerings • Linkage to outsourced resources for scalable capacity • Detailed schedule for bureau consolidation • Software, Platform and Infrastructure services
Public Cloud Clearinghouse	<ul style="list-style-type: none"> • Single point of contact for high volume enterprise-wide services • Explore cloud capabilities such as: <ul style="list-style-type: none"> ○ Google Apps ○ GSA Cloud Apps ○ Infrastructure as a Service ○ Virtual Private Cloud
IOC Evaluation	<ul style="list-style-type: none"> • Optimize customer experience • Plan and timeline for phasing in additional customers and services
Cloud Full Operational Capability (FOC)	<ul style="list-style-type: none"> • Software, Platform and Infrastructure services • Information stored across multiple clouds • Major application services in cloud

Goal 2.2 – Redesigned and consolidated network

Scope of Work:

The redesigned network is a key component supporting the other strategic goals especially Goal 2.1. As envisioned in the QDDR, the network must respond to the requirements of the diverse customer base, using a cost-sharing business model. This network will include State domestic bureaus and offices, overseas posts, and other agencies using the FAN. It will accommodate all security and IPv6 transition requirements, while providing maximum user flexibility, including ability to interact with external parties, U.S. citizens, and foreign publics.

The redesigned network will be engineered for the cloud environment, as shown in Figure 3, providing excellent worldwide network performance. The network must meet the following specifications/characteristics:

- **High Level of Connectedness** – The network must have a high degree of connectedness such that the failure of any one link does not disconnect a significant number of users.
- **High Degree of Flatness** – The end-to-end delay from any point on the network to the “Cloud” must be as consistent as possible with a low standard deviation.
- **Be Centrally Focused** – The cloud approach will allow two or more primary data centers, with the potential use of remotely deployed processing/storage nodes, to function as a single logical entity. The strategy of the Department of State is to move as much information into the cloud as possible thereby eliminating the need for regional solutions.
- **Be Information Sharing Focused** – The network is the backbone for the FAN and must facilitate secure cross-agency and cross-office information exchange. The network must enable the Foreign Affairs Community to bridge the silos of information which currently exist. The redesigned network should not be strictly a utility networking service (such as DTS/BRN) for other agencies.
- **Deliver Business Continuity Services** – In order to ensure maximum availability of applications, the data centers in the cloud require fail over routing, load balancing support, dynamic capacity, and other business continuity related support services.



Figure 3 Global Network

Key performance indicators for Goal 2.2 are:

- Network performance meets SLAs and provides excellent user experience for personnel anywhere in the world.
- Network meets application performance requirements using Concierge as a representative global application used by post and Washington users.
- Number of agencies using FAN and being billed via ICASS overseas.
- Redesigned infrastructure decreases the number and use of DINS.

Table 6 Goal 2.2 Major Projects

Projects	Description
Foreign Affairs Network (FAN) Requirements Analysis	<ul style="list-style-type: none"> • Must clarify how the new network will meet strategic cloud requirements • Must include minimum performance requirements • Must address DINS, cloud, mobile technology, cyber security, other agency and green requirements
FAN Business Model	<ul style="list-style-type: none"> • Must include SLAs, pricing, & customer roles • Must specify levels of service, determine extent of base offerings vs. fee for service • Communication plan showing service offerings, pricing, service levels, etc. • Define customer oversight process
FAN Design and Initial Operational Capability (IOC) Implementation	<ul style="list-style-type: none"> • Network design specifications must clearly indicate how requirements will be met and conform to technical architecture • Model network before implementation • Engage all customer groups to develop test and oversight plan and to validate against requirements • Implement redesigned network • Independently test and evaluate redesigned network and take corrective action if needed • Initial group of other agencies operational as FAN customers • Provision agencies – charge-back
IOC Evaluation	<ul style="list-style-type: none"> • Optimize customer experience • Evaluate end user experience quarterly • Document lessons learned and refine FAN offerings • Plan and timeline for phasing in additional customers and services
Full Operational Capability (FOC)	<ul style="list-style-type: none"> • Address lessons learned • Provision additional agencies



Goal 2.3 – An evolving suite of user-driven mobile technology and end-user services

Scope of Work:

End-user devices continue to become smaller, more mobile, while delivering enhanced functions and features. State users are currently making use of mobile phones, laptops, netbooks, and PDAs. Usage and demand will surely increase over the timeframe of this plan.

The focus of this sub-goal is to ensure that State personnel have 24/7 access to and can take full advantage of evolving mobile technology along with end-user services and applications delivered via the cloud. The plan calls for the establishment of an enterprise-based environment for delivering these devices and services, providing mobile versions of major corporate applications. IRM will engage end users to explore requirements and potential solutions, and to ensure that the devices and services offered are responsive. As depicted in Figure 5, IRM will rely on best practices, such as the iPhone App Store, to develop this goal. IRM will adapt existing technical solutions rather than develop “one off” custom solutions. The “apps” delivered under this goal will support the work of diplomacy and development officers, other agency requirements via the FAN, as well as administrative functions.

End users will have a single point of contact for computer equipment acquisition and maintenance, as well as for application downloads and access, network performance, security, etc. Users will be issued mobile devices that are theirs to keep as they move from job to job across bureaus and countries and as they continue to telework and telecommute.

All aspects of mobile computing must be taken into account –network capabilities, mobile devices, mobile applications, mobile access, data, etc.



Figure 4 Mobile Devices and Services

Key performance indicators for Goal 2.3 are:

- Blackberries and other mobile devices meet SLAs – i.e., they are delivered within two business days of request, work globally, and are tied to users instead of bureaus.
- At least one mobile application available for all overseas users.
- Virtualized desktops and thin clients available and in use by at least 10 percent of users.
- Increased use of telework and telecommuting as evidenced by numbers of mobile workers and amount of time spent out of the office while connected and productive.

Table 7 Goal 2.3 Major Projects

Projects	Description
End-User Infrastructure Provisioning Service	<ul style="list-style-type: none"> • Conduct independent analysis of GITM • Ensure GITM is driven by customer requirements and cloud computing needs • Provide on-line, self-service, menu-driven ordering • Explore options for maximum flexibility and outsourcing potential • Virtualize desktops and utilize thin clients
Mobile Computing Requirements Analysis and Implementation Plan	<ul style="list-style-type: none"> • Establish a mobile computing end users focus group to develop requirements • Develop CONOPS and initial offerings • Produce a plan for phasing in new devices, functions, and features • Explore and adapt best practices in the Intelligence Community for Classified Mobile Computing
Mobile Computing Initial Operating Capability (IOC)	<ul style="list-style-type: none"> • Establish technical architecture, framework, CONOPS tied to specific devices • IOC capabilities to include PASS e-services
IOC Evaluation	<ul style="list-style-type: none"> • Assess end-user experience and refine plan to reflect lessons learned • Establish requirements and measures of success for FOC
Implement Full Operating Capability (FOC) Mobile Computing	<ul style="list-style-type: none"> • Address lessons learned • Define additional FOC mobile capabilities to include self-service for personnel data, access to a wide variety of business applications



Goal 2.4 – Enhanced risk management, cyber security, and reduction of sensitive holdings

Scope of Work:

IT security governance and solutions must become increasingly swift and agile to support the Department's diplomacy and development mission, as spelled out in the QDDR, to accommodate the rapid changes in information technology. The Department must remain current with technology if it is to meet its global mission. Too often, new technology and solutions fall prey to cumbersome and outmoded processes and thinking adversely impacting national security. The Department is often so far behind on hardware and software versions that upgrades are forced when a company drops support for legacy versions. Failure to provide users with the requisite solutions only ensures that they will find other ways to do business thereby significantly increasing the risk to the Department as a whole. It is better to understand and manage risks as opposed to attempting to avoid them altogether. Slow adoption of technology has the same negative effects as a risk avoidance mentality.

This goal focuses on increasing the speed of technology adoption at State while increasing enterprise IT security. There are several key tenets of improving security outlined in the ITSP:

- Relocate sensitive information to safe zones inside of data processing centers.
- Provide enterprise-wide security services that are used by all major applications, relieving business owners of this responsibility, capturing economies of scale and ensuring consistent and high quality cyber security.
- Empower system and information owners to determine and accept risks, placing reasonability for balancing risks, costs, and benefits where it can most effectively be exercised.
- Streamline the adoption of new technology through effective risk management.
- Change the expectations for security experts and foster an environment, so they focus on identifying secure, practical solutions for accomplishing mission objectives, rather than highlighting reasons why something cannot be done.
- Streamline system acquisition by using pre-authorized solutions and using government-wide authorization processes via FedRAMP when security conditions permit.



IRM will build on the significant strides made by the Office of Information Assurance to streamline IT security through continuous monitoring and find ways of leveraging this approach and others to mitigate future risks as the Department rapidly introduces new technologies. The Department invested ARRA funds for a Cyber Security Initiative that will support its strategic IT and mission goals, focusing on the following:

- **Provide a standard process for training and certifying system and information owners to accept risk management responsibility.** This is crucial for accomplishing the goal of delegating risk management authority, streamlining the decision-making process, and ensuring that the correct tradeoffs are made.
- **Improve collaboration to ensure enterprise security services.** Cyber security responsibilities are distributed across many offices in various bureaus. This compartmentalization makes it possible to build expertise in each particular area but often impedes collaboration and integration of the appropriate cyber security controls.
- **Develop and implement a single enterprise identity management security service** that all applications can use. Business owners can choose how to apply the Identity, Credentialing, and Access Management (ICAM) service for single sign-on from minimally to maximally restrictive required to protect privacy information.
- **Provide standard security solutions to support a global virtual Desktop environment and remote access initiatives to ensure that sensitive data is protected.** This will be accomplished in collaboration with Goal 2.3, which focuses on mobile computing, end user devices, and includes providing virtualized desktops and thin clients.

Key performance indicators for Goal 2.4 are:

- Reduction in sensitive data holdings at post, both numbers of files and volume of data.
- Increasing use of single sign-on based on ICAM services, as evidenced by numbers of applications and numbers of users.
- Formal delegation of risk management authority to an increasing number of system and information owners who then accept responsibility for their own applications and data.
- Demonstrated reduction in time for approval and adoption of new technology, and availability of current or near-current versions of new technologies with X months of commercial availability.

Table 8 Goal 2.4 Major Projects

Projects	Description
Cyber Security Architecture	<ul style="list-style-type: none"> • Architecture to be driven by cloud computing and include a technical design that conforms to the Department-wide technical architecture • Ensure appropriate balance of functionality and security employing risk management • Security must address all mission requirements
Plan for reducing data holdings at post	<ul style="list-style-type: none"> • Develop categories of data holdings in terms of potential for elimination from post • Develop phased plan with definitive milestones for reducing data holdings • Provide dashboard to track progress and provide broad visibility
Identity, control and access management (ICAM) services	<ul style="list-style-type: none"> • Research best practices in identity control and access management and their relationship to cloud computing • Key milestones include implementation of single sign-on and timeline for retrofitting existing applications • Monitor progress of existing applications to use single sign-on and other ICAM services
Streamline ITCCB and related Configuration Management (CM) and security governance processes	<ul style="list-style-type: none"> • Reduce the significant time and effort required for even the simplest of changes • Delegate risk acceptance decision authority to business/information owners who are in the best position to judge the risks associated with their information • Business owners should be given wide latitude as long as risks to infrastructure are not significantly increased

Goal 2.5 – Green computing

Scope of Work:

This goal focuses on two aspects of green computing: (1) reducing the environmental impact of IT at State; and (2) using IT solutions to reduce the environmental impact of other State operations, for example, reducing energy consumption through intelligent building management software.

Efforts under this goal will begin with assessment of current energy consumption and impact on greenhouse gas and other harmful emissions. IT solutions will provide tools for data collection and monitoring, and for creating the assessments. Once the assessment phase is complete, short and long term plans will be developed in conjunction with other applicable agencies and bureaus such as A, OBO and GSA. We envision that IT solutions will come into play once implementation begins, to track and report progress via dashboards.

Preliminary key performance indicators for Goal 2.5 are:

- ESOCs receive LEED certification.
- Demonstrated reduction in energy consumption due to IT.
- Achievement of additional performance measures outlined in the Department’s Green IT plan (Agency Sustainability Plan).

Table 9 - Goal 2.5 Major Projects

Projects	Description
Green Technologies Design Specifications	<ul style="list-style-type: none"> • Implement Portfolio of Green Technologies • Obtain LEED Certifications for computer centers (ESOC East, ESOC West, Old War, Beltsville)
Baseline and monitor energy consumption	<ul style="list-style-type: none"> • Monitor and publish Greenhouse Gas Metrics & energy consumption measures



Goal 3: State's IT Leadership

This goal ensures effective governance of all IT resources, domestic and overseas, and focuses on accountability to our customers for excellence and service delivery. The QDDR stresses the importance of improved performance management by expanding training and streamlining performance evaluation process. It includes three sub-goals.

Goal 3.1 – Governance

Scope of Work:

This goal will take State's IT governance processes to the next level, introducing greater customer involvement and oversight, greater coordination of IT initiatives to reflect strategic priorities, and multi-year investment planning and budgeting. It advocates effective release and deployment management to minimize risks associated with adjustments to the infrastructure than can result in instability, loss or corruption of data, loss of network or access to systems and applications, and "downtime" or similar system interruptions. This goal is the responsibility of the eGov Program Management Office, working on behalf of the Under Secretary for Management, CIO, and eGov Program Board, and follows the Federal CIO IT Management Reform Program.

Key performance indicators for Goal 3.1 are:

- Evidence of increased use and value of enterprise architecture products and services in producing consistent and effective IT solutions, promoting interoperability, information sharing, and collaboration.
- Reduced software and maintenance costs due to improved enterprise licensing, disciplined life cycle management, and prompt phase-out of legacy systems.
- All applications capable of working at all posts and fully tested prior to implementation to ensure that all functional and performance requirements are met, as evidenced by decreasing numbers of trouble tickets and complaints.

Table 10 Goal 3.1 Major Projects

Projects	Descriptions
Customer Oversight Board	<ul style="list-style-type: none"> • Promote active engagement by customers within State and outside (FAN users) • Enlist a customer champion to chair the Board • ICASS–like Board for WCF • Distinguish core infrastructure from discretionary • Measure effectiveness of the Board
Multi-year investment plan	<ul style="list-style-type: none"> • Reflect full life cycle costs including “tail costs” and fee based for extra resources (aka “fee for burst.”) • Include impact on existing operations, explicitly noting phase-out of legacy systems • CIO review and possible deferral of funding for projects not meeting performance goals • Align CPIC, budget formulation and budget execution processes
Global Application Development Master Schedule	<ul style="list-style-type: none"> • Coordinate with major system developers inside and outside IRM • Consider impact of development schedule on strategic goals and priorities, key processes (ITCCB, C&A, capital planning), IV&V, acceptance testing and change management • Include a plan and process to coordinate global application deployments
Enterprise Architecture Planning	<ul style="list-style-type: none"> • Focus on interoperability and application services • Limit EA products to those that provide value to system sponsors and developers • Engage EA customers to ensure that products are useful and effective • Monitor use and perceived value, and continue to refine the process as a result
Next generation enterprise license management	<ul style="list-style-type: none"> • Explore and negotiate innovative business arrangements, reflecting cloud-based software use • Consider impact on the FAN and other agency participation • Mandatory use of enterprise licensing

Goal 3.2 – Performance Management

Scope of Work:

This goal will provide a framework and process for performance management across all IT projects and services. It will institute guidance and criteria for metrics and measures that can be used by individual project sponsors and managers. This goal will also provide a dashboard tool for displaying consistent, relevant, and dynamic information for management at all levels to ensure visibility and accountability.

Key performance indicators for Goal 3.2 are:

- Increase in mission-oriented outcome measures for IT investments.
- All infrastructure services have published service levels and are measured regularly – real time status and trends of all services displayed on a customer facing dashboard.
- Evidence of management attention to performance measurement and satisfaction with dashboard information, evidenced by increasing numbers of management users and volume of inquiries about dashboard data.

Table 11 Goal 3.2 Major Projects

Project	Description
Institutionalize performance measurement framework	<ul style="list-style-type: none"> • Must reflect best practices in metrics and measurement • Small number of critical indicators for each project, ensuring a focus on high priority factors • Ensure the feasibility of capturing relevant and reliable measures; ideally measurement data will come directly from operational systems
Project Tracking Dashboard	<ul style="list-style-type: none"> • Cloud-based tool capable presenting data from IT investment projects and systems • Monthly reviews with the CIO and quarterly reviews with the eGov PB to review key metrics on selected projects
Training Program	<ul style="list-style-type: none"> • Implement FSI programs for training and support of performance, governance, and change management • Clear and measurable training objectives

Goal 3.3 – Workforce Management and Training

Scope of Work:

The IT Strategic Plan will result in profound changes in demand for technical and user support, and thus in the roles and skills of IT staff. IMOs report that changes are already under way as personnel become increasingly dependent on mobile computing and 24/7 availability of IT systems. The future will bring even more dramatic and rapid change, and State's workforce must be ready to adapt. The FSI School of Applied Information Technology (SAIT) curriculum committee is currently reviewing all existing IT curriculum for all IT specialists to adapt it to changing technology.

To respond to these changes, IRM, HR, and FSI will develop multi-year plans for attract, develop and sustain a properly skilled IT workforce needed to carry out the ITSP. This goal will also address training for end users to ensure they can maximize the value they receive from the IT capabilities to be deployed.

Key performance indicators for Goal 3.3 are:

- Percentage of non-IT personnel demonstrating proficiency in key technologies.
- FSI's IT course content is updated rapidly and appropriate training is always available before new technology is introduced; designated IT support personnel demonstrate proficiency in new technology prior to implementation.
- Numbers of IT personnel re-trained and reassigned to reflect changed demand resulting from ITSP goals.

Table 12 Goal 3.3 Major Projects

Projects	Description
Multi-year IT workforce plan	<ul style="list-style-type: none"> • Consider models and what-if scenarios to determine future requirements and then map existing positions and employees to them • Plan must address transition from the current workforce
Multi-year IT training plan	<ul style="list-style-type: none"> • Based on skills and competencies needed by IT and non-IT staff to enable effective technology use • Continue to explore best practices in training technologies and approaches • Training plans must identify investments needed, measures of success, and processes for testing to ensure competence



NEXT STEPS

The next steps in the tactical planning process are:

- Approval by the eGov Program Board.
- Publish initial version of the ITTP online and begin official execution and monitoring.
- Engage champions and specify pilot projects to ensure quick results -- within three to six months.
- Complete the project templates and identify necessary project adjustments.
- Create resource plans for all required investments and projects, and indicate any resource shifts needed.
- Establish performance dashboards.



Acronyms

BMP	Office of Business Management and Planning
BPR	Business Process Engineering
BRN	Black Router Network
C&A	Certification and Accreditation
CIO	Chief Information Officer
CM	Configuration Management
CONOPS	Concept of Operations
COOP	Continuity of Operations
DINS	Direct Internet Services
DTS	Diplomatic Telecommunications Service
eDIP	Office of e-Diplomacy
EDW	Enterprise Data Warehouse
e-Gov PMO	e-Government Program Management Office
e-GovPB	e-Government Program Board
ENM	Office of Enterprise Network Management
ESB	Enterprise Service Bus
ESOC	Enterprise Server Operations Center
ESOC	Enterprise Server Operations Center
FAN	Foreign Affairs Network
FedRAMP	Federal Risk and Authorization Management Program
FOC	Full Operational Capability
FSI	Foreign Service Institute
GITM	Global Information Technology Modernization
GSA	General Services Administration
HR	Bureau of Human Resources
IA	Division of Information Assurance
ICAM	Identity Control and Access Management
ICASS	Integrated Cooperative Administrative Support Service
IIP	International Information Programs (Bureau of International Programs)
ILMS	Integrated Logistics Management System
IMO	Information Management Officer
IOC	Initial Operational Capability
IPMS	Integrated Personnel Management System
IRM	Bureau of Information Resource Management
IT	Information Technology
ITCCB	Information Technology Configuration Control Board



ITI	Office of Information Technology Infrastructure
IV&V	Independent Verification and Validation
KPI	Key Performance Indicators
LEED	Leadership in Energy and Environmental Design
NGO	Non-Governmental Organization
OPS	Office of Operations
PASS	Post Administrative Software Suite (Concierge)
PDA	Personal Digital Assistant
QDDR	Quadrennial Diplomacy and Development Review
SLA	Service Level Agreement
SPO	Strategic Planning Office
VPC	Virtual Private Cloud
WBS	Work Breakdown Structure
WCF	Working Capital Fund