

Archived Information



U. S. Department of Education
Office of the Chief Information Officer

Information Resources Management (IRM)
Strategic Plan
FY2012 – 2015

May 2012

Version 2.0



Contents

<i>Purpose</i>	3
1 Introduction	3
2 IRM Goals	4
3 Goal One: Portfolio Alignment.....	5
3.1 Department Alignment	5
3.1.1 Department Strategic Plan.....	6
3.1.2 Segment Architecture	8
3.2 Federal Alignment.....	11
3.2.1 Open Government Directive	11
3.2.2 Customer Service	12
3.2.3 Cloud Computing	12
3.2.4 Data Center Consolidation	13
3.2.5 Homeland Security Presidential Directive (HSPD) 12	14
3.2.6 Trusted Internet Connection (TIC)	15
3.2.7 Internet Protocol Version 6 (IPv6)	16
3.2.8 Electronic Stewardship.....	16
4 Goal Two: Technology Services.....	17
4.1 Current Services.....	17
4.2 Future Services.....	18
4.2.1 Enhanced Services.....	19
4.2.2 OCIO Support Services	30
4.3 Management Structure for Future Services	32
5 Goal Three: Information and Technology Management	34
5.1 IT Governance Structure	34
5.1.1 Enterprise Architecture (EA) Program Office.....	35
5.1.2 Investment and Acquisition Management Team (IAMT).....	35
5.2 Key Department Contributors to the IRM Governance Process.....	35
5.2.1 IT Acquisition (Procurement)	35
5.2.2 Regulatory Information Management	36
5.2.3 Information Assurance Services (IAS)	36
5.2.4 Information Technology Services (ITS).....	37
5.2.5 Human Resources Management.....	38
6 List of Figures	39
7 List of Tables	39



Purpose

This purpose of this document is to describe how information technology (IT) will be acquired and managed within the U.S. Department of Education (The Department) to support the achievement of the strategic plan goals. There are five sections that discuss different aspects of implementing and managing information technology resources. These 5 sections are as follows:

Section 1 is the Introduction, which specifies the Chief Information Officer's objectives and planning horizon of the IRM Strategic Plan. The Introduction also provides an overview of the external policies incorporated in the Department's IRM Strategic Plan.

Section 2 identifies the strategic goals set by the CIO to achieve the Department's technology objectives.

Section 3 of the IRM Strategic Plan discusses Goal One: The Department's IT portfolio alignment. This section discusses how the portfolio is aligned to meet the Department's business mission and to Federal IT initiatives.

Section 4 of the IRM Strategic Plan discusses Goal Two: OCIO's technology services. This section describes the current technology services offered at the Department, along with future technologies that will meet the Department's growing business requirements.

Section 5 of the IRM Strategic Plan discusses Goal Three: IT management. This section identifies the key stakeholders and provides an overview of what they manage and contribute to the information resource management process.

1 Introduction

The Chief Information Officer at the Department has primary responsibility to ensure that IT is acquired and information resources are managed in a manner consistent with statutory, regulatory, and Departmental requirements and priorities. The CIO provides management advice and assistance to the Secretary of Education and to other senior staff on information resources investment and operations. The CIO also promotes a shared corporate vision about the Department's information activities and provides services to effectively manage information and to provide value-added enterprise-wide systems and infrastructure.

This Department Information Resources Management Strategic Plan for FY 2012 - 2015 describes:

- The relationship between the IT vision and the enterprise business goals and performance objectives
- The set of value-added IT services delivered or planned to be delivered
- The set of IT management processes and plans for ensuring the effective use of IT resources across the Department

While the IRM Strategic Plan serves as the strategic document for the Office of the Chief Information Officer (OCIO), it is built from other more detailed strategic, operational and tactical plans of each information management element throughout the Department, ranging from enterprise architecture to E-Government. The IRM Strategic Plan describes what will be implemented over the planning horizon, while the other strategic, operational and tactical plans describe how these goals will be accomplished. Together, these plans allow the OCIO to ensure that IT activities are aligned with and supportive of the Department's mission and strategic goals.



In addition, the Department recognizes the need to integrate external policies and directions as defined by Congress and the Administration into its IRM Strategic Plan. As such, the Department's IRM Strategic Plan responds to:

- Federal Information Security Management Act (FISMA),
- Office of Management and Budget (OMB) Circular A-130,
- Government Performance Results Act of 1993,
- Clinger-Cohen Act of 1996,
- E-Government Act of 2002,
- Office of Management and Budget (OMB) Memorandum for Federal Data Center Consolidation Initiative February 2010,
- 25 Point Implementation Plan to Reform Federal Information Technology Management of December 2010, and the
- Federal Enterprise Architecture.

This document is the Department's IRM Strategic Plan. OMB Circular A-130 describes the IRM Strategic Plan as a management tool that is "strategic in nature and addresses all information resources management activities of the agency." The CIO is responsible for developing and maintaining the document as required by the OMB Circular A-11, Section 53, requires that the IRM Strategic Plan be submitted together with the Department's IT budget request.

2 IRM Goals

The CIO's objective is to support the Department's mission through effective management of value-adding technologies. The IRM Strategic Plan describes the technology strategic goals to achieve the CIO's objective.

The three goals defined in the IRM Strategic Plan are:

Portfolio Alignment – Ensure that the IT investment portfolio supports the Department's business mission and performance objectives.

Technology Services – Orient OCIO as a provider of enterprise common services in addition to basic infrastructure services.

Information and Technology Management – Ensure effectiveness of IT governance, data and information processing capabilities and technology utilization across the enterprise.



Figure 1: IRM Strategic Plan Goals



3 Goal One: Portfolio Alignment

Goal One of the Department's IRM Strategy is to ensure the IT investment portfolio supports the Department's business mission. The IT portfolio objective is to accomplish:

- Alignment to Departmental Business Mission
- Alignment to Federal IT initiatives

The IRM Strategic Plan describes how the Department's technology investments are managed to support the business mission and performance objectives of the Department's program offices, and to respond to Federal IT initiatives.

3.1 Department Alignment

The Department's IRM Strategic Plan is designed to demonstrate how the Department's information resources are aligned to support achievement of the Department's business.

The Department's Enterprise Architecture (EA) Program Office developed a Segment Architecture approach to align the IT portfolio to the Departmental strategic goals.



3.1.1 Department Strategic Plan

The OCIO’s technology goals are to support the achievement of the Department mission and strategic performance goals and objectives for 2012 – 2015.

The Department of Education’s mission is:

Department of Education Mission
“To promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.”

The Department’s Strategic Plan 2012-2016¹ embodies six Department of Education strategic goals:

Table 1: Department of Education Strategic Goals

Goal One:	K-12: Prepare K-12 students for college and career by improving the education system’s ability to consistently deliver excellent classroom instruction and supportive services
Goal Two:	Higher Education, Career-Technical Education, and Adult Education: Increase college access, quality, and completion by strengthening higher education and lifelong learning opportunities for youth and adults
Goal Three:	Early Learning: Improve the health, social-emotional, and cognitive outcomes for all children from birth through third grade, especially those with high needs
Goal Four:	Capacity for Systemic Continuous Improvement: Enhance the education system’s ability to continually improve through better and more widespread comprehension and use of data, research and evaluation, transparency, innovation, and technology
Goal Five:	Equity: Ensure effective educational opportunities for all students regardless of race, national origin, gender, disability, language, sexual orientation, and socioeconomic status
Goal Six:	Department Capacity: Improve the organizational capacities of the Department to implement the Strategic Plan

¹ U.S. Department of Education Strategic Plan 2012-2016



The Department’s Strategic Goals are articulated through Strategic Objectives. The Department’s Strategic Objectives are depicted below in Table 2:

Table 2: Department of Education Strategic Goals and Strategic Objectives²

Strategic Goals	Strategic Objectives
Goal One: K-12: Prepare K-12 students for college and career by improving the education system’s ability to consistently deliver excellent classroom instruction and supportive services	1.1 Support state-led effort to develop and adopt college-and career-ready standards that are internationally benchmarked and aligned to valid and reliable assessments 1.2 Improve the preparation, recruitment, development, evaluation, and rewarding of effective teachers, principals, and administrators 1.3 Increase the success, safety, and health of students in high-need schools and communities 1.4 Support states and districts in turning around 5,000 of the nation’s persistently lowest-achieving schools 1.5 Increase competence in science, technology, engineering, and mathematics (STEM) for all and prepare the next generation for careers in STEM-related fields
Goal Two: Higher Education, Career-Technical Education, and Adult Education: Increase college access, quality, and completion by strengthening higher education and lifelong learning opportunities for youth and adults	2.1 Close the opportunity gap by improving the affordability of and increasing access to college and workforce training, especially for adult learners, low-income students, underrepresented minorities, and other chronically underserved populations 2.2 Foster institutional quality to ensure that completers have attained an educational credential that demonstrates that they are prepared to excel in a global society and economy, accountability, and transparency 2.3 Increase degree and certificate completion and job placement, with special attention to underrepresented and economically disadvantaged populations
Goal Three: Early Learning: Improve the health, social-emotional, and cognitive outcomes for all children from birth through third grade, especially those with high needs	3.1 Increase access to high-quality learning programs and comprehensive services, especially for children at risk of school failure 3.2 Improve the quality and effectiveness of the early learning workforce so that early learning professionals have the skills and abilities necessary to improve young children’s health, social-emotional, and cognitive outcomes 3.3 Improve the capability of states and early learning programs to develop and implement comprehensive early learning assessment systems, whose data are used to improve student outcomes and to ensure programs are monitored for effectiveness
Goal Four: Capacity for Systemic Continuous Improvement: Enhance the education system’s ability to continually improve through better and more widespread comprehension and use of data, research and evaluation, transparency, innovation, and technology	4.1 Facilitate development of interoperable data systems from early learning through postsecondary education and the workforce that will enable data-driven decisions making by increasing comprehension of and access to timely, reliable, and high-value data 4.2 Connect research and evaluation with policy and practice to support education improvement and Department decision making 4.3 Present relevant and accessible information that increases the demand for high-quality education services and attainment and improves education performance, while maintaining student privacy 4.4 Accelerate the development and broad adoption of innovative programs, processes, and strategies, including education technology

² U.S. Department of Education Strategic Plan 2012-2016



Strategic Goals	Strategic Objectives
Goal Five: Equity: Ensure effective educational opportunities for all students regardless of race, national origin, gender, disability, language, sexual orientation, and socioeconomic status	
Goal Six: Department Capacity: Improve the organizational capacities of the Department to implement the Strategic Plan	6.1 Continue to build a high-performing, skilled workforce within the Department 6.2 Improve Department’s program efficacy through comprehensive risk management and grant monitoring 6.3 Build Department capacity to support states on reform implementation and achievement of improved outcomes for students 6.4 Improve workforce productivity through information technology and performance management systems

Source: U.S. Department of Education Strategic Plan 2012-2016

3.1.2 Segment Architecture

The Department authorized the EA Program Office to develop Segment Architectures to carry out the Department’s Strategic Plan.

The EA Program Office, in accordance with the Federal Enterprise Architecture (FEA) practice guidance, identified business units that support common missions and that provide common services. These business units are then grouped into categories by how they address the various business and technology needs of the program and principal offices across the Department: core mission, business service, and enterprise services. As a result of the identification and development process, the EA Program Office described the Department’s business using the following 13 segments:

Table 3: The Department’s 13 Segments

Segment Name	Segment Definition	Segment Category
Budget Formulation & Execution	Enable the Department’s budget personnel to reduce manual processes and improve budget formulation and execution efficiency and data accuracy	Business Service
Compliance	Assurance that policies mandated by the Department and by Federal law are being carried out	Core Mission
Evaluation & Policy Analysis	Assessment of the Department’s programs and related policies for meeting national education objectives	Core Mission
Facilities Management	Track assets and the provision of services related to those assets, to include the operation of office buildings, space planning, and other capital assets that are possessions of the Department	Enterprise Service
Financial Management	Deliver responsible financial management capabilities, including centralized data, increased access, electronic record keeping, and improved reporting	Business Service
Grants	Review, award, and disbursement of formula and discretionary grants through the various program offices	Core Mission
Human Capital Management	Improve the strategic management of the department’s human capital	Business Service
Information Assurance	To build and enable mutual trust needed to support widespread use of electronic identity authentication interactions between the public and the government	Enterprise Service
Information Dissemination	Distribution of education information products through multiple channels and formats	Core Mission
IT Infrastructure	Improve customer service and reduce the Department’s operational risks by improving performance, providing a common technology platform for business applications, and facilitating better information management	Enterprise Service



Segment Name	Segment Definition	Segment Category
IT Management	Facilitate the interagency-wide governance of information resources, to include the practices of enterprise architecture, and capital planning and investment control	Enterprise Service
Loans	Management and delivery of federally funded or federally guaranteed financial assistance for post-secondary education	Core Mission
Research	Research and statistical analysis on the condition of education in the U.S.	Core Mission

Next, the EA Program Office worked with the Segments to establish business purpose and goals that align the Segments’ business to the Department’s mission. The alignments between the Segment Architectures to the Department Strategic Goals are shown below:

Figure 2: Segment Alignment to Department Strategic Goals

Lines of Business (LoB)	Goal 1: K-12	Goal 2: Higher Education, Career-Technical Education, and Adult Education	Goal 3: Early Learning	Goal 4: Capacity for Systemic Continuous Improvement	Goal 5: Equity	Goal 6: Department Capacity
Budget Formulation & Execution						●
Compliance	●	●			●	●
Evaluation & Policy Analysis	●	●	●	●	●	●
Facilities Management						●
Financial Management						●
Grants	●	●	●	●	●	●
Human Capital Management						●
Information Assurance				●		●
Information Dissemination				●		●
IT Infrastructure				●		●
IT Management				●		●
Loans		●				●
Research				●		●

Segments have not submitted Modernization Plans aligning to the 2012-2016 Departmental Strategic Goals. This diagram represents EA’s projection of the Segment Alignment.

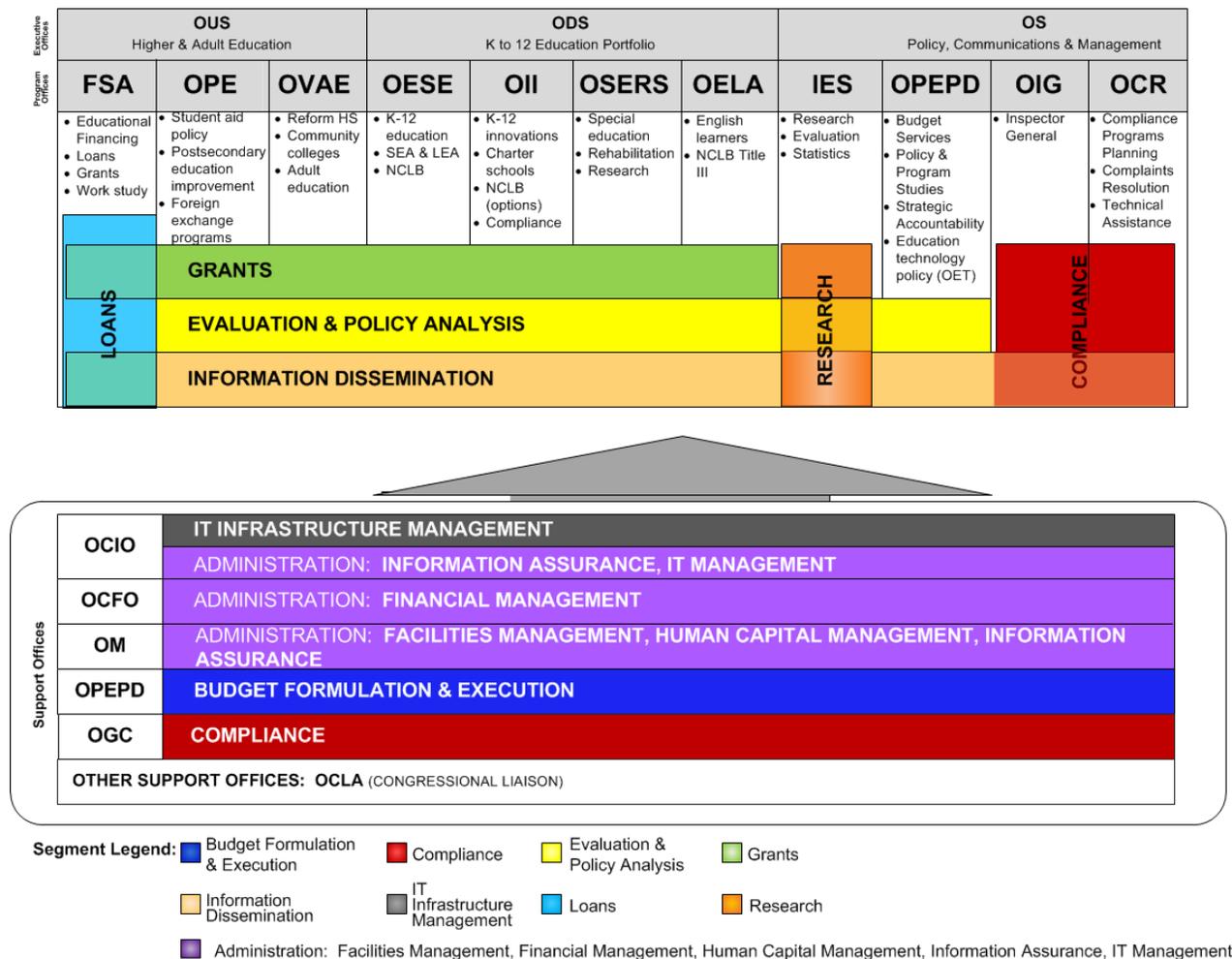


Figure 2 illustrates the alignment between the Segments and the Department’s Strategic Goals. Aligning the Segments to the Department mission sets the direction of the Segments’ business and investment decisions.

The investments in the Department’s IT portfolio are developed to improve the business of the program offices they support.

Figure 3 provides a visual representation of principal offices and their engagement with the Department’s 13 Segments.

Figure 3: Principal Office and Segment Engagement



The segment architecture approach is expected to improve the Department’s performance and help identify ways to reduce cost by aligning business processes and investment activities while eliminating unnecessary duplication of processes, investments and technologies.



3.2 Federal Alignment

The Department's goal to align its portfolio also includes alignment to Federal technology missions.

By implementing the following initiatives in compliance with government-wide mandates, the IT portfolio will support the Federal government's technology direction:

- Open Government
- Data.gov
- Customer Service
- Cloud Computing
- Data Center Consolidation
- Homeland Security Presidential Directive (HSPD) 12
- Trusted Internet Connection (TIC)
- Internet Protocol version 6 (IPv6)
- Electronic Stewardship

3.2.1 Open Government Directive

The December 2009 Open Government directive set an unprecedented standard for openness in government. Open Government practices became an even more prominent priority at the Department with the issuance of the President's Open Government directive, Transparency and Open Government, on January 21, 2009.

The overall mission of the directive is to establish greater transparency, collaboration and participation between Federal agencies and the public. The goals of Open Government are to:

Goal 1: Increase the Department's transparency and accountability.

Goal 2: Solicit and incorporate more public input into Department operations.

Goal 3: Increase collaboration and communication with other organizations.

Goal 4: Create a culture of openness within the Department.

The Department will take the following steps to achieve the Open Government Goals:

- Publish government information online
- Improve the quality of government information
- Create and institutionalize a culture of Open Government
- Create an enabling policy framework for Open Government

The Department has already developed an Open Government Plan that promotes open government practices with standards and procedures to ensure that these principles are adopted across the agency. The Department and the OCIO will continue to coordinate open government implementation to ensure alignment with the Department's strategic plan and technology investments.

The [Department's Open Government Plan](#) will strive to give the American people a transparent, participatory, and collaborative Department that works for and with the public to improve education in this nation.



3.2.1.1 Data.gov

As part of the [Open Government Initiative](#), Data.gov shares the Open Government initiative's goals to increase agencies transparency and accountability with the public by providing improved access and usability of Federal data.

Additionally in FY2012, OMB, General Services Administration, the Department and other federal agencies with education-related data (e.g., National Science Foundation, National Aeronautics and Space Administration, Veterans Affairs, U.S. Department of Agriculture, U.S. Department of State), launched the Data.gov Education Community at <http://education.data.gov>. This website showcases education-related datasets, challenges, mobile and web applications and other interests to the community.

Data.gov and Data.ED.gov are user-friendly platforms with a searchable data catalog that makes more data and information available to the public and also provides regular updates to project maps, dated milestones, and financial data regarding Open Government and other key initiatives. These Data.gov programs provide the public with an increased access to high value, machine readable datasets so that the public can easily find, download, and use information generated by the Department.

3.2.2 Customer Service

The Department's Customer Service Plan is designed to improve the delivery of services to our customers by redesigning the business processes and systems that impact key customer interactions, including increasing online services and user friendly services. The Customer Service Plan also addresses the [Executive Order 13571 – Streamlining Service Delivery and Improving Customer Service](#) to improve the quality of service the Federal government provides to the public, private entities, and intra-governmental agencies.

The [Department's Customer Service Plan FY 2012](#) outlines ED's efforts to improve customer relationships and the customer experience by delivering faster and better services to the public while reducing costs.

3.2.3 Cloud Computing

The February 2011 Cloud Computing Initiative and the Federal Cloud Computing Strategy require all Federal agencies to shift to a "Cloud First" policy. The goal is to become a more reliable, efficient, and innovative Government.

The Department of Education is currently undergoing efforts to adopt cloud computing technologies whenever a secure, reliable, cost-effective cloud option exists in compliance with the following guidance and regulations:



- 25-point Implementation Plan to Reform Federal Information Technology Management (Federal CIO Vivek Kundra) December 9, 2010
- Federal Chief Information Officers Council (FCIOC) Privacy Committee, *Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies*, August 2010
- Federal Information Security Management Act (FISMA) of 2012, Public Law 104-347
- NARA Bulletin 2010-05, *Guidance on Managing Records in Cloud Computing Environments*
- NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011
- NIST SP 800-145, *A NIST Definition of Cloud Computing*, September 2011
- NIST SP 800-146, *DRAFT Cloud Computing Synopsis and Recommendations*, May 12, 2011
- OMB Circular A-130
- The Cloud Computing Act of 2011 (Federal CIO Steven Van Roekel)
- The Federal Risk and Authorization Management Program (FedRAMP)
- Department of Education Cloud Computing Security Guidance, DRAFT, January 18, 2012

Please see Section 4.2.1.2.1 for more information on the Department's cloud computing activities.

3.2.4 Data Center Consolidation

The 2010 Federal Data Center Consolidation Initiative (FDCCI) called for a government-wide effort to consolidate federal data centers with goals to:

- Promote the use of Green IT
- Reduce Federal costs
- Improve IT security posture
- Shift Federal computing to more efficient technologies

The Department of Education is on track with its data center consolidation progress and has completed an inventory of its data centers and related assets and developed consolidation plans with a technical roadmap and clear consolidation targets.

Through data center consolidation, the Department aims to reduce its energy consumption, reduce operational costs, strengthen its IT security, and move toward employing innovative and efficient technologies.

Please see Section 4.2.1.2.2 for more information on the Department's data center consolidation activities.



3.2.5 Homeland Security Presidential Directive (HSPD) 12

The Federal Government established the 2004 mandate for Homeland Security Presidential Directive (HSPD) 12 - Policies for a Common Identification Standard for Federal Employees and Contractors requiring a government-wide standard for secure and reliable forms of identification.

To meet the physical and logical access requirements of HSPD-12, the Department's top HSPD-12 agenda items are identity management, access control, and two factor authentication. The Department of Education's goals in the department-wide integration of HSPD-12 are to reduce identity fraud, protect personal privacy, enhance security, and increase efficiency.

Please see Section 4.2.1.2.3 for more information on the Department's HSPD-12 activities.

3.2.5.1 Identity Management

The Federal government is moving toward the idea of sharing credentials across multiple agencies and allowing citizens to use non-government credentials to conduct business with the government online. The Department has been a participant in the identity management initiative, which is part of the E-Government agenda outlined by the President's Management Council.

Identity management provides the capability for the Department's customers to use identity credentials other than those currently provided by the Department of Education, such as those from the top five identity providers: (1) banks, (2) universities, (3) Internet service providers, (4) merchants, and (5) employers.

The Department's identity management program seeks to provide identity credentials to the Department's customers while strengthening security, reducing inconvenience, and minimizing the cost of identity management.

The Department's approach to implementing identity management is to build a solid infrastructure that supports shared authentication services across multiple applications. The first building block is the Security Architecture infrastructure that includes identity and access management (IBM Tivoli Access Manager and Identity Manager suite of products). The Security Architecture provides tools, technologies, and policies for identity and access management across the Department. The goal is to provide consistent access control, authorization and auditing for applications that integrate with this infrastructure. Once the Security Architecture is developed and deployed, the Identity Management infrastructure can be layered on top of it and deployed to any application already in the Security Architecture.

3.2.5.2 Department ID and Access Control Implementation

To meet the requirement of HSPD-12, the Department's Office of Management Security Services provides policy to Department facilities in how to manage the vetting and credentialing of individuals requiring access to agency information systems and facilities. Having consistent policies in place will reduce vulnerabilities to the Department's physical and logical assets and allows.

The Department's HSPD-12 solution, the ID Card and Access Control System, is currently in place and is used by employees and contractors at the Department's headquarters and regional locations. All of these systems are networked to form one system.



The ID Card and Access Control System also provides complete access control and alarm monitoring for sites, including the following additional features:

- Access Control
- Security
- Point Monitoring
- Elevator Control
- Photo ID Badges
- Guard Tour
- Key Tracking
- Image Recall with Historic and User Accountability Reporting
- Live CCTV display/control
- Interface with Paging, CCTV, Parking, Central Station Automated Alarm Systems, HVAC, and Elevator Control Systems

The Department maintains privately leased, GSA owned, or GSA leased facilities, all of which have staggered lease renewal dates. As facility leases expire, the determination of whether to relocate or to extend the present lease will be determined. Security systems for all locations must be 100% compatible with the existing systems for proper monitoring and access control.

3.2.5.3 Two Factor Authentication

To improve the security and protect the assets of the Department, all employees and contractors are required to access authorized ED systems using two factor authentication. Two factor authentication requires two authentication methods to access a system. At the Department, users are required to use their PIV-enabled identification badge and a Personal Identification Number (PIN) for access to the Department's network.

3.2.6 Trusted Internet Connection (TIC)

The Trusted Internet Connection (TIC) Initiative derives from the National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 and is the first of 12 initiatives in the President's Comprehensive National Cybersecurity Initiative (CNCI). The TIC Initiative aims to optimize and standardize the security of the Federal government's network connections.

The Department's TIC implementation will comply with the following OMB Memoranda:

- OMB M-08-05: Implementation of Trusted Internet Connections
- OMB M-08-16: Guidance for Trusted Internet Connection Statement of Capability Form
- OMB M-08-26: Transition from FTS2001 to NETWORKX
- OMB M-08-27: Guidance for Trusted Internet Connection Compliance
- OMB M-09-32: Update on the Trusted Internet Connections Initiative

Please see Section 4.2.1.2.4 for more information on the Department's TIC activities.



3.2.7 Internet Protocol Version 6 (IPv6)

The Internet protocols specify communication and interoperability rules on the Internet and on other IP networks, including addressing schemes. Internet Protocol version 4 (IPv4) is most widely used in current Federal network environments. With the exponential increase in demand across the global Internet community, IPv4's address space is nearing depletion, underscoring the need to transition to IPv6, which offers a larger Internet address space. The OMB Memorandum M-05-22 mandates Federal agencies enable Internet Protocol version 6 (IPv6) within their current IPv4 networks.

On September 28, 2010, the Federal CIO issued a memo instructing all agencies to transition to native IPv6 according to the following schedule:

- Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012.
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014.
- Designate an IPv6 Transition Manager to serve as the person responsible for leading the agency's IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary.
- Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.

ED has developed a Departmental IPv6 Transition Guide, which describes the Department's policies and activities to meet the Federal IPv6 requirements. The IPv6 Transition Manager and IPv6 Working Group are making steady progress in meeting IPv6 milestones, which include the FY2012 external application compliance and FY2014 internal application compliance milestones.

Please see Section 4.2.1.2.5 for more information on the Department's IPv6 transition activities.

3.2.8 Electronic Stewardship

In support of Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance, the Department will continue to serve as an active member on the Federal Electronic Stewardship Working Group (FESWG) and other interagency related activities, including the Federal Electronics Challenge. The executive order, released in October 2009, includes the following areas associated with IT electronic stewardship that the Department will continue to implement and address throughout the acquisition, operations and end-of-life management lifecycle:

- Establish and implement policies to enable power management, duplex printing and other energy efficient or environmentally preferable features
- Use environmentally sound disposal practices for excess or surplus electronic products
- Implement best practices in energy-efficient management of servers and data centers

The Department's Strategic Sustainability Performance Plan will outline our Electronic Stewardship programs and will comply with the following guidance:

- Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance
- Executive Order 13423, Strengthening Federal Environmental, Energy, and Transportation Management



4 Goal Two: Technology Services

The OCIO provides a broad range of information technology services to address the current and future business needs of the Department. The OCIO is committed to modernizing the Department with innovative technology that will provide future cost and performance improvements in meeting the agency mission and strategic goals.

The OCIO’s goal includes delivery of common IT services supporting the Department’s core technical infrastructure as well as future delivery of new and enhanced services to further enable the Department’s business modernization.

The OCIO will enable program offices to better focus on their mission competencies by providing a robust enterprise platform with technology services that:

- **Improve performance** by providing a highly capable communications and computing infrastructure
- **Improve efficiency** with interoperable technologies that can link work across independent tools that can reduce staff needs
- **Reduce costs** for IT service delivery by standardizing software and hardware platforms

The OCIO will ensure that the implementation and management of the Department’s technology services support the Department’s mission and strategic performance goals as well as Federal policies and initiatives indicated in Goal One.

4.1 Current Services

The OCIO’s role is to provide a stable technology infrastructure to support the business requirements of the Department. The OCIO’s goal is to continue providing IT services that support the deployment, operations, and maintenance of the Department’s core technical infrastructure while seeking to improve operational and cost performance.

The OCIO will continue the delivery of common IT resources, such as hardware, software, networks, and other services that support program offices business needs. The OCIO will continue delivery of the following supportive technologies during the current IRM Strategic Plan:

Table 4: Current Delivery of Services

Hardware
Assistive technologies
Hardware infrastructure maintenance and upgrade

Software
Assistive technologies
Data Management
Desktop Operating System – Upgrade to Windows 7
Email, Messaging, and Collaboration
Office Productivity Tool – Microsoft Office Suite 2010
Voice and Data



Network
Data Center
Data Warehouse
DNS SEC
Intranet
IPv4 Compatible/IPv6 Capable
Security
Servers

Services
Enterprise Architecture
IT Acquisition
IT Capital Planning
IV&V
Security (Authorization & Accreditation, Continuous Monitoring, HSPD-12, Remote Access)
Service Level Agreements

Any upgrades and/or changes will be determined as needed by the Department’s business requirements.

As the OCIO provides delivery of these common IT products and services to maintain a stable technology platform, the OCIO will also seek ways to improve productivity and cost performance by eliminating costly duplicate, legacy, and stand-alone systems.

4.2 Future Services

To prepare the Department to meet its future business goals, the OCIO’s role will evolve to provide a broader set of technology services to the Department. This future direction will position the OCIO to become a provider of enterprise common services beyond the current technical infrastructure. These future services fall into two areas:

- Enhanced Services
- OCIO Support Services

OCIO continues to develop a clear design for the future enhanced set of service offerings and how these new services will be deployed, supported, and governed. What follows is the OCIO’s current thinking around what IT shared services will be offered based on the Department’s business needs, and the management challenges that OCIO will need to address in the near future to provide these services in an effective and efficient manner.

The future core enterprise technology platform will improve the overall Department’s productivity and fiscal performance with faster, more reliable, and more innovative technologies.



4.2.1 Enhanced Services

The OCIO will develop, deploy, and maintain a set of enhanced technology services to support the Department’s future business needs. The selection of future services will be prioritized by Department business requirements, Federal mandates, and by the CIO’s Innovation Agenda.

4.2.1.1 Department Priorities

The OCIO regularly receives requests for new services that will improve the Department’s business performance. Program offices, business units, and staff commonly requested the following technologies:

Table 5: Common Service Requests

Requested Service	Definition
Collaboration Management	Allow people to work together more efficiently by enabling greater information sharing
Data Management	Usage, processing, and general administration of unstructured information
Document/Record/Content Management	Control the capture and maintenance of an organization’s documents and files
Knowledge Management	Support the identification, gathering, and transformation of documents, reports, and other sources into meaningful information
Mobility Tools	Tools that enable mobile computing
Report Management	Support the organization of data into useful information
Security and privacy	Tools that support confidentiality, integrity, and availability
Work Management	Allow the monitoring of activities within a business process

The OCIO prioritizes its technology efforts by the most requested services from across the Department. Most of the Department’s business units have requested collaboration management and electronic document/record/content management as enterprise services.

In FY 2011, the Department funded an enterprise implementation of SharePoint to provide collaboration services. The OCIO will continue to expand the use of the collaboration platform during FY 2012 – 2015.

Collaboration management tools will allow the Department to integrate and work together on a unified platform. A unified collaborative platform is the most effective way to connect people, processes, and information across the Department and will enable stakeholders to quickly adapt, scale, and extend the platform in response to shifting business needs.

A **document/record/content management** solution allows the Department to control the capture and maintenance of an organization’s documents and files. The availability of an electronic records management tool will provide quick and reliable information for decision making by developing standardized processes for classifying, storing, securing, archiving, and disposing of records.

The OCIO plans to provide SharePoint, Microsoft Office Productivity Suite, and HP TRIM as the collaboration management and electronic document/record/content management solutions to create the foundation for an enhanced enterprise technology platform. The proposed platform can be used to enhance support to the Department’s work activity and business applications such as GEMS, TRIM TRIO, and others. Using the proposed platform, the Department will be able to utilize the various technology services that are provided to create other automated business support applications.



The **proposed enterprise technology platform** diagram below illustrates the future vision of the enhanced enterprise technology platform followed by a table that links each requested enhanced service to the proposed technology that meets that need.

Figure 4: Proposed Enterprise Technology Platform

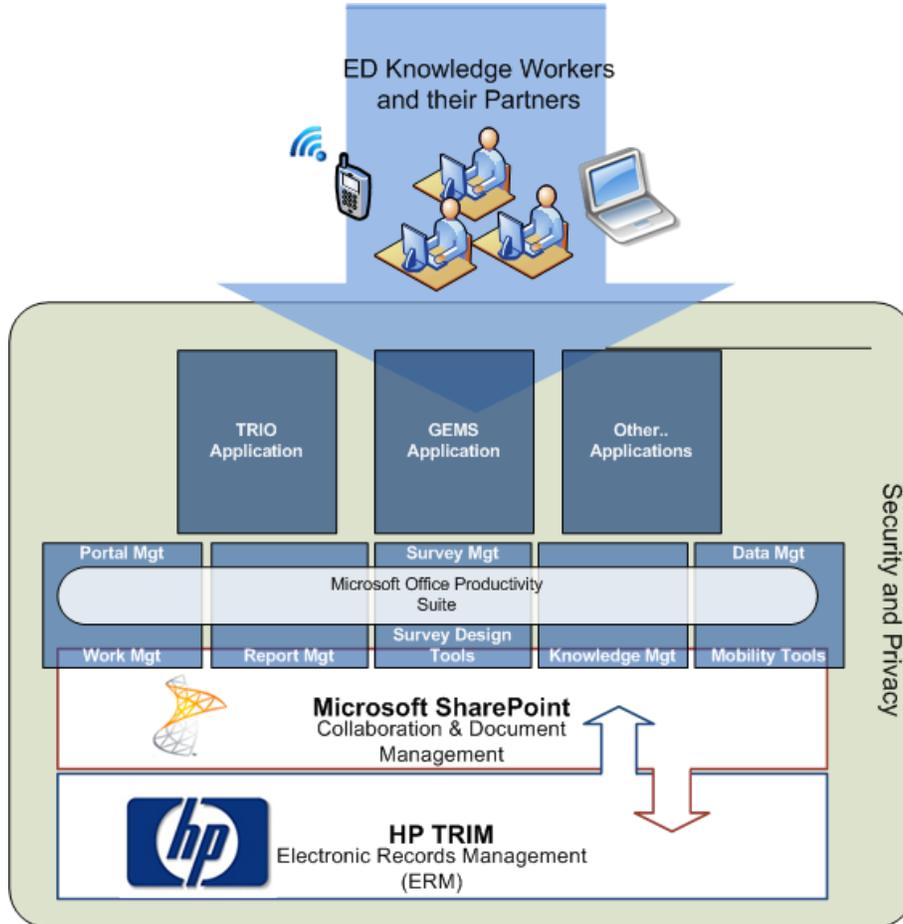


Table 6: Proposed Technology Solutions

Proposed Solution	Requested Service
Microsoft Office	Work Management, Mobility Tools, Survey Design Tools
Microsoft SQL Server	Data Management, Report Management
Microsoft SharePoint	Collaboration Management, Document/Record/Content Management, Survey Management, Portal Management
Microsoft OS Software	Security and Privacy, Mobility Tools
Microsoft Exchange, Outlook	Work Management, Knowledge Management, Data Management, Collaboration Management
Microsoft InfoPath	Report Management, Work Management, Knowledge Management, Data Management, Document/Record/Content Management
HP TRIM	Document and Records Management



4.2.1.2 Federal Technology Initiatives

The OCIO's proposed enhanced enterprise platform will also accommodate the implementation of the following government-wide technology initiatives:

- Cloud Computing
- Data Center Consolidation
- HSPD-12
- IPv6
- TIC
- Electronic Stewardship

The Federal government's technology initiatives are intended to lead government innovation while increasing business efficiency and fiscal responsibility of the Federal government.

4.2.1.2.1 Cloud Computing

The purpose of the Federal Cloud First policy is to move toward a more reliable, efficient, and innovative government. The OCIO's cloud computing implementation will modernize the Department's IT infrastructure with greater efficiency and improved virtualized technologies to support the Department's business performance.

The OCIO will publish a Cloud Computing Security Guidance to ensure the use of cloud services are managed in accordance with existing Federal IT management and security requirements, and to facilitate a well-managed and successful adoption of cloud computing by establishing a process that directs attention to IT-related requirements, management and security processes, and risk factors. The purpose of guidance is to provide CIO-level oversight to address the possibility of a higher level of risk from these new and still-evolving IT service models.

During the current IRM Strategic Plan, the OCIO plans to provide the following cloud computing services:

Infrastructure-as-a-Service (IaaS): The Department will migrate the Department's technical infrastructure to the private cloud. The cloud infrastructure will incorporate fundamental computing resources such as processing, storage and networks so that Department users can deploy and run software, such as operating systems and applications. IaaS will increase utilization of existing investments, reduce infrastructure investments, and decrease IT expenses.

Platform-as-a-Service (PaaS): The Department will provide an integrated computing solution on the cloud. A complete host of computing tools, such as development tools, will be available on the Web. PaaS will improve the management and procurement of IT hosting capabilities.

Software-as-a-Service (SaaS): The Department will migrate its desktop software applications and data to the cloud infrastructure. The software is accessible from various client devices through a thin client interface, such as a Web browser. SaaS will improve the management, cost, and accessibility of software applications.

Additional migration of technology services to the cloud will be evaluated in an ongoing basis. These three cloud services will provide the Department's program offices and end-users with ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.



Table 7: Current (Q1 FY12) Cloud Services³

Service	Service Model	Deployment Model
Survey Services The Civil Rights Data Collection (CRDC) collects data on key education and civil rights issues in our nation's public schools for use by the Department as well as outside policymakers and researchers. The CRDC collects information about students in public schools, including enrollment, educational services, and academic proficiency results, disaggregated by race/ethnicity, sex, limited English proficiency and disability. By moving to a cloud solution, the CRDC was able to survey over 15% more school districts and make the surveys easier for districts to fill out by tailoring each survey so only applicable information was requested.	SaaS	Public Cloud
Agency Private Cloud Services The Department is implementing a private cloud capability to offer Infrastructure as a Service offerings internally. By consolidating the Department's IT infrastructure under this offering, the Department is expecting improved asset utilization by 60-70%, a reduction in overall costs, improved service to its users, and greater agility in demand across the agency.	IaaS/ PaaS	Private Cloud
E-Mail Messaging Security Services Spam filtering, spoofing, and quarantine services for email messaging senders and receivers are provided via a public cloud service provider.	SaaS	Public Cloud
Digital Communications Management Services Robust digital newsletter and email list services are provided by a public cloud service focused on government clients.	SaaS	Community Cloud
Customer Relationship Management Services The Center for Faith-based and Neighborhood Partnerships at the Department uses a cloud-based provider of a customer relations management tool to track contacts and community outreach.	SaaS	Public Cloud
Web Content Hosting Services Federal Student Aid through its Enterprise IT Services (Consolidated ITA/EAI) and other small investments is merging over 70+ existing standalone websites into four integrated views for specific audience segments. These actions are also aligned well with OMB Memo M-11-24, Implementing Executive Order 13571 on Streamlining Service Delivery and Improving Customer Service.	IaaS/ PaaS	Public Cloud

4.2.1.2.2 Data Center Consolidation

The purpose of the government-wide data center consolidation effort is to reduce Federal cost and to shift Federal technologies to more green, innovative and secure solutions. The OCIO's data center consolidation efforts will leverage the cloud infrastructure to optimize its technology services and its IT security, and reduce operational costs.

³ Table taken from U.S. Department of Education Data Center Consolidation Plan



The Department has completed an inventory of its data centers and related assets and developed consolidation plans with a technical roadmap and clear consolidation targets. During the current IRM Strategic Plan, the ED Data Center Consolidation Plan identifies plans to implement the following activities:

- Shut down one data center (shifting from 5 to 4 total data centers)
- Relocate assets to a central primary data center
- Optimize services through virtualized cloud

4.2.1.2.3 HSPD-12

The Federal government established the 2004 mandate for Homeland Security Presidential Directive (HSPD) 12 - Policies for a Common Identification Standard for Federal Employees and Contractors requiring a government-wide standard for secure and reliable forms of identification.

To meet the physical and logical access requirements of HSPD-12 the Department's top HSPD-12 agenda items are identity management, access control, and two factor authentication. The Department of Education's goals in the department-wide integration of HSPD-12 are to reduce identity fraud, protect personal privacy, enhance security, and increase efficiency.

ED will continue to focus on the implementation of the FISMA priorities of Trusted Internet Connections, HSPD-12 and Continuous Monitoring. HSPD-12 implementation focuses agencies on upgrading their physical and logical access control infrastructure to require HSPD-12 PIV credentials for access to IT systems and facilities. As of March 2012, the Department has issued over 4,900 PIV cards to employees and contractors. As stated in the [FY 2011 Annual Report to Congress on the Implementation of the Federal Information Security Management Act of 2002](#), the Federal government had an increase of 11% in HSPD-12 compliance, and it was attributable to several agencies that made significant strides in HSPD-12 implementation to include the Department of Education, which increased 59% in PIV authentication usage in FY 2011.

Currently In Progress. The Department maintains a quarterly HSPD-12 Implementation Status report at http://www2.ed.gov/about/reports/annual/hspd_12.doc

4.2.1.2.4 Trusted Internet Connection (TIC)

The TIC Initiative aims to optimize and standardize the security of the Federal government's network connections. The Department's TIC implementation will improve the Department's security posture and incident response capabilities.

The Department received its Authority to Operate (ATO) as a Trusted Internet Access Provider (TICAP) in January 2010. Most of the technology required has already been implemented in accordance with TIC 1.0. The technologies behind this capability provide improved situational awareness and risk reduction to potential hacker, malware, malicious behavior, and data loss, as well as potential outages and negative public exposures caused by individuals, crime syndicates, or state sponsored "hacker cells." The fulfillment of this requirement can be seen through blocking of Internet sites that are not in alignment with Department policies and existing rules of behavior, as well protection from viruses and worms. Through proper handling of inbound and outbound email and implementing quarantine and junk mail filters, the Department minimizes other potential security issues via spear phishing attacks and the importation of malicious files.



The Department’s current TIC efforts include activities to reduce and consolidate its external network connections, and enhance its external network monitoring capabilities. Forthcoming initiatives related to TIC are: secure email gateways, wireless networks, mobile computing, and teleworking.

Continuous monitoring is provided directly via US CERT for our Internet and external connections. This continuous monitoring provides critical situational awareness, oversight and coordination among all Federal agencies when dealing with attacks that directly target them.

The reduction and consolidation of Internet and external connections provides a smaller risk footprint to manage and oversee, as well as minimization of exposure risks.

The Department has also updated and deployed network and system warning banners to allow for improved prosecution of violators.

In FY2010, the Department implemented Domain Name System Security (DNSSEC) across all of its .GOV domains. The Department will continue to adapt to new TIC 2.0 standards that include added capabilities for HTTPS proxies and Web Application Protection, while remediating TIC 1.0 findings. Major outstanding efforts require further external connection consolidation through DHS monitoring equipment, which will protect information technology assets not housed within either EDUCATE or the VDC environs.

Table 8: TIC Milestones

TIC Milestones	Dates
TIC CCV (audit)	11/09
TICAP Authority To Operate (ATO) (per TIC v1.0 standards)	01/10
TIC CCV (audit)	05/11
Implement Web Content HTTPS filter	04/12
Develop Internal-only Knowledge Management WIKI on IA, Cybersecurity issues	04/12
TIC CCV (audit)	05/12
Standup secondary TIC site (Backup Data Center)	08/12
Consolidate existing VDC & EDUCATE external connections (already residing within the PTC)	08/12
Consolidate COD Internet connection (FSA)	08/12
Implement Telecommunications Services Priority (TSP) codes on circuits	09/12
Implement TIC 2.0 / Obtain TICAP ATO (per TIC v2.0 standards)	09/12
Upgrade public/external facing servers and services (e.g., web, email, DNS, ISP services, etc.) to operationally use native IPv6	09/12
Remediate TIC 2.0 audit findings	05/11 – 10/13
Consolidate non-TIC external connections	01/10 – 08/16
Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6	09/14



4.2.1.2.5 IPv6

The Department's goal in transitioning to an IPv6 capable environment is to provide enhanced technology services to improve the Department's business and efficiency. IPv6 offers several increased benefits from an IPv4 network environment. By enhancing its network features and offering innovative Internet services, IPv6 will enable the Department to support continued growth in users and Internet-based functionality.

The Department has identified key advances from IPv4 to IPv6 as:

- Expanded addressing capability
- Security extensions for authentication and privacy
- Flow labeling capability
- Improved efficiency in routing and packet handling
- Support for auto-configuration and plug-and-play capabilities
- Support for embedded IP security (IPSec)
- Elimination of the need for Network Address Translation (NAT)
- Support for widely deployed routing protocols
- Network efficiency and bandwidth conservation

The Department has identified two primary IPv6 goals:

2012: Public External Facing Servers and Services

- Defining characteristic is that direct connectivity is available to the general public over the Internet
- From a technical perspective, in-scope systems will be at the far side of the socket connection made by the public (e.g., the web server that presents pages to a customer's web browser).
- Includes DNS servers and Mail servers
- **Does not** include systems that provide services to Internet facing servers (e.g. backend database servers)
- **Does not** include utility or internal support servers (e.g., software deployment servers, servers for backup operations)

2014: Internal Client Applications that communicate with public Internet Servers

- Internal client applications refers to software running on computer systems within the Department that are originating connections as clients to other systems
- That communicate with public Internet servers further restricts scope to server systems that are on the Internet and provide services to the public as a whole
- Systems that are on the Internet but provide only restricted access to a limited audience would be private Internet servers and are thus out of scope
- Supporting Enterprise Networks: The network infrastructure that provides the connectivity from in scope ED systems to the Internet



US Department of Education
Information Resources Management (IRM) Strategic Plan
 FY 2012 – 2015

These are the Department’s IPv6 transition activities for externally facing services:

Table 9: External IPv6 Transition Activities

Task Force Phase	Group	Activities	Milestones	Owner	Milestone Date	
Externally-Facing Servers/Services/Applications/Systems	Inventory 10/2010 - 5/2011	Application	Develop IPv6 inventory that includes the IP (IPv4, 6, dual) and retirement status of external-facing applications	IPv6 inventory data call to POC	Application Owner	3/30/2011
		Application	Submit funding requests for select phase to POC.	Non-major data call, Select Presentations	Application Owner	4/30/2011
		Application	Develop high-level transition milestones for external apps	IPv6 data call Update	Application Owner	5/1/2011
		Governance	Appoint Agency Transition Manager	Appointment of Agency Transition Manager	OCIO-EA	10/30/2010
		Governance	Establish an internal tiger team reporting to the CIO	Internal Tiger Team meeting notes	OCIO-EA	3/30/2011
		Governance	Update IPv6 Transition Plan	Updated IPv6 Transition Plan	OCIO-EA	4/30/2011
		Infrastructure	Identify a website for enablement (www.ed.gov)	IPv6 enabled website	OCIO-ITS	3/30/2011
		Infrastructure	IPv6 service request completed	IPv6 service	OCIO-ITS	5/15/2011
		Infrastructure	Develop inventory of network components that support external systems.	Updated Inventory List	OCIO-ITS	4/30/2011
		Infrastructure	Determine requirement for IPv6 test lab	Test lab requirements	OCIO-ITS	4/30/2011
		Infrastructure	Submit funding requests for select phase to POC.	Non-major data call, Select Presentations	OCIO-ITS	5/16/2011
		Infrastructure	Develop IPv6 Addressing, Network Management, and Testing Plan	IPv6 Addressing Plan, Network Management Plan, Testing Plan	OCIO-ITS	5/30/2011
		Infrastructure	Begin inventory of agency Mail Exchanges (MX)	MX Inventory	OCIO-ITS	5/30/2011
		Assessment 4/2011 - 9/2011	Application	Certify external apps for IPv4, IPv6 or Dual Stack Capability	IPv6 inventory data call to POC	Application Owner
	Application		Examine external applications for IPv4 dependency	IPv4 dependency report	Application Owner	8/30/2011
	Application		Prioritize external applications for upgrades or retirement	Priority list	Application Owner	6/30/2011
	Application		Develop Transition and Remediation Plans for external applications	Transition Strategy, Remediation Plan (per application or system)	Application Owner	8/30/2011
	Governance		Participate in World IPv6-day	Participation	OCIO-EA	6/8/2011
	Governance		Record the agency’s first public ipv6-enabled web site	IPv6 Web Site AAAA record	OCIO-EA	6/8/2011
	Governance		Begin research, develop, & vet security concerns	Security report on IPv6	OCIO-IA	9/30/2011
	Governance		Begin development of IPv6 security policy	Security policy document	OCIO-IA	9/30/2011
	Governance		Begin development of IPv6 security procedures	Security procedures document	OCIO-IA	9/30/2011
	Governance		Begin development of IPv6 security technical implementation guides (STIG)	STIGs for network devices	OCIO-IA	9/30/2011
	Infrastructure		Develop Test Lab Requirements and budget requests	Requirements document, POC budget request	OCIO-ITS	7/1/2011
	Infrastructure		Enable IPv6 Web server (www.ed.gov)	IPv6 Web server (www.ed.gov) enabled	OCIO-ITS	5/15/2011
	Infrastructure		Establish one (minimum) DNS server with AAAA record	Authoritative DNS with AAAA record	OCIO-ITS	5/15/2011
	Infrastructure		Examine MX for IPv4 dependency	IPv4 dependency report	OCIO-ITS	7/1/2011
	Infrastructure		Ensure addressing plan ready to implement	Addressing plan certification	OCIO-ITS	6/30/2011
	Infrastructure		Prioritize network components for upgrade or retirement	Priority list	OCIO-ITS	8/30/2011
	Infrastructure		Develop Transition and Remediation Plans for network components	Transition Strategy, Remediation Plan	OCIO-ITS	8/30/2011
	Remediation 4/2011 - 4/2012		Application	Begin upgrade of external applications to support IPv6	Application upgrade	Application Owner
		Application	Develop an application Test Plan	Test plan	Application Owner	4/30/2012
		Governance	Update Transition Plan	Updated Transition Plan	OCIO-EA	9/30/2011
		Governance	Begin deployment of IPv6 security procedures	Security procedures document	OCIO-IA	10/1/2011
Governance		Identify additional public services and services, including sub agencies	Updated URL List	OCIO-EA	12/30/2011	
Governance		Begin support staff, operations and security staff training	Training class	OCIO-EA	4/30/2012	
Infrastructure		Finalize plan for DNS, review IPSec signing to include AAAA records	Updated DNS Plan	OCIO-ITS	9/30/2011	
Infrastructure		Begin deployment of IPv6 security technical implementation guides (STIG)	implemented STIGs in configurations of network devices	OCIO-ITS	10/1/2011	
Infrastructure		Prioritize MX for upgrades or retirement	MX Upgrade Plan	OCIO-ITS	9/30/2011	
Infrastructure		Upgrade MX components to support IPv6	MX component upgrade certification	OCIO-ITS	9/30/2011	
Infrastructure		Upgrade DNS to support IPv6	OCIO-ITS	9/30/2011		
Infrastructure		Authoritative DNS servers to provide transport over IPv6	IPv6 Transport validated	OCIO-ITS	12/30/2011	
Infrastructure		Upgrade network components to support IPv6	OCIO-ITS	12/30/2011		
Testing 5/2012-8/2012		Application	Begin testing IPv6 applications	Test Plan Results	Application Owner	5/30/2012
	Application	Certify operation of needed IPv4 applications on network	Test Plan Results	Application Owner	8/30/2012	
	Application	Certify external-facing applications as IPv6 Operational	Test Plan Results	Application Owner	8/30/2012	
	Application	Certify external-facing applications as Dual Stack Operational	Test Plan Results	Application Owner	8/30/2012	
	Governance	Update Transition Plan	Updated Transition Plan	OCIO-EA	8/30/2012	
	Infrastructure	Test Lab in Place	Test Lab	OCIO-ITS	5/1/2012	
	Infrastructure	Begin testing IPv6 systems	Test Plan Results	OCIO-ITS	5/30/2011	
	Infrastructure	Certify external/public-facing servers as IPv6 Operational	Security Authorization	OCIO-ITS	8/30/2012	
Implementation 9/2012 - 10/2012	Infrastructure	Certify external/public-facing servers as Dual Stack Operational	OCIO-ITS	8/30/2012		
	Application	Deploy external-facing IPv6 Applications	Security Authorization	Application Owner	9/30/2012	
	Application	Begin decommission of IPv4 applications as needed	Updated IPv6 inventory data call	Application Owner	10/1/2012	
	Infrastructure	Implementation IPv6 systems	Security Authorization	OCIO-ITS	9/30/2012	
Infrastructure	Begin Decommission of IPv4 Nodes asneeded	Updated IPv6 inventory data call	OCIO-ITS	10/1/2012		
Governance	Validate upgrade of public/external facing servers	IPv6 report to OMB, updated Transition Plan	OCIO-EA	10/1/2012		



These are the Department’s IPv6 transition activities for internally facing services:

Table 10: Internal IPv6 Transition Activities

Task Force Phase	Group	Activities	Milestones	Owner	Milestone Dates
Inventory 3/2012-9/2014	Application	Develop IPv6 inventory that includes the IP (IPv4, 6, dual) and retirement status of external-facing applications	IPv6 inventory data call to POC	Application Owner	3/10/2012
	Application	Submit funding requests for select phase to POC	Non-major data call, Select Presentations	Application Owner	5/30/2012
Assessment 6/2012-9/2012	Application	Examine applications for IPv4 dependency	IPv4 dependency report	Application Owner	7/30/2012
	Application	Prioritize applications for upgrades or decommissioning	Priority List	Application Owner	7/30/2012
	Application	Develop Transition Strategy and Remediation Plan	Transition Strategy and Remediation Plans (per application or system)	Application Owner	7/30/2012
	Governance	Research, develop, & vet security concerns	Security report on IPv6 (internal-facing)	OCIO-IA	6/30/2012
	Governance	Develop IPv6 security procedures	STIGs	OCIO-IA	6/30/2012
	Governance	Update Transition Plan (co-incides with update for external-facing)	Updated Transition Plan	OCIO-EA	9/30/2012
	Governance	Procurement policy updated for internal applications	Updated procurement policy for IPv6	CAMS	9/30/2012
	Infrastructure	Examine applications for IPv4 dependency	IPv4 dependency report	OCIO-ITS	7/30/2012
	Infrastructure	Prioritize applications for upgrades or decommissioning	Priority List	OCIO-ITS	7/30/2012
	Infrastructure	Update addressing plan for internal-facing applications	Updated addressing plan	OCIO-ITS	6/30/2012
Remediation 9/2012 to 7/2013	Infrastructure	Update Transition and Remediation Plans if necessary	Updated Transition, Remediation Plans	OCIO-ITS	8/30/2012
	Application	Develop Test Plan	Test Plan	Application Owner	9/30/2012
	Application	Upgrade applications to support IPv6	Updated IPv6 inventory data call to POC	Application Owner	7/30/2013
	Infrastructure	Develop Test Plan	Test Plan	OCIO-ITS	9/30/2012
Testing 7/2013-8/2014	Infrastructure	Upgrade applications to support IPv6	Updated IPv6 inventory data call to POC	OCIO-ITS	7/30/2013
	Application	Test IPv6 applications	Test Plan results	Application Owner	7/30/2014
	Application	Certify operation of needed IPv4 applications on network	Test Plan results	Application Owner	8/30/2014
Implementation 9/2014	Application	Certify internal facing applications as IPv6 Operational	Test Plan results	Application Owner	8/30/2014
	Infrastructure	Ensure test lab is available for internal application testing	Test Lab	OCIO-ITS	7/30/2013
	Application	Implement Internal-facing IPv6 Applications	Test Plan Results	Application Owner	9/30/2014
	Application	Begin decommission of IPv4 applications as needed	Updated IPv6 inventory data call	Application Owner	9/30/2014
	Infrastructure	Implement internal-facing IPv6 Applications	Test Plan Results	OCIO-ITS	9/30/2014
	Infrastructure	Begin decommission of IPv4 applications as needed	Updated IPv6 inventory data call	OCIO-ITS	9/30/2014
	Governance	Validate upgrade of internal-facing applications for IPv6	IPv6 report to OMB, updated Transition Plan	OCIO-EA	9/30/2014

The Department has successfully met the following IPv6 Transition Milestones:

- **October 2010:** Appointed ED IPv6 Transition Manager
- **April 2011:** Updated Departmental IPv6 Transition Guidance
- **April 2011:** Collected Inventory for Externally Facing Applications
- **May 2011:** Developed IPv6 Milestones for Externally Facing Applications
- **June 2011:** Participated in World IPv6 Day
- **September 2011:** Data Call on IPv6 Implementation Progress

Currently in Progress: IPv6 Remediation Activity. Tracking on the Department’s IPv6 progress is best viewed at NIST’s “Estimating IPv6 & DNSSEC Deployment Status” website at <http://usgv6-deploymon.antd.nist.gov/cgi-bin/cfo?agency=education>



4.2.1.2.6 Electronic Stewardship

The purpose of the electronic stewardship program activities is to support the Federal leadership goals for economic, energy and environmental leadership as outlined in Executive Order 13514.

Specific goals and activities supporting the agency's Strategic Sustainability Performance Plan include:

- **2008:** The Department deploys EPEAT Gold and Silver qualified desktop computers, notebook computers and monitors across the enterprise. The Department uses environmentally sound disposal practices for excess or surplus electronic products via an e-Stewards certified recycler.
- **2009:** The Department joins the Federal Electronics Challenge as an agency partner and its "ED Centralized" facility partner. The Department submits its baseline survey and participates in the Federal Electronics Stewardship Working Group
- **2010:** The Department is awarded its first Federal Electronics Challenge (Bronze Level) Award for its operations and maintenance activities. The Department submits its first annual report.
- **2011:** The Department begins implementing "duplex printing as a default" on its network-based printing and digital imaging equipment. All regional office locations are completed.
- **2013:** The Department completes migration to "duplex printing as a default" across its entire portfolio of network-based printing and imaging equipment.
- **2014-2016:** The Department continues to operate and maintain Energy Star and EPEAT Gold and Silver equipment, maintains power management settings, duplex printing and environmentally preferred purchasing of electronic equipment, and serves as a Federal champion for electronic stewardship.

4.2.1.3 CIO's Innovation Agenda

The CIO promotes a shared vision of the Department's information activities and offers services to effectively manage information to provide value-adding enterprise-wide systems and infrastructure. While the IRM Strategic Plan is a reactive response supporting the Department's mission, the CIO's Innovation Agenda is a proactive approach to transforming the Department's IT infrastructure to create the business value of tomorrow.

It is the CIO's role to recognize and implement information technology as a business enabler and catalyst to drive value across the enterprise.

The CIO's Innovation Agenda identifies new technologies and services to generate cutting-edge business growth and advantage. The new technologies should be flexible and responsive to support the existing infrastructure, while offering new opportunities for growth.

The current focus of the CIO's Innovation Agenda is Access Anywhere Computing, which will integrate mobile computing and consumer-owned devices into the Department's computing environment.



4.2.1.3.1 Access Anywhere Computing

The Department will make it easier for staff to work inside and outside the office by making the applications and data available on multiple platforms and accessible anywhere. This will improve performance and reduce costs in the following ways:

Improved Performance

- Leverage of employee-owned devices to help increase productivity by helping employees enjoy the benefits of single device management
- Increase optimization of ED infrastructure
- Retain high-quality employees while maintaining oversight and security of agency data on employee-owned devices

Improved Efficiency

- Allow a user to integrate with workgroups, through cloud services, on any device, anywhere
- Allow a user access to their applications, such as office productivity software on travel, at home, and/or in the office
- Enable virtual desktops and applications with the same features for the same user experience on any device, anywhere, offline, or online

Reduced Costs

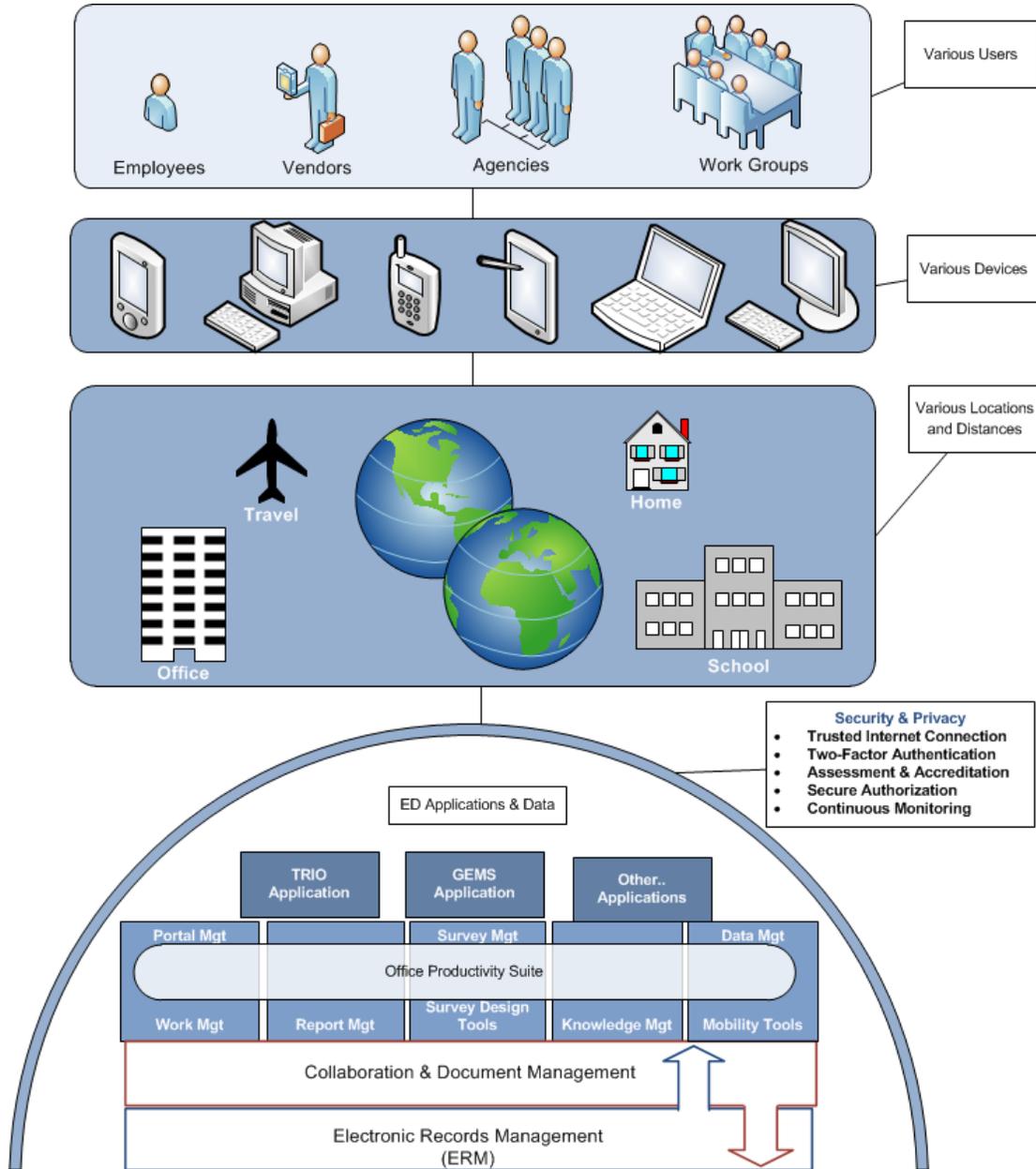
- Allow dedication of agency IT resources toward strategic projects rather than management of many devices
- Enable use of employees-owned IT resources to improve work life balance with virtual work experience
- Allow faster, cost-effective on-boarding of new employees and contractors, while ensuring corporate data security
- Enable shared services and cloud computing
- Allow compatibility with hardware devices such as:
 - tablets
 - mobile phones
 - desktops

Delivery of these applications will be via web servers, portal servers, and virtual host servers. Virtual host servers will **let workers use personal mobile devices for work, while letting IT retain security and control over work-related apps on those devices.**



Access anywhere computing allows for unified automated application management with dynamic services and applications. This will eliminate the need for manual access management (e.g., creation and reset of accounts, and licensing), Also, this means users will have faster access to their applications.

Figure 5: The Department’s Access Anywhere Model



4.2.2 OCIO Support Services

The OCIO may offer the Department’s business customers the following three technology support services:

- IT Planning and Design Services
- IT Project Management Services
- End-user IT Support Services



IT Planning and Design Services will help program offices align their business priorities with enabling IT capabilities to further both the POC and the Department's overall mission. These services could include:

- Program office IT planning services in support of multi-year IT investment and project plans that provide the maximum benefits of available IT resources to the offices. These services could include future state IT visions for POCs, future state concepts of operation that identify the role of technical capabilities in supporting the business unit mission, and the development of transition strategies and project portfolios that leverage existing and new IT components.
- Solutions architecture and design services including the definition, description, and high-level requirements for discrete IT projects and/or the application of common enabling services (e.g., workflow and collaboration tools) to solve specific business needs

IT Project Management Services include a full range of services for applying technical capabilities to solve office business needs. These services are envisioned to involve custom application development services, package installation and deployment services, or individual subject matter expertise to support program office development teams (e.g., project management, acquisition guidance/support). These services could include:

- Applications development, enhancement and deployment services (e.g., web applications and decision support applications development)
- Commercial off the shelf (COTS) software package identification, selection, installation, and support
- IT solutions project management and acquisition support services

The selection and deployment of these services will require OCIO to engage in the following activities to provide IT solution development and deployment services:

- Development of detailed plans and product recommendations for various types of Common Enabling Services (CES)
- Support to program offices to define relevant knowledge work requirements that will be optimally fulfilled by the CES
- Acquisition, deployment, and operations of COTS products on the infrastructure to provide CES
- Development of common enterprise-wide solutions or custom-developed solutions for individual program offices
- Ongoing training, configuration support, help desk and related customer service top program office users to maintain or adjust usage of CES



End-user Support Services would be provided as a shared service to the Department to fill a key gap in the current IT support model at the Department. The future direction for IT at the Department is heavily focused on data access and analytical activities in support of the Department’s mission. With the exception of small pockets within certain organizations, the Department has little expertise in supporting its end users in these areas. As the Department moves toward the application of enterprise data stores, enhanced analytical tools for end users, and the rollout of common enabling infrastructure tools to its knowledge workers, these same knowledge workers will require support to effectively apply these new capabilities to their day-to-day efforts. A set of shared services will be provided to deliver this support to the end users and could include the following:

- End user data access, query and reporting support services, including Executive Dashboard support services, to ensure the users understand the data available to them, how to access that data, and how best to manipulate the data in performing sophisticated analyses,
- Technology/solutions training and support services for end users so the users can effectively use the new capabilities and derive value from these investments, and
- Enterprise application operations and end user support services (e.g., EDEN and Enterprise Data Warehouse application support) involve the basic support for shared applications – efficiently delivered as a shared service. Applications that are shared across an organization require support that is also shared.

4.3 Management Structure for Future Services

The Department will focus on these key goals for the implementation of all future technology services:

- 1) Establishing an effective product and service delivery model
- 2) Implementing an effective governance model
- 3) Supporting the programs to develop a funding strategy
- 4) IT as a service provider to the Department

The service delivery model for shared services will be based on the following set of guiding principles for the OCIO’s operating model:

- Promote a supplier-customer relationship between IT and the business units to foster a “customer service” culture in IT while maintaining the fiduciary role of OCIO
- Implement an appropriate funding model for shared services that promotes financial transparency so that customers understand the costs associated with the products/services they consume, and understand the cost levers available to them (e.g., accept a higher level of service for a higher cost to meet special business needs)
- Introduce a “product-centric” model that integrates multiple disciplines and ensures accountability for the products/services offered to the customers. This model would include future product strategy, service level options, product refresh plans, etc.
- Separate the product/service planning and development functions (plan/build) from the operations functions to allow each to excel in their own individual disciplines and ensure that strategic, tactical, and operational imperatives are met



The product and service model defines roles, responsibilities, and accountabilities for operating the shared services at the Department. Some of the management issues include:

- When should the Department come to OCIO for a service and when should the service be contracted-out?
- What is the role of OCIO in satisfying office-specific business needs and how does that role differ if the need is enterprise-wide?
- How can OCIO maintain its fiduciary role when another organization or entity delivers the shared service?
- How will the Department decide whether a shared service is to be provided by OCIO or another organization (e.g., Office of the Chief Financial Officer, Institute for Education Sciences)?
- What is the governance model that will address investment priorities, funding mechanisms, portfolio effectiveness, service levels for shared services, and adherence/compliance actions?
- Are there service-specific governance models that are required, i.e., shared applications require shared support functions and shared governance?
- What are the appropriate organizational and contractual vehicles that are required to deliver shared services?

Specific steps to move toward the shared services operating model include addressing the following:

- Understand and document the needs of the customers for specific products and services that can best be developed, delivered, and supported centrally
- Support the goals of Federal IT reform initiatives, such as [Federal Information Technology Shared Services Strategy](#), the [.GOV Reform Effort to Improve Federal Websites](#), and the [Federal Mobility Strategy](#), using shared IT resources to the maximum extent possible
- Offer these shared products and services to the business efficiently and at an appropriate level of service and cost
- Install product and service monitoring functions to adjust the product and service mix (i.e., specific products, services, new service levels, etc.) to reflect changes in the business needs and the demand for these products and services
- Define and adopt a sound management model that allows the organization to effectively address the strategic, tactical, operational, and governance issues simultaneously



5 Goal Three: Information and Technology Management

The IRM Strategic Plan’s information and technology management goal is to coordinate IT management processes and plans to ensure the effective use of IT resources across the Department.

The following are key Department stakeholders who govern and contribute to the information resource management process.

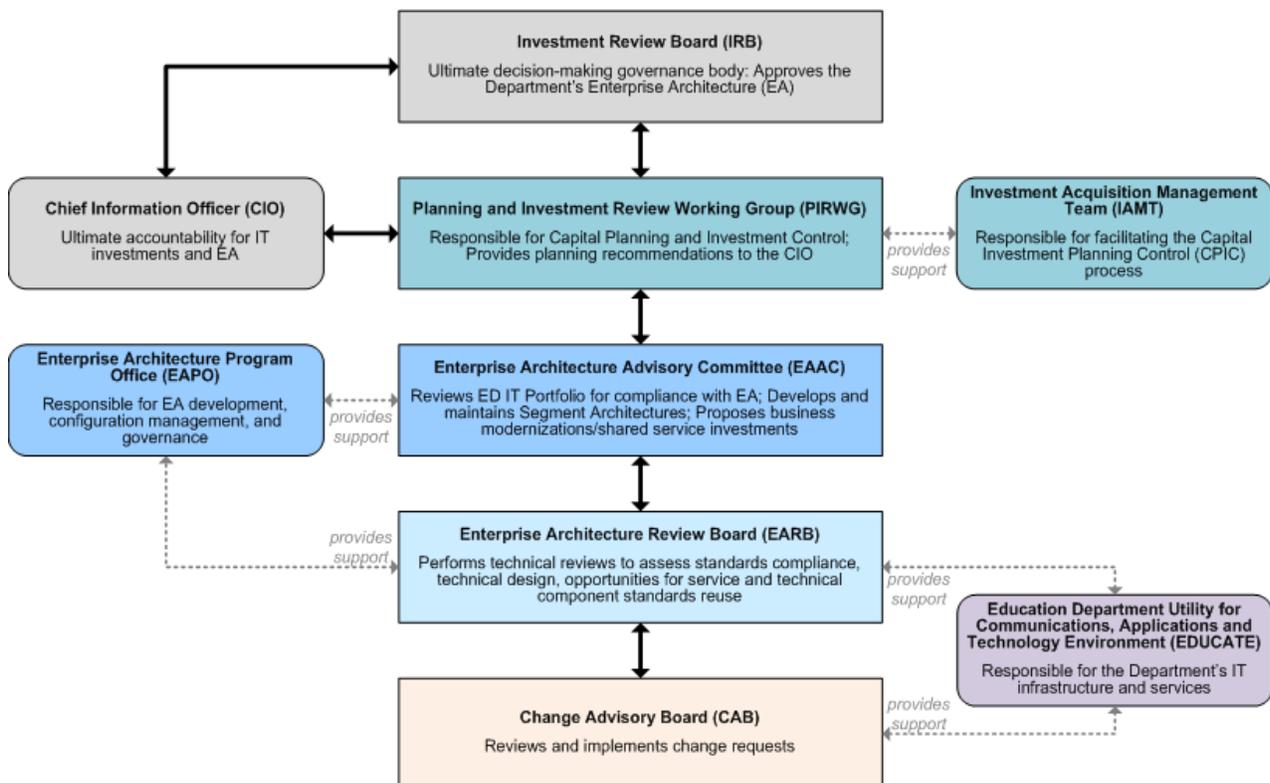
5.1 IT Governance Structure

The stakeholders in the Department’s IT governance structure determine IT management policies and plans directly impacting the Department’s information resources management process.

The Department’s IT governance process is codified in Departmental Directive OCIO 1-106, Lifecycle Management (LCM) Framework. The LCM Framework provides the foundation for the implementation of standards, processes and procedures used in developing and managing technology. The Department’s IT governance process ensures alignment of current and future IT initiatives to its strategic business objectives, as outlined in the FY 2012-2016 Department Strategic Plan.

The Department’s IT governance process applies to major program/mission critical investments and non-major program/mission support investments that are included in the Department IT portfolio. The IT governance process ensures that the Department’s IT portfolio is managed in a manner that is consistent with agency policy and OMB requirements. The IT governance process is managed through organizational entities – review boards and subordinate working groups shown in Figure 4.

Figure 6: The Governance Process at the Department





5.1.1 Enterprise Architecture (EA) Program Office

The Enterprise Architecture Program Office is an essential component of the Department's IT governance process. The EA Program Office provides governance services, produces guidance, and influences policies that directly impact information resources management.

The EA Program Office facilitates two governance bodies, the Enterprise Architecture Advisory Committee and the Enterprise Architecture Review Board:

- **Enterprise Architecture Advisory Committee (EAAC):** Provides support and guidance to the development of the Departmental Enterprise Architecture and advises the Planning and Investment Review Working Group (PIRWG) on information technology needs and priorities.
- **Enterprise Architecture Review Board (EARB):** Provides support to the EAAC and EA program office by maintaining the Department's technical standards, ensuring standards compliance and interoperability, facilitating component reuse, and validating solution architecture compliance with Department security standards.

5.1.2 Investment and Acquisition Management Team (IAMT)

The Investment and Acquisition Management Team (IAMT) is an essential member of the Department's IT governance process. The IAMT ensures that all Department of Education IT acquisitions are reviewed and accounted for in the Department's capital planning and investment IT portfolio. The IAMT supports the Department's information resources capital planning and investment control (CPIC) processes along with Department-wide bodies such as the Investment Review Board (IRB) and the PIRWG to ensure continuity in the selection, monitoring, and evaluation of the Department's IT investments.

5.2 Key Department Contributors to the IRM Governance Process

The following Department programs are key contributors to the effective management of IT resources across the Department.

5.2.1 IT Acquisition (Procurement)

The Department's Contracts & Acquisition Management (CAM) team proactively leads the acquisition process, planning, negotiating, awarding and administering of contracts, including contracts for IT investments. CAM activities ensure the Department's procuring and contracting are completed in accordance with established Department and federal acquisition policies and procedures. CAM also enforces a procurement career management program to ensure adequate and professional acquisition work force at the Department. The Performance and Logistics Group (PLG), within CAM, provides technology, systems, acquisition policy and logistical support to Department groups.



5.2.2 Regulatory Information Management

Privacy, Information and Records Management Services (PIRMS) is the Department's organization responsible for providing policies, standards, and procedures that ensures the Department's activities comply with the Federal information management requirements. PIRMS maintains the Department's Regulatory Information Management (RIM) for:

- Privacy (Privacy Safeguards Division)
- Parent and student privacy rights (Family Policy Compliance Division)
- Information Collection Clearance (Information Collections Clearance Division)
- Federal Records Management
- Freedom of Information Act Request Processing

PIRMS ensures Department activities are compliant with information management requirements through the following governance bodies:

- Data Integrity Board
- Data Release Workgroup, chaired by the Chief Privacy Officer
- FOIA Coordinators – all POCs
- Program Records Officials and Records Liaison Officers – all POCs
- Electronic Records Management Executive Steering Committee (new in FY 2012 – subset of SES/GS-15)
- Information Collection Coordinators – all POCs
- Directives Liaison Officers – all POCs

Regulatory Information Management is a key component in the Department's IRM efforts, and contributes to the effective management of the IRM Strategic Plan goals, portfolio alignment and technology services.

PIRMS reviews Department investments and acquisitions to ensure compliance with Department and Federal Regulatory Information Management policy and procedures.

- Ensures internal compliance with the statutory requirements and regulatory controls on information program offices think they need to collect from public stakeholders
- RIM's clearance process shapes the systems and databases that the POCs develop in order to administer Departmental programs

5.2.3 Information Assurance Services (IAS)

Information Assurance Services (IAS) oversees the Department's information technology security program and ensures the confidentiality/privacy, integrity, and availability of the Department's information and information resources. IAS ensures that the Department is fully compliant with FISMA, and all related statutes and directives. The organization provides standardized security services and solutions in areas such as risk management; access controls; identity and access management, authentication; encryption solutions; public key infrastructure (PKI) technology; and certification and accreditation (C&A). IAS also directs the agency's Managed Security Services Program (MSSP) ensuring contractor compliance with MSSP requirements governing the management of the agency's enterprise-wide security operations center; the mitigation of security vulnerabilities and improvement of the Department's IT security posture; portal security; and sound configuration management of EDUCATE and its tenant systems.



5.2.4 Information Technology Services (ITS)

Information Technology Services (ITS) supports all enterprise-wide initiatives that reside on the agency's network (EDUCATE) to include network security, network and telecommunications design and operations, end user services, production server hosting services, and the agency's intranet and Internet services. Additionally, ITS maintains and operates the Department's primary data center and disaster recovery facility. As assigned, ITS develops and maintains common business solutions that are required by multiple program offices.

The ITS team manages or provides oversight for all enterprise-wide information technology. It develops recommendations and implements IT solutions designed to enhance and enable the Department business processes that affect all like investments across the department.

- **Cloud Computing Services** – acquisition and use of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) solutions, including existing GSA BPAs.
- **Shared IT Services** – acquisition and use of service offerings provided by other Federal agencies that when leveraged may provide the investment at a lower cost, with a faster implementation method than the original acquisition strategy. Services range from web hosting, cloud solutions to unique and smaller goods.
- **Web Hosting Services** – use of GSA or open-competition contract vehicles, such as GSA Network, Alliant and IT Schedule 70 for professional services for a full range of IT services, hardware and software.
- **Electronic Stewardship / e-Cycling** – best practices for "green IT" practices for acquiring sustainable and environmental friendly IT solutions for conferences, computer equipment and beyond.
- **OMB Mandates** – ensures investment is consistent with new and existing OMB mandates and federal regulations that may impact the acquisition strategy of numerous investments.

5.2.4.1 Network Services Team

The Network Services Team provides support for the agency's enterprise-wide portfolio of networking, telecommunications and multimedia services. Team members serve as subject matter experts for areas related to:

- **Network (WAN/MAN/LAN)** – acquisition and use of network hardware and software for connectivity to and from the Internet ranging from voice, video and data circuits, routers, switches, firewalls, intrusion detection/protection services, Domain Name Service (DNS), Internet Protocol version 6 (IPv6) requirements, remote access services, Virtual Private Network (VPN) technology, and authorization and use of various ports and protocols.
- **Telecommunications / IP Telephony** – including use of traditional (analog) and Voice over Internet Protocol (VoIP) phone services, call center support services, Interactive Voice Response (IVR), toll-free numbers, digital subscriber line (DSL) and cable modems, calling cards, audio conferencing, etc.
- **Multimedia Services** – acquisition and use of multimedia platforms and services, including audio-visual services, auditorium and events, webinar technology, voice, video and data conferencing.
- **Mobility and Wireless Services** – acquisition and use of mobile devices, platforms and services including wireless handhelds, smartphones, tablets, WiFi (WLAN) services, mobile hotspots, Aircards, including support for emerging technologies, telework solutions and Bring Your Own Device (BYOD) policies and support mechanisms



5.2.4.2 Operational Services Team

The Operational Services Team provides support for the ongoing operations and maintenance of the agency's enterprise-wide deployments of a full range of technology services:

- **Desktop Services** – acquisition and use of desktop computers, notebook computers, and monitors, including emerging technology such as virtual desktop interface (VDI)
- **Data Center Services** – acquisition and use of network hardware and software for connectivity to and from the Internet, including routers, switches, firewalls, intrusion detection/protection services, Domain Name Service (DNS), and authorization and use of various ports and protocols
- **E-Mail Services** – acquisition and use of digital communication services, such as e-mail, instant messaging, personal information management (calendaring, tasks, journal)
- **ListServ Services** – acquisition and use of multimedia platforms and services, including audio-visual services, auditorium and events,
- **Print Management Services** – acquisition and use of print and digital imaging equipment, including multifunction devices (print, copy, fax, scan), scanners, facsimile (fax) machines
- **Assistance Technology (AT)** – acquisition, compatibility and use of electronic and information technologies in support of Section 508 of the Rehabilitation Act, as amended, in support of persons with disabilities

5.2.5 Human Resources Management

The Department's Human Capital and Client Services (HCCS) provide leadership and direction in the formulation and implementation of policies, programs, and systems to promote efficient and effective human capital management. In performing its responsibilities, HCCS:

- Maintains the traditional values of the Federal civil service system including integrity, continuity, nonpartisanship, merit and equal employment opportunity.
- Provides the Secretary, Deputy Secretary, and other executive level managers with expert human capital management advice and a high level of technical services that further the goals and objectives of the Department.
- Establishes and maintains staff resource utilization needs for key officials within the Department.
- Ensures that Federal and Departmental human capital goals, policies, and practices are communicated to all levels of management and, where appropriate, to employees.
- Evaluates the effectiveness of human capital and resources programs.

These HCCS activities are essential in promoting effective information resource management throughout the Department.



6 List of Figures

Figure 1: IRM Strategic Plan Goals	5
Figure 2: Segment Alignment to Department Strategic Goals.....	9
Figure 3: Principal Office and Segment Engagement.....	10
Figure 4: Proposed Enterprise Technology Platform	20
Figure 5: The Department’s Access Anywhere Model.....	30
Figure 6: The Governance Process at the Department.....	34

7 List of Tables

Table 1: Department of Education Strategic Goals.....	6
Table 2: Department of Education Strategic Goals and Strategic Objectives.....	7
Table 3: The Department’s 13 Segments.....	8
Table 4: Current Delivery of Services	17
Table 5: Common Service Requests.....	19
Table 6: Proposed Technology Solutions	20
Table 7: Current (Q1 FY12) Cloud Services	22
Table 8: TIC Milestones	24
Table 9: External IPv6 Transition Activities.....	26
Table 10: Internal IPv6 Transition Activities	27