

Archived Information



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

Information Resources Management (IRM)

Strategic Plan

FY2013 – 2016

Final

May 2013



Contents

- 1 Introduction (DXXA) 5
- 2 IRM Goals (AXXA) 6
- 3 Goal One: Portfolio Alignment (AXXB) 7
 - 3.1 Department Alignment 7
 - 3.1.1 Department Strategic Plan (AXXA) 7
 - 3.1.2 Segment Architecture 9
 - 3.1.3 Value Measurement Methodology (VMM) (CXXC) (CXXD) (CXXE) 12
 - 3.2 Federal Alignment (BXXA) (BXXB) (BXXC) 13
 - 3.2.1 Digital Government Strategy (GXXA) 15
 - 3.2.1.1 Information Centric 16
 - 3.2.1.2 Shared Platform 17
 - 3.2.1.3 Customer Centric 18
 - 3.2.1.4 Security and Privacy (EXXA) 21
 - 3.2.2 Federal Data Center Consolidation 23
- 4 Goal Two: Technology Services (AXXB) (CXXG) 24
 - 4.1 Current Services 24
 - 4.2 Future Services 26
 - 4.2.1 CIO’s Innovation Agenda 27
 - 4.2.1.1 Access Anywhere Computing 28
 - 4.2.1.2 OCIO Support Services 30
 - 4.2.2 Common Enabling Services (CES) 31
 - 4.2.3 Commodity IT and Shared Services 34
 - 4.2.3.1 Maturing the IT portfolio (HXXA) 34
 - 4.2.3.2 Use of savings resulting from consolidations of Commodity IT (HXXB) 34
 - 4.2.3.3 Maximizing use of inter- and intra-agency shared services (HXXC) 34
 - 4.2.3.4 Continuity of operation for mission critical applications (EXXB) 35
 - 4.2.4 Cloud Computing 35
 - 4.2.5 Cybersecurity Initiatives (EXXA) 37
 - 4.2.5.1 Homeland Security Presidential Directive-12 37
 - 4.2.5.2 Trusted Internet Connection (TIC) 38



US Department of Education
Office of the Chief Information Officer

4.2.5.3	Continuous Monitoring (CM)	40
4.2.6	IPv6.....	41
4.2.7	Electronic Stewardship.....	43
5	Goal Three: Information and Technology Management (AXXB)	45
5.1	IT Governance Structure (CXXA) (CXXB)	45
5.1.1	Enterprise Architecture Program Office (EAPO)	46
5.1.2	Investment and Acquisition Management Team (IAMT).....	47
5.2	Key Department Contributors to the IRM Governance Process (CXXB).....	47
5.2.1	IT Acquisition (Procurement)	47
5.2.2	Regulatory Information Management	47
5.2.3	Information Assurance Services (IAS) (GXXB)	48
5.2.4	Information Technology Services (ITS).....	48
5.2.4.1	Network Services Team.....	49
5.2.4.2	Operational Services Team	49
5.2.5	Human Capital Management (FXXA)	50
5.2.6	Accessibility (IXXA) (IXXB) (IXXC).....	50
6	List of Figures	53
7	List of Tables	53



Document Purpose

This purpose of this document is to describe how 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 IT resources. These five sections are as follows:

Section 1 is the Introduction, which specifies the Chief Information Officer's (CIO) objectives and planning horizon of the Information Resources Management (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 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 (DXXA)

The CIO 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 2013 - 2016 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 and Results Act of 1993
- Clinger-Cohen Act of 1996
- E-Government Act of 2002
- Implementing Portfolio Stat Memorandum OMB M-12-10
- Chief Information Officer Authorities Memorandum OMB M-11-29,
- Federal Enterprise Architecture (FEA)



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.” OMB Circular A-11, Section 53, authorizes the CIO as the person responsible for developing and maintaining the IRM Strategic Plan. It also requires that the IRM Strategic Plan be submitted together with the Department’s IT budget request.

2 IRM Goals (AXXA)

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 necessary to achieve the CIO’s objective.

The three goals defined in the IRM Strategic Plan are:

1. **Portfolio Alignment** – Ensure that the IT investment portfolio supports the Department’s business mission objectives while delivering business value
2. **Technology Services** – Orient OCIO as a provider of technology-based business solutions including infrastructure services
3. **Information and Technology Management** – Ensure effectiveness of the IT portfolio by fostering innovation, increasing IT portfolio value, and enhancing cyber security

Figure 1: IRM Strategic Plan Goals





3 Goal One: Portfolio Alignment (AXXB)

Goal One of the Department’s IRM Strategy is to ensure that the IT investment portfolio supports the Department’s business mission objectives while delivering business value. 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 mission.

3.1.1 Department Strategic Plan (AXXA)

OCIO’s technology goals are to support the achievement of the Department mission and strategic performance goals and objectives for 2011 – 2014.

The **Department of Education’s mission** is:

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

The Department’s Strategic Plan 2011-2014 embodies six Department of Education strategic goals:

Table 1: Department of Education Strategic Goals

Goal One:	Postsecondary Education, Career and Technical Education, and Adult Education: Increase college access, quality, and completion by improving higher education and lifelong learning opportunities for youth and adults.
Goal Two:	Elementary and Secondary: Prepare all elementary and secondary students for college and career by improving the education system’s ability to consistently deliver excellent classroom instruction with rigorous academic standards while providing effective support services.
Goal Three:	Early Learning: Improve the health, social-emotional, and cognitive outcomes for all children from birth through 3rd grade, so that all children, particularly those with high needs, are on track for graduating from high school college- and career-ready.
Goal Four:	Equity: Ensure and promote effective educational opportunities and safe and healthy learning environments for all students regardless of race, ethnicity, national origin, age, sex, sexual orientation, gender identity, disability, language, and socioeconomic status.
Goal Five:	Continuous Improvement of the U.S. Education System: Enhance the education system’s ability to continuously improve through better and more widespread use of data, research and evaluation, transparency, innovation, and technology.



US Department of Education
Office of the Chief Information Officer

Goal Six: U.S. Department of Education Capacity: Improve the organizational capacities of the Department to implement this Strategic Plan.

Source: U.S. Department of Education Strategic Plan 2011-2014

The Department’s Strategic Goals are articulated through Strategic Objectives. The Department’s Strategic Objectives are depicted in the following Table.

Table 2: Department of Education Strategic Goals and Strategic Objectives

Strategic Goals	Strategic Objectives
<p>Goal One: Postsecondary Education, Career and Technical Education, and Adult Education. Increase college access, quality, and completion by improving higher education and lifelong learning opportunities for youth and adults.</p>	<p>Sub-goal 1.1: Access. Close the opportunity gap by improving the affordability of and access to college and workforce training, especially for low-income students, first-generation college students, individuals with disabilities, and other chronically underrepresented populations.</p> <p>Sub-Goal 1.2: Quality. Foster institutional quality, accountability, and transparency to ensure that postsecondary education credentials represent effective preparation for students to excel in a global society and a changing economy.</p> <p>Sub-Goal 1.3: Completion. Increase degree and certificate completion and job placement in high-need and high-skilled areas (especially Science, Technology, Engineering and Mathematics [STEM]), particularly among underrepresented and economically disadvantaged populations.</p>
<p>Goal Two: Elementary and Secondary. Prepare all elementary and secondary students for college and career by improving the education system’s ability to consistently deliver excellent classroom instruction with rigorous academic standards while providing effective support services</p>	<p>Sub-Goal 2.1: Standards and Assessments. Support state-led efforts to develop and adopt college- and career-ready, internationally benchmarked standards, with aligned, valid, and reliable assessments.</p> <p>Sub-Goal 2.2: Great Teachers and Great Leaders. Improve the preparation, recruitment, development, support, evaluation, and recognition of effective teachers, principals, and administrators.</p> <p>Sub-Goal 2.3: School Climate and Community. Increase the success, safety, and health of students, particularly in high-need schools and communities.</p> <p>Sub-Goal 2.4: Struggling Schools. Support states and districts in turning around the nation’s persistently lowest-achieving schools.</p> <p>Sub-Goal 2.5: Science, Technology, Engineering, and Mathematics. Increase access to and excellence in STEM for all students and prepare the next generation for careers in STEM-related fields.</p>
<p>Goal Three: Early Learning. Improve the health, social-emotional, and cognitive outcomes for all children from birth through 3rd grade, so that all children, particularly those with high needs, are on track for graduating from high school college- and career-ready.</p>	<p>Sub-Goal 3.1: Access. Increase access to high-quality early learning programs and comprehensive services, especially for children with high needs.</p> <p>Sub-Goal 3.2: Workforce. Improve the quality and effectiveness of the early learning workforce so that early childhood educators have the skills and abilities necessary to improve young children’s health, social-emotional, and cognitive outcomes.</p> <p>Sub-Goal 3.3: Assessment and Accountability. Improve the capacity of states and early learning programs to develop and implement comprehensive early learning assessment systems</p>



US Department of Education
Office of the Chief Information Officer

Strategic Goals	Strategic Objectives
<p>Goal Four: Equity. Ensure and promote effective educational opportunities and safe and healthy learning environments for all students regardless of race, ethnicity, national origin, age, sex, sexual orientation, gender identity, disability, language, and socioeconomic status</p>	<p>Sub-Goal 4.1: Continue to Increase the Infusion of Equity Throughout the Department’s Programs and Activities. Promote and coordinate equity- focused efforts in Departmental programs.</p> <p>Sub-Goal 4.2: Civil Rights Enforcement. Ensure equal access to education and promote educational excellence throughout the nation through the vigorous enforcement of civil rights laws.</p>
<p>Goal Five: Continuous Improvement of the U.S. Education System. Enhance the education system’s ability to continuously improve through better and more widespread use of data, research and evaluation, transparency, innovation, and technology</p>	<p>Sub-Goal 5.1: Data Systems. Facilitate the development of interoperable longitudinal data systems from early learning through the workforce to enable data-driven decision-making by increasing access to timely, reliable, and high-value data.</p> <p>Sub-Goal 5.2: Research and Evaluation. Support multiple approaches to research and evaluation to support educational improvement and Department decision-making.</p> <p>Sub-Goal 5.3: Transparency. Present relevant and reliable information that increases demand for educational attainment and improves educational performance, while maintaining student privacy.</p> <p>Sub-Goal 5.4: Technology and Innovation. Accelerate the development and broad adoption of new, effective programs, processes, and strategies, including education technology</p>
<p>Goal Six: U.S. Department of Education Capacity. Improve the organizational capacities of the Department to implement this Strategic Plan</p>	<p>Sub-Goal 6.1: Effective Workforce. Continue to build a high-performing, skilled workforce within the Department.</p> <p>Sub-Goal 6.2: Programmatic Risk Management. Improve the Department’s program efficacy through comprehensive risk management and grant monitoring.</p> <p>Sub-Goal 6.3: Implementation and Support. Build Department capacity to support states’ and other grantees’ implementation of reforms that result in improved outcomes for students.</p> <p>Sub-Goal 6.4: Productivity and Performance Management. Improve workforce productivity through information technology and performance management systems.</p>

Source: U.S. Department of Education Strategic Plan 2011-2014

3.1.2 Segment Architecture

The OCIO’s Enterprise Architecture Program Office (EAPO) developed a Segment Architecture approach to align the IT portfolio to the Departmental strategic goals.

The EA Program Office, in accordance with the FEA practice guidance, identified business units that support common missions and 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 13 segments in the following table.



US Department of Education
Office of the Chief Information Officer

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	Ensure that policies mandated by the Department and by Federal law are being carried out	Core Mission
Evaluation & Policy Analysis	Assess 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	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	Distribute 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
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	Manage and deliver 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 EAPO 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 in the following figure.



Figure 2: Segment Alignment to Department Strategic Goals

Lines of Business (LoB)	Goal 1: Postsecondary Education, Career and Technical Education, and Adult Education	Goal 2: Elementary and Secondary	Goal 3: Early Learning	Goal 4: Equity	Goal 5: Continuous Improvement of the U.S. Education System	Goal 6: U.S. Department of Education 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						

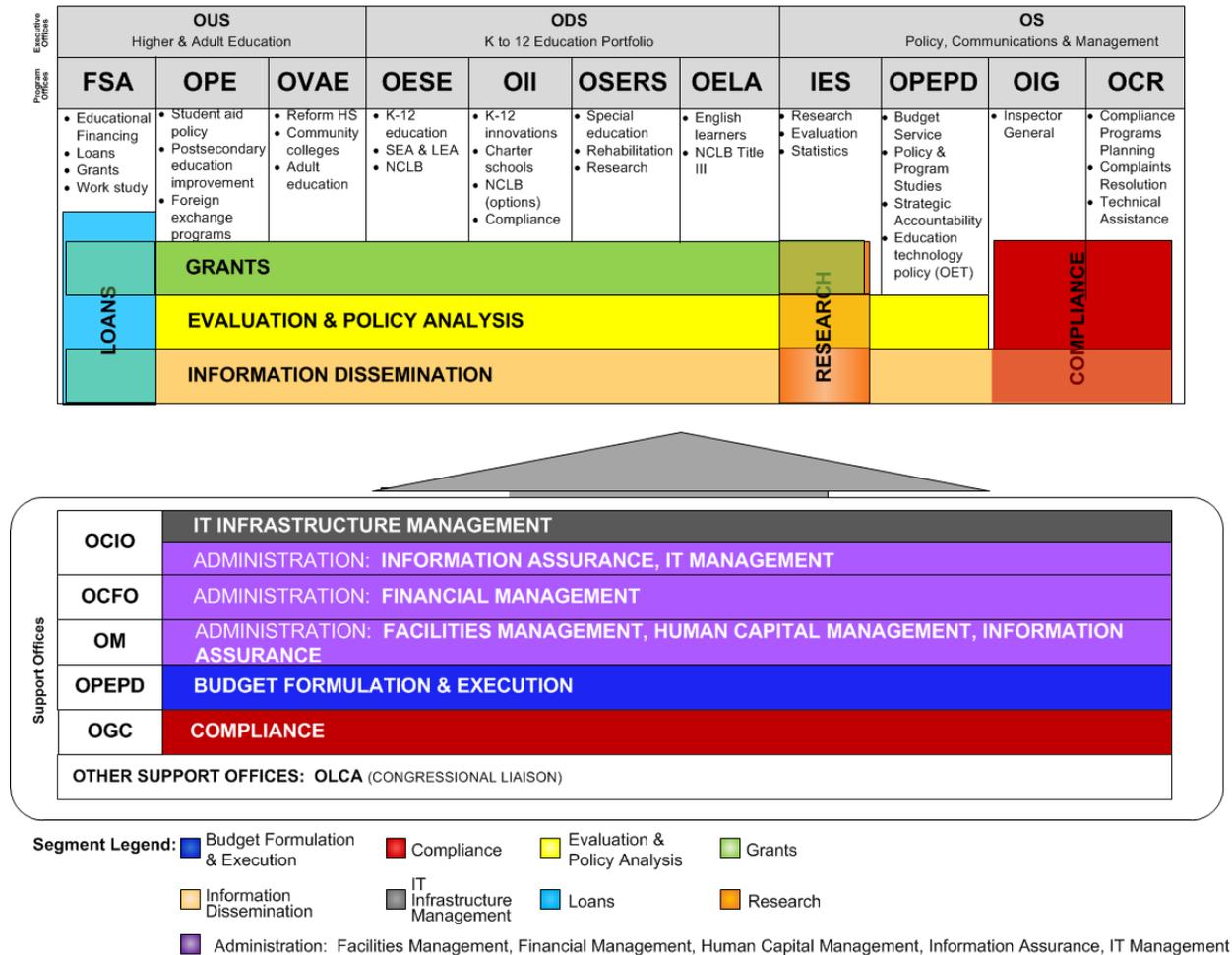
Aligning the segments to the Department mission sets the direction of the segments’ business and investment decisions.

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

The following figure 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.

3.1.3 Value Measurement Methodology (VMM) (CXXC) (CXXD) (CXXE)

The VMM is the process that is used to assess the relative value of the Department’s IT investments. The VMM applies a numerical scale to the Department’s mission priorities, value drivers and performance metrics to assign a value score to each of the Department’s IT investments. The VMM value score is combined with other rating factors such as the CIO ratings and Planning and Investment Review Working Group (PIRWG) select score to make funding and management decisions about the Department’s IT investment portfolio.

The PIRWG uses the VMM in the portfolio selection process to make funding recommendations about IT investments and IT investment opportunities. The segment owners of the Department’s lines of business (LOB) use VMM to make IT investment planning decisions and determine their priority and



funding recommendations to the PIRWG about those IT investments. The VMM also helps the Department identify opportunities for investment consolidation and/or termination, thereby increasing the efficiency of IT services and resource utilization by the Department.

3.2 Federal Alignment (BXXA) (BXXB) (BXXC)

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

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

- Digital Government Strategy
- 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

On May 23, 2012, the White House released its strategy for digital government, "Building a 21st Century Platform to Better Serve the American People." The strategy has three primary objectives:

1. Enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device
2. Ensure that as the government adjusts to this new digital world, we seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways
3. Unlock the power of government data to spur innovation across our Nation and improve the quality of services for the American people

Four overarching principals drive this digital government transformation:

1. An "**Information-Centric**" approach – Transforming from managing "documents" to managing discrete pieces of open data and content, which can be tagged, shared, secured, mashed up and presented in the way that is most useful
2. A "**Shared Platform**" approach – Enables the government to work together, both within and across agencies, to reduce costs, streamline development, apply consistent standards, and ensure consistency in how the Department creates and delivers information
3. A "**Customer-Centric**" approach – Influences how data is created, managed, and presented through websites, mobile applications, raw data sets, and other modes of delivery, and allows customers to shape, share and consume information, whenever and however they want it
4. A platform of "**Security and Privacy**" – Ensures this innovation happens in a way that ensures the safe and secure delivery and use of digital services to protect information and privacy



US Department of Education
Office of the Chief Information Officer

The Department is committed to supporting the digital government strategy through the engagement in the action plan presented in the following table.

Digital Government Strategy Principal	Departmental Action Plan Activity	Time Frame		
		3 months	6 months	12 months
Information Centric Approach	Engage with customers to identify at least two existing major customer-facing services that contain high-value data or content as first-move candidates to make compliant with new open data, content, and web API policy	x		
	Make open data, content, and web APIs the new default by ensuring all new IT systems follow the open data policy and operationalize ED.gov and developer pages		x	
	Make high-value data and content in at least two existing major customer-facing systems available through web APIs, apply metadata tagging and publish a plan to transition additional high-value systems			x
Shared Platform Approach	Establish an agency-wide governance structure for developing and delivering digital services	x		
	Develop an enterprise-wide inventory of mobile devices and wireless service contracts		x	
	Evaluate the government-wide contract vehicles in the alternatives analysis for all new mobile-related procurement			x
Customer Centric Approach	Engage with customers to identify at least two existing priority customer-facing services to optimize for mobile use	x		
	Ensure all new digital services follow digital services and customer experience improvement guidelines (within six months of the guidelines release date)		x	
	Optimize at least two existing priority customer-facing services for mobile use and publish a plan for improving additional existing services (within six months of released guidance)			x
	Implement performance and customer satisfaction measuring tools on all government websites (within three months of released guidance)		x	
Platform of Security and Privacy	(Via CIO Council) Evaluate opportunities to accelerate the secure adoption of mobile technologies into the federal environment at reduced cost		x	
	(Via CIO Council) Develop guidelines for standardized implementation of digital privacy controls and educate agency privacy and legal officials on options for addressing digital privacy, records retention, and security issues		x	



3.2.1 Digital Government Strategy (GXXA)

Implementing the Digital Government Strategy

The Department of Education's approach to the Digital Government Strategy focuses on:

- Better serving the Department's customers
- Sharing ideas, solutions, and best practices across the Department
- Offering more cohesive processes for the delivery of digital services
- Ensuring cost effective delivery of services
- Ensuring digital services provide value
- Reducing redundancies in digital services and data collections across the Department

The Department's Data Strategy Team (DST) is conducting an inventory of all public and restricted datasets, and is studying ways to build more coordinated policies and processes for data collection and release throughout the information life cycle across the Department. The DST is establishing a Disclosure Review Board to be led by the Department's Chief Privacy Officer. The Department's Digital Government Strategy working group plans to propose revisions to the Department's Lifecycle Directive Framework (OCIO 1-106) policy document and to standard language for contracts and statements of work to promote interoperability and data openness for new and renewed IT systems.

To further promote interoperability and openness, the Department of Education Office of Educational Technology, the White House, and the George Washington School of Business hosted a Data Jam in July 2012. This event brought together educational technology experts and entrepreneurs to brainstorm and commit to developing new products, services, and product features that utilize open data to improve student performance. This customer input will inform how the Department prioritizes making online systems and data more accessible through web APIs (Application Programming Interfaces). The purpose of the Data Jam was to prepare for a larger "Datapalooza" event which was held in October 2012 at the White House. Datapalooza provided an opportunity to highlight open educational data sets (education.data.gov), individual electronic student data (MyData), and data about learning content (LearningRegistry)--as well as tools and services that use these data to improve student choices around learning. Datapalooza was streamed live (and posted online afterward) for anyone who wanted to attend.

The Department engaged with the broader education community and other interested developers and entrepreneurs through social media outlets and the Department's official Homeroom Blog. For more than two weeks, blog visitors had the opportunity to comment on the blog post and provide feedback about services and data to open through web APIs. Representatives from the Department's OCIO, the Office of Communications and Outreach, and other key offices collected, analyzed, and synthesized the feedback from the blog and social media comments and incorporated public support for data more accessible through web APIs as a factor in how they prioritized the systems. The Department's White House Innovation Fellow is engaged in the Project Open Data initiative, and the Department plans to make its data inventory available as a JSON file and to manage its data publication workflow to be compatible with the new implementation approach for Data.gov.



3.2.1.1 Information Centric

3.2.1.1.1 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.

Open Data

The Department formed a DST composed of all the Department's offices that work with data collections to coordinate data-related policy activities within the Department. The DST established a number of working groups pertaining to various data-related initiatives within the Department, developing or redesigning policy, processes, and/or tools. Among them, DST established the Data Inventory Group (DIG), tasked with developing a database of information about all department-sponsored data collections that can be used to produce education statistics. The primary purpose of the database is to provide a centralized searchable source of background information about the Department's collections, with the goal of facilitating both internal and external awareness of available data, and increasing data use and coordination among current and future data collections.



DIG members met first as a group and then worked via email to determine the type of background information (metadata) to collect, and to identify the initial scope of the Group's product. DIG members agreed that as a starting point, any data collection that has an OMB clearance would be included in the inventory database, encompassing both Department-sponsored data collections and reporting requirements for Department-sponsored grants. The database is currently being populated using the electronic OMB clearance packages (i.e., those submitted for clearance since 2005). To date, metadata for 46 program areas, big and small (including EdFacts and many NCES studies), have been entered into the DIG database based on 269 OMB clearance packages. Program by program, the metadata are now being prepared for review by their respective program staff, after which their entries will be finalized. Work is also under way to supplement the background metadata with detailed variable lists for each data collection, and to transport the metadata into an outward-facing searchable data dictionary to increase public awareness of and access to the Department's data holdings. This functionality will be based on the Comprehensive Knowledge Archive Network (CKAN) platform.

3.2.1.1.2 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 increased access to high value, machine readable datasets so that they can easily find, download, and use information generated by the Department.

3.2.1.2 Shared Platform

3.2.1.2.1 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 adopting cloud computing technologies whenever a secure, reliable, cost-effective cloud option exists in compliance with the following guidance and regulations:

- Federal Chief Information Officers Council (FCIOC) Privacy Committee, Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies, August 2010
- 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
- The Federal Risk and Authorization Management Program (FedRAMP)
- Department of Education Cloud Computing Security Guidance, DRAFT, January 18, 2012

3.2.1.2.2 Shared Services

The Department's shared services strategy addresses the [Federal Information Technology Shared Services Strategy](#), which provides policy guidance on the full range and lifecycle of intra- and inter-agency IT shared services. This strategy is part of the OMB "25-Point Implementation Plan to Reform Federal IT Management," which seeks to increase return on investment, eliminate waste and duplication, and improve the effectiveness of IT solutions. The approach is commonly referred to as the "Shared-First" strategy.

The Department's shared service plan also seeks to comply with the following guidance:

- OMB Memorandum M-11-29, Chief Information Officer Authorities, August 8, 2012
- OMB Memorandum M-12-10, Implementing PortfolioStat, March 30, 2012

Please see Section 4.2.3 for more information on the Department's shared services activities.

3.2.1.3 Customer Centric

3.2.1.3.1 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 the Department's efforts to improve customer relationships and the customer experience by delivering faster and better services to the public while reducing costs. The Department has undertaken two new ventures to enhance its customer experience:

1. Integrated Student Experience (ISE): Customer Engagement and Future Enhancements.



In FY12, the Department launched the ISE initiative to establish an integrated, customer-focused web experience for students, parents, and borrowers to facilitate decision-making about funding a postsecondary education. The ISE initiative provides students and parents with an enhanced customer experience across the student aid lifecycle, with the goal of increasing financial aid awareness and college attendance, while simplifying the application and servicing processes. The Department also announced a new, streamlined website and several social media tools that will make it easier for students and families to navigate the financial aid process and make informed decisions about paying for college. StudentAid.gov is the initial step in a multi-phase project to offer a “one-stop shop” where consumers can access federal student aid information, apply for federal aid, repay student loans, and navigate the college decision-making process. Available in English and Spanish and fully accessible on smartphones and tablets, the website combines content and interactive tools from several web sites and features instructional videos and info-graphics to help answer frequent questions about financial aid. Also, the Department has revamped its federal student aid-related social media sites, including Facebook (<http://www.facebook.com/FederalStudentAid>), Twitter (<http://twitter.com/FAFSA>), and YouTube (<http://www.youtube.com/federalstudentaid>), to provide more options for students to learn about student aid.

The following elements characterize the scope of the Department’s planned enhancements in FY13 and FY14:

- Continued enhancements and improvements are planned based on user feedback through surveys, usability testing and focus groups.
- The Department is currently building Phase II version 1.0, which will be a presentation front onto the National Student Loan Data System (NSLDS) information allowing customers fast, easy access to their loan data.
- During subsequent phases, StudentAid.gov will offer a single view of transactional tools, such as loan status, entrance and exit counseling and other processes needed throughout the financial aid lifecycle.
- Other planned improvements include continuing to consolidate and streamline content and functionality from the Department’s other key websites.
- The Department also plans to offer a career and scholarship search tool, as these are known important components to the college preparation process.
- \$1.6M in cost saving has been identified to date for retiring websites; the continued consolidation of websites under Phase II and future phases is expected to result in additional significant cost savings for the Department.

2. ED and the IRS Partnership Alliance.

In support of the President’s 2020 goal to have the highest proportion in the world of students graduating from college, the Department recently signed a Memorandum of Understanding (MOU) with the IRS for reciprocal efforts to promote services to each organization’s customer base. The IRS’s primary goal in establishing this collaboration is to actively communicate service options that bring value to taxpayers and the IRS, and to increase awareness and use of them. In particular, the IRS is seeking to



further grow the Volunteer Income Tax Assistance (VITA) and the Tax Counseling for the Elderly (TCE) Programs, which offer free tax help for taxpayers who qualify. The Department's benefit is increased awareness of federal student aid programs and expanded access to the federal student aid application, as they remain critical elements in accomplishing the President's 2020 Goal. The partnership will focus on expanding current options and seeking new avenues to provide individuals in low-income communities with information, assistance, and access to relevant IRS services and relevant federal student aid services. An evaluation component to monitor success of partnership will also be included.

The Department will help the IRS generate greater awareness and use of the VITA and TCE programs. An initial action item will involve a broadcast email communication to recent Free Application for Federal Student Aid (FAFSA) filers regarding the free tax preparation services available through the IRS. Characteristics of the target population are:

- '12-'13 FAFSA filers
- Independent student with email address
- Tax return status of Completed or Will File with an AGI of less than \$25,000

This should be accomplished by the mid-February timeframe. The Department estimates the email volume to be around 4-5 million.

3.2.1.3.2 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 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 outlines the agency's electronic stewardship programs and complies 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

Please see Section 4.2.7 for more information on electronic stewardship.



3.2.1.4 *Security and Privacy* (EXXA)

3.2.1.4.1 Homeland Security Presidential Directive (HSPD) 12

The Federal government established the 2004 mandate for 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. Agency 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 4.2.5.1 for more information on the Department's HSPD-12 activities.

3.2.1.4.2 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.

3.2.1.4.3 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 reduces vulnerabilities to the Department's physical and logical assets.



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.

3.2.1.4.4 Two-Factor Authentication

To improve the security and protect the assets of the Department, all employees and contractors are required to access authorized Department 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.

3.2.1.4.5 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 Memorandum M-08-05, Implementation of Trusted Internet Connections
- OMB Memorandum M-08-16, Guidance for Trusted Internet Connection Statement of Capability Form
- OMB Memorandum M-08-26, Transition from FTS2001 to NETWORKX



- OMB Memorandum M-08-27, Guidance for Trusted Internet Connection Compliance
- OMB Memorandum M-09-32, Update on the Trusted Internet Connections Initiative

Please see Section 4.2.5.2 for more information on the Department's TIC activities.

3.2.1.4.6 Internet Protocol Version 6 (IPv6)

Internet protocols (IPs) specify communication and interoperability rules on the Internet and on other IP networks. 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. 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

The Department developed an IPv6 Transition Guide, which describes the Department's policies and activities to meet the Federal IPv6 requirements. The Department's IPv6 Transition Manager and IPv6 Working Group have met the FY2012 external application compliance milestones and are making steady progress on FY2014 internal application compliance milestones.

Please see Section 4.2.6 for more information on the Department's IPv6 activities.

3.2.2 Federal 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 has achieved its data center consolidation target, completed an inventory of its data centers and related assets, and completed its targets of consolidation to two data centers.



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

4 Goal Two: Technology Services (AXXB) (CXXG)

Goal Two is to orient OCIO as a provider of technology-based business solutions including infrastructure services. OCIO provides a broad range of IT services to address the current and future business needs of the Department. OCIO is committed to modernizing the Department with innovative technology that will provide future cost savings and performance improvements in meeting the agency mission and strategic goals.

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

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 and enhance staff productivity
- **Reduce costs** for IT service delivery by standardizing software and hardware platforms

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

OCIO's role is to provide a stable technology infrastructure to support the business requirements of the Department. 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.

OCIO will continue the delivery of common IT resources, such as hardware, software, networks, and other services that support program offices business needs. OCIO will continue delivery of the following supportive technologies during the FY 2013 - FY 2016 IRM Strategic Plan.



Table 4: Current Delivery of Services

Hardware
Assistive technologies
Hardware infrastructure maintenance and upgrade
Software
Assistive technologies
Data Analytics
Data Management
Desktop Operating System – Upgrade to Windows 7
Email, Messaging, and Collaboration
Office Productivity Tools – Microsoft Office Suite 2010
Voice and Data
Network
Data Center
Data Warehouse
DNS SEC
Intranet
IPv4/ 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 OCIO delivers these common IT products and services to maintain a stable technology platform, it 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, OCIO's role will evolve to provide a broader set of technology services to the Department. This future direction will position OCIO to become a provider of enterprise common services beyond the current technical infrastructure.

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 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.

Management Structure for Future Services

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

- Establish an effective product and service delivery model
- Implement an effective governance model
- Support the programs to develop a funding strategy
- Provide IT services to the Department

The service delivery model for shared services will be based on the following set of guiding principles for 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 of 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 customer 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

4.2.1 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 services and IT infrastructure to create the business value of tomorrow.

It is the CIO's role to recognize and implement IT 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.

4.2.1.1 Access Anywhere Computing

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

Improved Performance

- Leverage 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 of people from both inside and outside of the Department, 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 employee-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
 - smart phones
 - desktops

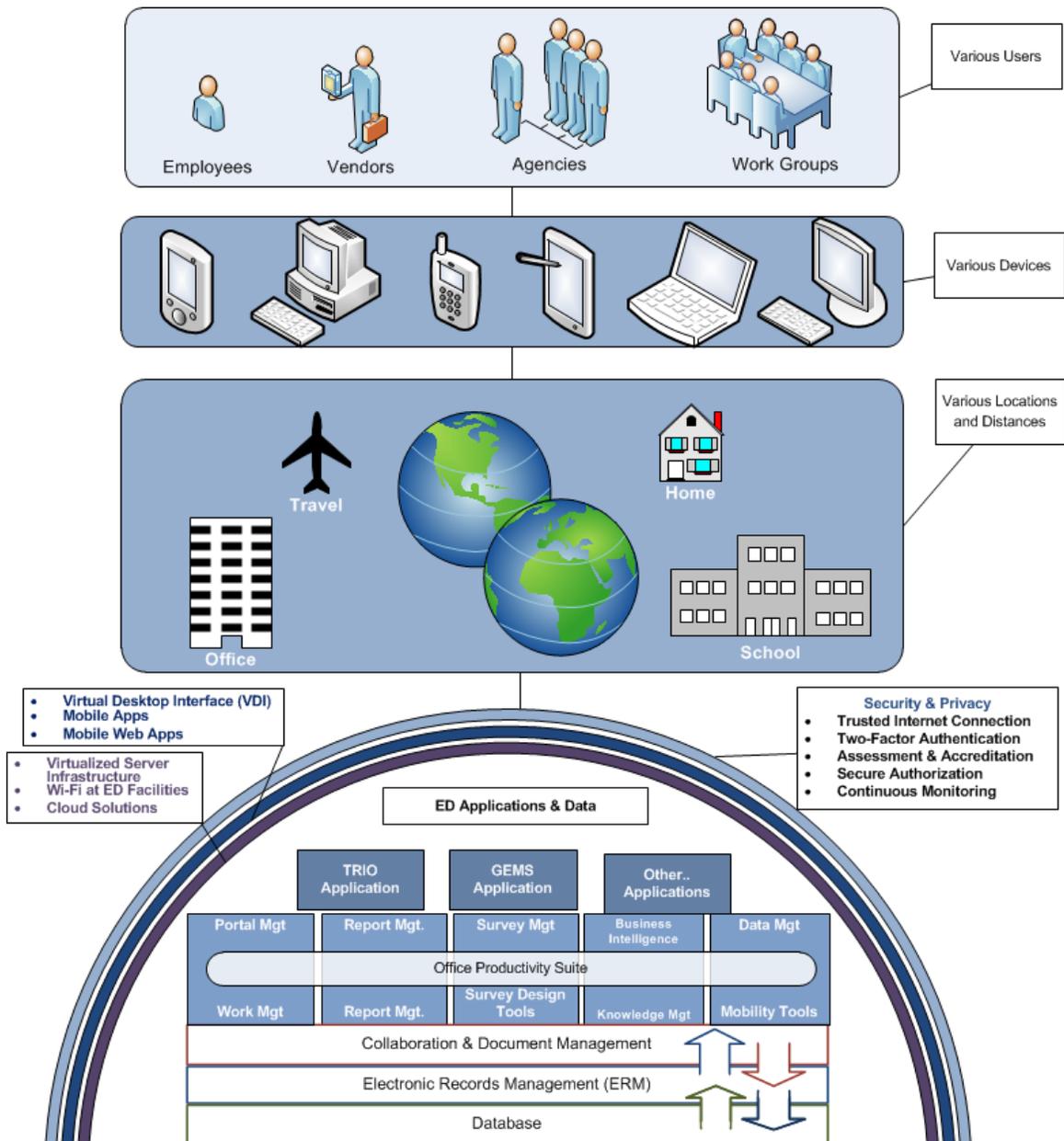


US Department of Education
Office of the Chief Information Officer

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 4: The Department’s Access Anywhere Model





4.2.1.2 OCIO Support Services

To support the CIO's innovation agenda, OCIO offers the Department's business customers the following three technology support services:

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

IT Governance and Planning Services help program offices align their business priorities with enabling IT capabilities that support accomplishing the mission of both the Principal Offices and the Department. These services could include:

- Governance services that validate the requirements, design, implementation and performance for IT projects and/or the application of Common Enabling Services (CES) (e.g., workflow and collaboration tools) that solve specific business needs
- 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 office
 - 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

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:

- Develop detailed plans and product recommendations for various types of CES's
- Support 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
- Develop 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: 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

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.

4.2.2 Common Enabling Services (CES)

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 Enabling Services

Requested Service	Definition
Collaboration Management	Allow people to work together more efficiently by enabling greater information sharing
Data Analytics	Support the identification, gathering, and transformation of documents, reports, and other sources into meaningful information
Data Management	Usage, processing, and general administration of unstructured information
Electronic Document/Record/ Content Management	Control the capture and maintenance of an organization’s documents and files
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



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. OCIO will continue to expand the use of the collaboration platform during FY 2013 – 2016.

Data Analytics tools will allow many segments to access their reports and analysis from anywhere. For example, grants administrators may want to monitor a grant, or a lawyer may want to examine a case from anywhere.

Collaboration management tools will allow Department employees 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.

An electronic document/record/content management solution will allow 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 following **proposed enterprise technology platform** diagram 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 5: Proposed Enterprise Technology Platform

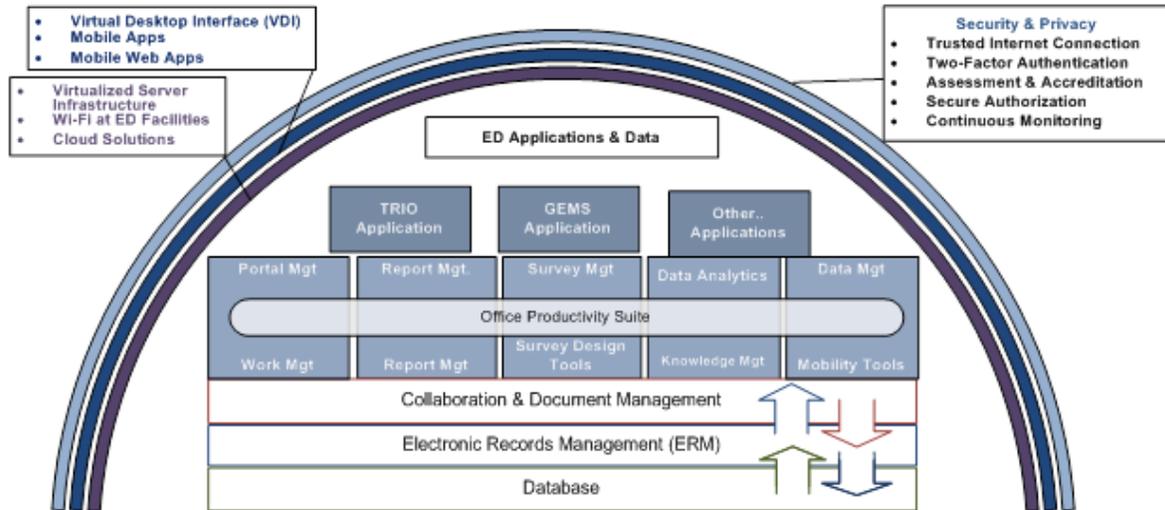


Table 6: Proposed Technology Solutions

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



4.2.3 Commodity IT and Shared Services

4.2.3.1 *Maturing the IT portfolio* (HXXA)

As part of the EA Roadmap, the Department has sought to optimize its IT infrastructure while operating an IT service management framework (primarily based on ITIL standards). The need for consolidation and use of shared services is identified through the segment modernization planning process. Modernization planning is an ongoing process, which uses performance objectives and business needs to determine if new investments or existing services should be utilized to meet the Department's business needs. During annual segment modernization planning, the segment owners review their line of business (LoB).

During annual segment modernization planning, each segment determines its required capabilities (currently met and unmet by existing investments) to achieve the segment's performance goals. The EAPO groups these needed capabilities into 18 common services. Additional details are provided in the Enterprise Modernization Roadmap.

4.2.3.2 *Use of savings resulting from consolidations of Commodity IT* (HXXB)

To date, the Department has successfully consolidated many enterprise services through the EDUCATE and Virtual Data Center (VDC) investments for (a) IT infrastructure; (b) Enterprise IT Systems; and (c) Business Systems. Moving forward, the Department has identified the following two major areas for consolidation:

- Web Hosting, Infrastructure, and Content Management (Enterprise IT Systems)
- Grants-Related Federal Financial Assistance (Business Systems, for details, see the Commodity IT Consolidation Plan, an appendix of the Enterprise Modernization Roadmap)

The Department plans to use the savings obtained from using commodity IT to invest in performance-enhancing innovations within the Department. The Department is investing heavily in consolidation-related activities and is still in the nascent phase of grants consolidation and web-hosting consolidation. Additional details are provided in the Commodity IT Consolidation Plan section of the Enterprise Modernization Roadmap.

4.2.3.3 *Maximizing use of inter- and intra-agency shared services* (HXXC)

Growing mission requirements in an environment of declining resources drives the Department to find innovative solutions to meet its needs. Shared IT services enable the Department to improve services and reduce overall costs, especially in areas of commodity IT, such as human resources, financial management, infrastructure, and business systems.

The Department aligns itself with the Federal Information Technology Shared Services Strategy, also known as the *shared-first* approach. The shared-first approach aims to:

- Improve return on investment across the Department's entire IT portfolio through the coordinated use of portfolio reviews and commodity IT system and services consolidation
- Close productivity gaps by implementing integrated governance processes and innovative IT service solutions



- Increase communications with stakeholders as shared service managing partners, customers, and providers in the full lifecycle of IT shared service activities

Each system developed within the Department is reviewed by the Investment Review Board (IRB) for adherence to our IT value management and IT investment strategy. It is also reviewed by the Enterprise Architecture Review Board (EARB) for conformance with EA to ensure compliance with our technical standards, reduce the potential of acquiring duplicative investments and driving business value for IT investments.

As one of the smallest Cabinet-level agencies, the Department has historically operated an intra-agency shared IT services model for IT infrastructure, email services, office automation, networking, telecommunications and multimedia. Throughout its history, the Department has also leveraged the products and services hosted by other agencies in lieu of maintaining Department systems for these services to drive cost efficiencies at the Department and Federal level. Most recently in October 2012, the Department moved from its internally hosted and developed “information collection” system to the Health and Human Services (HHS) <http://www.paperworkreduction.gov> portal for these services.

4.2.3.4 Continuity of operation for mission critical applications (EXXB)

Each system developed within the Department is reviewed by the EARB for adherence to numerous requirements, including continuity of operation and disaster recovery capabilities, consistent with documented Lifecycle Management Methodologies in Department directives and other Federal and Department regulations. In addition, the FISMA security authorization process evaluates systems as low, medium or high with respect to confidentiality, integrity and availability. Based on that analysis, applicable NIST Special Publication 800-53 controls will be required to provide a level of continuity of government operations.

4.2.4 Cloud Computing

The purpose of the Federal Cloud First policy is to move toward a more reliable, efficient, and innovative government. 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.

OCIO will publish Cloud Computing Security Guidance to ensure the use of cloud services is managed in accordance with 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 FY 2013 - FY2016 IRM Strategic Plan, OCIO plans to provide the following cloud computing services:

Infrastructure-as-a-Service (IaaS): The Department will provide fundamental computing resources such as processing, storage and networks so that Department users can deploy and run software, 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 platform based computing solution on the cloud consisting of specific operating systems, applications software and development tools; that will be available via the Web. PaaS will improve the management and procurement of IT systems development capabilities.

Software-as-a-Service (SaaS): The Department will migrate some of 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 on 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 Cloud Services¹

Service	Service Model	Deployment Model
<p>Survey Services</p> <p>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.</p>	SaaS	Public Cloud
<p>Agency Private Cloud Services</p> <p>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.</p>	IaaS/ PaaS	Private Cloud

¹ Source: U.S. Department of Education Data Center Consolidation Plan



Service	Service Model	Deployment Model
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+ 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

4.2.5 Cybersecurity Initiatives (EXXA)

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

- HSPD-12
- TIC
- Continuous Monitoring

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

4.2.5.1 Homeland Security Presidential Directive-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’s goals in the integration of HSPD-12 are to reduce identity fraud, protect personal privacy, enhance security and increase efficiency.

In order to meet the requirements of HSPD-12, M-11-11, and Federal mandates for Identity, Credential, and Access Management (ICAM), the Department developed an Enterprise Strategy that defined policy,



process, and technology requirements and a corresponding capability roadmap to meet specific targets to include the establishment of an Enterprise Identity Management (IDM) Solution. Part of this Enterprise IDM solution is an enterprise-wide authentication service or enterprise single sign on (eSSO).

To establish an eSSO capability for the enterprise, the Department will conduct an analysis of alternatives that will consider:

- Acquiring and establishing an enterprise solution for the Department
- Leveraging an existing Department solution and expanding for enterprise-wide use

The project will consider the following approaches for existing and new information systems to leverage an eSSO solution:

- Decentralized Federated – applications consuming credentials published by eSSO through secure channels
- Centralized Tight Integration – applications customized/configured to use components of eSSO
- Hybrid – a combination of applications consuming credentials published by eSSO (Federated Approach) and components provided by eSSO (Tight Integration)

The Department will continue to focus on the implementation of the FISMA priorities of TIC, 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 its PIV authentication usage by 59 percent 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

4.2.5.2 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 Connection 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 as protection from viruses and worms. Through proper handling of inbound and outbound email and implementing



US Department of Education
Office of the Chief Information Officer

quarantine and junk mail filters, the Department minimizes other potential security issues via spear phishing attacks and the importing 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 the agency's 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 Department of Homeland Security (DHS) monitoring equipment, which will protect IT assets not housed within either EDUCATE or the VDC environs.

All external connections, as defined by OMB and the DHS, must have their network traffic pass through Einstein devices. The Einstein devices are monitored and managed by DHS and serve as a monitoring tool to detect malicious activity. This includes all Internet connections, MPLS connections, out-of-band management connections, remote access connections (VPN and dial-in) and all site to-site VPN connections.

The Department intends to optimize its external connections and improve the Department's incident response capability through centralized gateway monitoring. By reducing the number of access points, the Department and DHS can more easily monitor and identify potentially malicious traffic. All external connections, as defined by OMB and DHS, must have their network connection's traffic pass through the EINSTEIN hardware. To comply with DHS and OMB requirements, the TIC initiative is focused on ensuring the Department implements requirements set forth in the TIC 1.0 and 2.0 reference architectures.



Table 8: TIC Milestones

FY 2012	FY 2013	FY 2014	FY 2015
<p>The Department Trusted Internet Connection (TIC) access point and supporting infrastructure in Plano, TX achieved 94% compliance with 51 TIC 1.0 critical capabilities required of single-service TICAPs</p>	<p>The Department will address specific TIC Reference Architecture 1.0 and 2.0 capability gaps; initiatives include:</p> <ul style="list-style-type: none"> • Deployment and transition to a Stratum Level 1 time source for both the VDC and EDUCATE networks • Development of policy, guidance, and processes to facilitate the consolidation of external connections • Planning and initiating activities to establish an alternate TIC at the FTC • Market research and pilot of a web application security solution 	<p>The Department will:</p> <ul style="list-style-type: none"> • Perform progressive transition of prioritized systems, with external connections, that are not currently routed through a TIC access point to a TIC access point • Complete alternate TIC site implementation • Implement a web application security solution • Plan for and initiate implementation of additional capabilities as required in response to new TICAP requirements or new federal mandates 	<p>The Department will:</p> <ul style="list-style-type: none"> • Continue transition of prioritized systems, with external connections, that are not currently routed through a TIC access point to a TIC access point • Plan for and initiate implementation of additional capabilities as required in response to new TICAP requirements or new federal mandates

4.2.5.3 Continuous Monitoring (CM)

OMB Memorandum M-11-33, FY 2011 Reporting Instructions for the FISMA and Agency Privacy Management, requires that all agencies develop a continuous monitoring program. The Department’s continuous monitoring program is based on a phased-in maturity model approach. The phases align with the Continuous Monitoring Maturity Model found in the Continuous Monitoring and Risk Scoring (CM/RS) Concept of Operations (CONOPS) for Supporting Cyber Security Operations, as developed by the DHS Federal Network Security Branch. The Department is currently assessed to be at Maturity Level II with the implementation of some automated scanning tools and SCAP-compliant products. From FY13 through FY15, this project will enable the transition from Levels III through V as described below.

Maturity Level III: Focuses on IT governance compliance. Reporting requirements specified in OMB M-11-33 include the following:

- **Asset Management.** Enable the Department to capture and establish a baseline of authorized IT assets (e.g., computing hardware, network devices, software)
- **Configuration Management.** Enable the Department to capture and establish a series of security configuration baselines based on agency-specified security configuration benchmarks such as CyberScope, SCAP data and Federal Desktop Core Configuration (FDCC), USG Configuration Baseline (USGCB), etc.
- **Vulnerability Management.** Enable the Department to associate known vulnerabilities to misconfigurations and missing patches.



Maturity Level IV: Focuses on continual situational awareness of operational effectiveness. Continues the implementation of tasks from Maturity Level III and includes specific tasks for Maturity Level IV:

- Development of a continuous monitoring data portal to aggregate and correlate data efficiently to:
 - De-conflict findings from different tools
 - Aggregate data in a common format for further processing and forensic purposes
 - Integrate and fuse findings and data to provide continually updated situational awareness
 - Visualize and generate reports for presentation to various tiers of the organization

Maturity Level V: Enriches the continuous monitoring program through innovative techniques that align security with Department business processes in order to anticipate and respond to change and risk by:

- Establishing and developing a governance, risk, and compliance tool that allows business units to work together using common processes and information. Centralized views into enterprise risk, automated and repeatable business processes, integrated systems, and information as well as flexibility to evolve as business needs change. This will help the Department become more agile, gain greater visibility into their data, and drive a trusted operational framework across the enterprise.
- Implementing tools to evaluate a range of decisions and score estimated outcomes to support decisions at all tiers of the Department and permit a common framework for intra/inter Departmental decisions.

4.2.6 IPv6

The Department's goal in transitioning to an IPv6 capable environment is to provide enhanced technology services that improve the Department's business performance and operational efficiency. IPv6 will enable the Department to support continued growth in users, devices and Internet-based functionality and services.

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

Through 2012, the Department successfully completed its required IPv6 transition activities for public, external-facing servers and services. These activities include:



- **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
- **October 2012:** All public/external server transitions have been completed

The Department's IPv6 goal for 2014 is to upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY14. Defining internal client applications that communicate with public Internet Servers means:

- Internal client applications refers to software running on computer systems within the Department that are originating connections as clients to other systems
- 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

Implementation of this goal would have the following impact:

- Native IPv6 will be enabled on EDUCATE Infrastructure
- The Department's Client PCs will have IPv6 Dual Stack enabled
- The Department's internal staff will be able to connect with externally hosted resources that are IPv6 only.



US Department of Education
Office of the Chief Information Officer

The following table represents the Department’s IPv6 transition activities for internally facing services:

Table 9: 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
	Infrastructure	Update Transition and Remediation Plans if necessary	Updated Transition, Remediation Plans	OCIO-ITS	8/30/2012
Remediation 9/2012 to 7/2013	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
	Application	Certify internal facing applications as IPv6 Operational	Test Plan results	Application Owner	8/30/2014
Implementation 9/2014	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

4.2.7 Electronic Stewardship

The purpose of the electronic stewardship program 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



5 Goal Three: Information and Technology Management (AXXB)

The IRM Strategic Plan's information and technology management goal is to ensure effectiveness of the Department's IT portfolio by fostering innovation, increasing IT portfolio value and enhancing cyber security.

5.1 IT Governance Structure (CXXA) (CXXB)

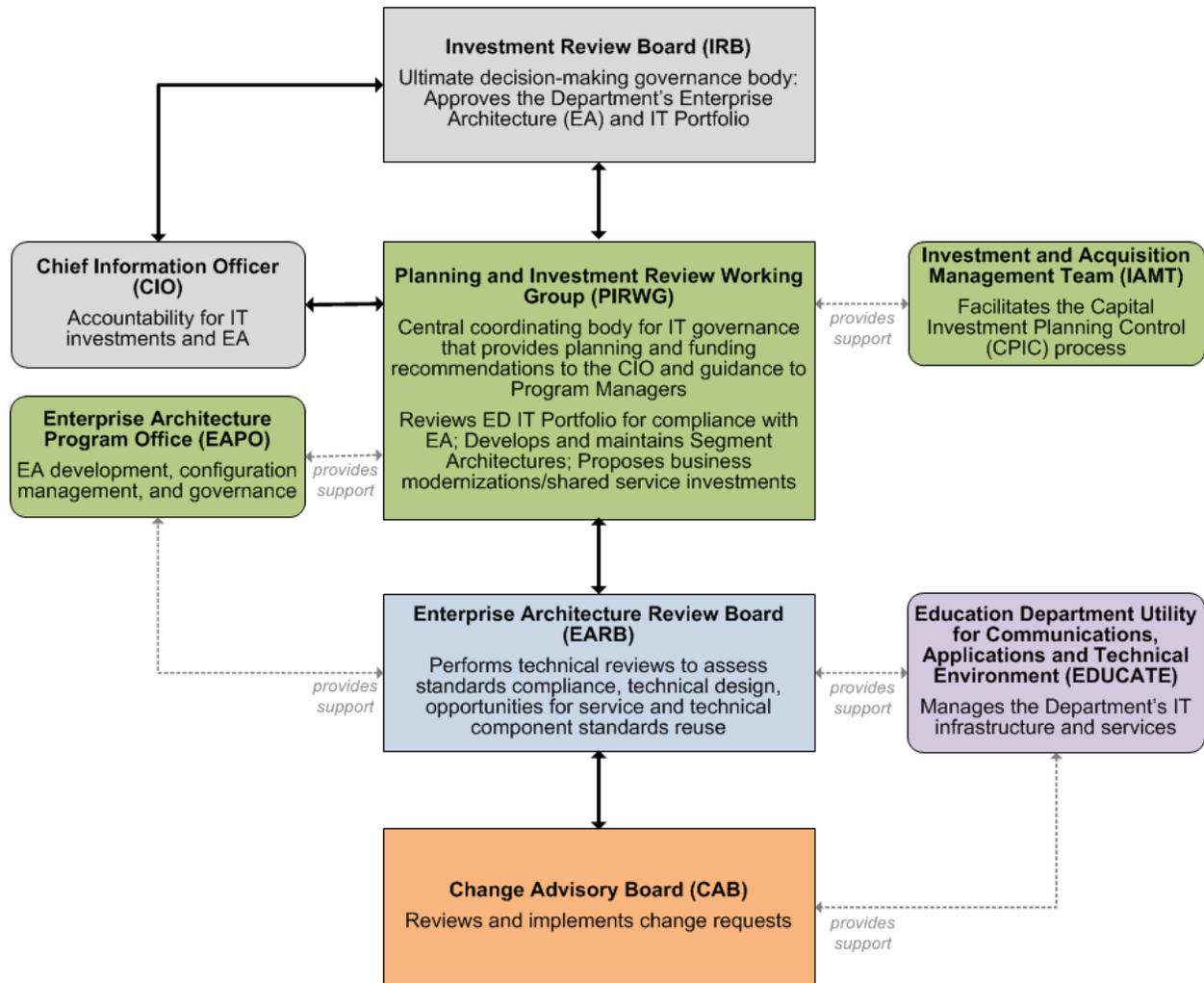
The stakeholders in the Department's IT governance structure determine IT management policies and plans directly impacting the Department's information resources management process.

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 2011-2014 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 the following figure.



Figure 6: The Governance Process at the Department



5.1.1 Enterprise Architecture Program Office (EAPO)

The EA 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 (a sub-component of PIRWG) and the EARB.

- **Enterprise Architecture Advisory Council (EAAC):** Provides support and guidance to the development of the Department EA and its IT needs and priorities
- **Enterprise Architecture Review Board (EARB):** Provides support to PIRWG 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 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 (CXXB)

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 and 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 provides a procurement career management program to ensure there is an adequate and professional acquisition work force at the Department. The Performance and Logistics Group, 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 ensure 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
- 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 Department programs

5.2.3 Information Assurance Services (IAS) (GXXB)

Information Assurance Services (IAS) oversees the Department's IT 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 technology and certification and accreditation. IAS 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 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 IT. 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



- **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, 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
- **Assistive 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 Capital Management (FXXA)

The Department's Human Capital and Client Services (HCCS) provides 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 Department 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.

5.2.6 Accessibility (IXXA) (IXXB) (IXXC)

Creating a diverse work environment for individuals of all abilities (IXXA)

A key aspect of creating a diverse environment where individuals of all abilities can work, interact, and develop into leaders involves meeting the statutory requirements of Sections 504 and 508 of the Rehabilitation Act of 1973. These sections of the Rehabilitation Act protect and enhance the civil rights of individuals with disabilities throughout the country and ensure equality of opportunity, comparable access and improved quality of life for these individuals.

Doing so involves the maintenance of a highly qualified, productive staff that has the tools it needs to perform its functions at its disposal. To ensure that staff with disabilities or impairments have the



technology that provides them equal opportunities to perform alongside their non-disabled colleagues, OCIO conducts needs assessments and provides subsequent recommendations to EDUCATE. The recommendations of OCIO are aimed at providing adequate IT-related, "reasonable accommodations" to those employees who have functional limitations that warrant the application of assistive technology solutions. Such solutions, which include special keyboards for individuals with repetitive strain injuries, screen readers and magnifiers for the visually impaired, video phones for the deaf and hard of hearing, etc., mitigate the specific functional limitations of those individuals, thereby increasing job performance and enhancing involvement in all aspects of work life.

Also key to the success of fulfilling the Department's mission for individuals with disabilities is to ensure that all Department staff and customers have full and equal access to information and information systems utilized by the Department to conduct mission-critical business. Here too, OCIO conducts accessibility reviews of all major software, web applications and sites to ensure that they properly meet the technical accessibility standards of Section 508 of the Rehabilitation Act.

To make certain that all disabled employees and customers have full and complete access to the Department's information and systems, OCIO reviews whether web pages are sufficiently labeled, multimedia is adequately captioned, software controls are accessible with both the keyboard and the mouse, and documents are properly tagged, containing good readable embedded text.

Integrating accessibility considerations into IT processes (IXXB)

OCIO conducts regular accessibility reviews of software and web applications and then includes results of these reviews as a regular part of the weekly EARB evaluation process for software acceptance.

In addition, OCIO reviews any work statements that contain IT-related procurements to ensure that language requiring Section 508 compliance is included in these SOWs. OCIO also maintains an Assistive Technology program, which houses the Section 508 Coordinator and 508 Compliance Testing Team. This team provides ongoing testing of web and software applications under consideration for procurement by the Department/EDUCATE. Additionally, it also provides technical assistance to any Department and vendor staff, upon request, to ensure that Section 508 concerns are properly considered and incorporated into the development and procurement processes. The team also provides assistance to the respective stakeholders on issues that do not meet the standards of Section 508 (i.e., technical standards interpretation, proper testing processes, equivalent facilitation, Section 508 exceptions and remediation strategies for web sites and software applications.)

OCIO, along with the Office of the Undersecretary and the Training and Development Center (TDC), also provides regular review, training and technical assistance on the development and remediation of Word, PDF, PowerPoint and Excel documents so that they meet the Department's requirements for accessible document design (published in 2012.) This accessibility enhancement initiative is aimed at meeting the Department's requirements for accessible design, and it continuously moves the Department toward the goal of ensuring that all documents posted on Department websites are accessible to and usable by individuals with disabilities.

Building upon the success of this endeavor, the Department is serving as a co-chair for a Community of Practice sponsored by the CIO Council Committee on Accessibility. This Community of Practice is



bringing together document accessibility experts from federal agencies to unify accessibility requirements for documents across all agencies, so that agencies will utilize the same set of requirements for their staff and vendors who must prepare documents for posting and dissemination.

Building workforce skills to support and enforce Section 508 requirements (IXXC)

Training on how to incorporate accessible document design into the day-to-day work process is currently being provided through the TDC on a regular basis to all Department staff. This is making a significant difference as an increasing number of documents produced by the POCs are being made accessible as a routine part of their production.

In addition, the Assistive Technology Team has held numerous training sessions for Department staff on a variety of topics, including the Section 508 standards, the document accessibility initiative, and accessible web design. The team has also conducted needs assessment awareness days, to familiarize staff with their rights to receive assistive technology, which will assist in reducing or eliminating functional limitations they experience in the workplace.

On a regular basis, the CIO meets with disabled Department staff and other interested persons to discuss new and innovative strategies in development that would increase the inclusion of individuals with disabilities in all IT-related Department processes. These meetings are also utilized to discuss specific pertinent issues experienced by staff with disabilities that need further attention and resolution by OCIO staff.



6 List of Figures

Figure 1: IRM Strategic Plan Goals	6
Figure 2: Segment Alignment to Department Strategic Goals.....	11
Figure 3: Principal Office and Segment Engagement.....	12
Figure 4: The Department’s Access Anywhere Model.....	29
Figure 5: Proposed Enterprise Technology Platform	33
Figure 6: The Governance Process at the Department.....	46

7 List of Tables

Table 1: Department of Education Strategic Goals.....	7
Table 2: Department of Education Strategic Goals and Strategic Objectives.....	8
Table 3: The Department’s 13 Segments.....	10
Table 4: Current Delivery of Services.....	25
Table 5: Common Enabling Services	31
Table 6: Proposed Technology Solutions	33
Table 7: Current Cloud Services	36
Table 8: TIC Milestones	40
Table 9: Internal IPv6 Transition Activities	43