Information Technology
in
Colorado State Government

August 2013

OFFICE OF THE
STATE AUDITOR

LEGISLATIVE AUDIT COMMITTEE
2013 MEMBERS

Representative Angela Williams
Chair

Senator Steve King
Vice-Chair

Senator Lucia Guzman
Senator Owen Hill
Representative Dan Nordberg
Representative Su Ryden
Representative Jerry Sonnenberg
Senator Lois Tochtrop

OFFICE OF THE STATE AUDITOR

Dianne E. Ray
State Auditor

Matt Devlin
Deputy State Auditor

Scott Collins
Legislative Audit Manager

Julie Chickillo
Legislative Auditor

The mission of the Office of the State Auditor is to improve government for the people of Colorado.

Office of the State Auditor

Dianne E. Ray, CPA
State Auditor

August 12, 2013

Members of the Legislative Audit Committee:

This is a Compilation Report in which we have combined information contained in other audits and assessments performed by our office with additional, publically available information to provide a comprehensive overview of the current status of Information Technology (IT) in Colorado state government. This report was prepared pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits and assessments of all departments, institutions, and agencies of state government.

The purpose of this report is to increase the level of transparency around state government IT operations and strategies and to provide decision makers and the public with the information necessary to make well-informed decisions regarding future state government IT initiatives. The report contains no recommendations or responses from state agencies.

TABLE OF CONTENTS

INFORMATION TECHNOLOGY IN COLORADO STATE GOVERNMENT

August 2013
Report Highlights

Dianne E. Ray, CPA
State Auditor

Governor's Office of Information Technology

PURPOSE

To increase awareness of Colorado state government IT operations and strategy and to provide state officials, decision makers, and the public with information regarding future plans around government IT initiatives.

IT GOVERNANCE BACKGROUND

- A strong governance structure must exist to ensure that IT is aligned with the mission and objectives of state agencies and the leadership within the Executive, Judicial, and Legislative Branches.
- Pursuant to Senate Bill 08-155, which took effect on July 1, 2008, IT operations for Colorado's 16 Executive Branch departments were centralized under the Governor's Office of Information Technology.
- OIT's operational domain is the State's IT infrastructure, including data centers, servers, mainframe operations, personal computers, data storage, operating systems, local and wide area networks, and communications.
- OIT's oversight does not include IT operations for the Departments of Law, State, or Treasury; institutions of higher education; or the Judicial or Legislative Branches, each of which handles its own IT operations.
- The Colorado Information Security Program, which is overseen by the State Chief Information Security Officer, establishes a statewide information security framework and governance model that forms the foundation of the State's information security control structure.
- Executive Governance Committees (EGCs), which include members designated by departmental executive directors, serve as advisory boards for making recommendations to OIT regarding changes to project funding, scheduling, release plans, staffing, and other issues that could impact a project.

KEY FACTS AND FINDINGS

- During Fiscal Year 2013, Colorado state agencies spent a total of $353 million on IT operations and initiatives. This represents about a 0.19 percent decrease from Fiscal Year 2012 and is about 1 percent of all state expenditures for Fiscal Year 2013.
- OIT's Enterprise Portfolio Management Office reviews and rates IT projects on a monthly basis. As of the end of Fiscal Year 2013, 271 projects at 16 Executive Branch agencies were rated:
  - 82 percent had a rating of "green," indicating that, overall, the projects were on track to deliver the committed scope, on time and on budget.
  - 15 percent had a rating of "yellow," indicating that the projects were not on track to deliver the committed scope by the committed deadline with the available resources, but there was a plan in place to remediate the issues.
  - 3 percent had a rating of "red," indicating that the projects were not on track and will require a plan to get back on track.
- The Office of the State Auditor (OSA) employs a risk-based approach whereby IT audit resources are allocated to assess the State's highest IT risk areas. Between Fiscal Year 2008 through Fiscal Year 2013, the OSA made more than 630 IT-related audit recommendations to the 16 Executive Branch departments, the institutions of higher education, and the Judicial Branch.
- Specific IT risk areas identified by the OSA and addressed by the OSA's audit recommendations include:
  - user account monitoring and control;
  - secure configurations for hardware, software, and network devices;
  - IT governance;
  - continuous vulnerability assessment, remediation, and incident response management;
  - disaster recovery and data backup;
  - information security policy, training, and awareness;
  - maintenance and monitoring of audit logs;
  - control of administrative privileges; and
  - inventory of computing devices.

For further information about this report, contact the Office of the State Auditor
303.869.2800 - www.state.co.us/auditor

This page intentionally left blank.

Information Technology in Colorado State Government

Chapter 1

With the installation of the State's first computer, information technology (IT) began to work its way into every aspect of Colorado state government. Years later, the very infrastructure that enables the State of Colorado to provide a variety of services to its people and to the business community relies heavily on IT. This report provides a compilation of information on the governance and operations of IT in state government. The purpose of this report is to increase awareness of Colorado state government IT operations and strategy and to provide state officials, decision makers, and the public with information regarding future plans around government IT initiatives.

The report is organized into the following three chapters:

- **Chapter 1 – Information Technology in Colorado State Government.** This chapter provides basic information on the governance and organization of IT, information security, and large IT projects within state government.

- **Chapter 2 – Fiscal Year 2013 in Review.** This chapter provides information on the funding, expenditures, strategic planning, state legislation that impacted IT in Fiscal Year 2013, major state IT projects in progress, and audits and reports for IT operations and services in state government for Fiscal Year 2013.

- **Chapter 3 – Information Technology for Fiscal Year 2014.** This chapter is forward-looking and lays out the IT funding for 2014, state legislation that will impact IT in Fiscal Year 2014, the Office of the State Auditor's analysis of IT risk areas, and planned Fiscal Year 2014 audits and reviews to address the risk areas that are most likely to occur or that could have the greatest impact on state operations.

IT Governance

The pervasive use of technology throughout state government has made it critical that a strong governance structure exists to ensure that IT is aligned with the

mission and objectives of state agencies and the leadership within the Executive, Judicial, and Legislative Branches. According to the IT Governance Institute, an organization that conducts research on global practices and perceptions of IT governance, IT governance models enable an organization to make decisions that are in its best interest, as well as provide methods to initiate and manage work throughout the organization. Governance ensures that organizations can evaluate stakeholder needs, conditions, and options to determine balanced, agreed-upon, enterprise-wide objectives to be achieved; set direction through planning, prioritization, and decision making; and monitor operational performance and compliance against agreed-upon direction and objectives.

According to the IT Governance Institute, IT governance focuses on the following key areas:

- **Strategic Alignment** – Linking agency and IT objectives and plans; defining, maintaining, and validating the IT value proposition; and ensuring that IT and agency operations align appropriately.

- **Value Delivery** – Ensuring that IT delivers agreed-upon benefits to agencies, such as improved service delivery, with an emphasis on quantifiably minimizing costs and increasing operational effectiveness and efficiency.

- **Resource Management** – Optimizing knowledge and infrastructure to properly manage the investment in critical IT resources, including processes, applications, infrastructure, and staff.

- **Risk Management** – Heightening the risk awareness of elected officials, executive directors, and senior-level managers so that there is a clear understanding of the State's risk tolerance across agencies and departments; transparency about the significant risks to public information resources and data; and risk management responsibilities that should be embedded in individual state agencies and departments.

- **Performance Measurement** – Tracking and monitoring strategy implementation, project completion, resource usage, process performance, and service delivery.

An effective IT governance model guides decision makers in building an organizational structure that effectively supports the entity and its business objectives. Governance models include formal and informal components. Formal aspects include executive or legislative mandates, memoranda of understanding, charters, and administrative directives. Informal aspects can include collaboration, culture, and communication methods.

IT Organization

In accordance with Article III of the Colorado Constitution, Colorado has three branches of government: the Legislative Branch, overseen by the General Assembly; the Judicial Branch, headed by the Chief Justice of the Colorado Supreme Court; and the Executive Branch, headed by the Governor. Until 2008, each department within the Executive Branch had its own IT division headed by a chief information officer who reported to the department's Executive Director. Individual departments made IT budgeting, procurement, and operational decisions with limited interaction or planning across the Executive Branch. Such a fragmented infrastructure was shown to increase the difficulty of achieving economies of scale, improving operational efficiency, lowering costs, and optimizing service delivery and resource utilization.

To address these concerns, in January 2007 Governor Bill Ritter, Jr., announced a multiyear IT consolidation plan to bring the decentralized IT operations, which were spread across 16 Executive Branch departments, under the Governor's Office of Information Technology (OIT). The "IT Consolidation Bill" (Senate Bill 08-155) was enacted during the 2008 Legislative Session. Senate Bill 08-155 took effect July 1, 2008.

OIT's operational domain is the State's IT infrastructure, including data centers, servers, mainframe operations, personal computers, data storage, operating systems, local and wide area networks, and communications.

On July 1, 2010, OIT took the first step to further consolidate the State's fragmented IT operations by bringing all IT personnel and the accompanying appropriations for full-time-equivalent (FTE) staff positions under one agency, as required by Senate Bill 08-155. While the IT functions for a majority of departments under the Executive Branch were consolidated under OIT, several departments and the two other branches of government remained outside of OIT's oversight. The following table shows the 16 Executive Branch departments currently under OIT oversight and the agencies and branches that currently fall outside of OIT oversight.

Governor's Office of Information Technology Oversight
Fiscal Year 2013

Under OIT Oversight	Outside of OIT Oversight
• Department of Agriculture • Department of Corrections • Department of Education • Department of Health Care Policy and Financing • Department of Higher Education • Department of Human Services • Department of Labor and Employment • Department of Local Affairs • Department of Military and Veterans Affairs • Department of Natural Resources • Department of Personnel & Administration • Department of Public Health and Environment • Department of Public Safety • Department of Regulatory Agencies • Department of Revenue • Department of Transportation	• Department of Law (Attorney General) • Department of State (Secretary of State) • Department of Treasury (State Treasurer) • Institutions of Higher Education • Judicial Branch • Legislative Branch

Source: Sections 24-37.5-102 through 105 C.R.S.

For the departments and branches of state government that remain outside of OIT's oversight, below is a brief description of the way in which they handle their IT operations.

- **Department of Law**: The Department of Law's Information Technology division handles the department's computer-related needs, including maintenance, training, and operation of the Attorney General's website.

- **Department of State**: The Department of State's Information Technology division supports the information system needs of the entire Secretary of State's office. The division maintains the department's IT infrastructure consisting of multiple servers, personal computers, networking equipment, firewall, telephone system, and other IT equipment to support data and imaging needs. The division also supports the Web presence of the Secretary of State.

- **Department of Treasury**: Although otherwise outside of OIT oversight, the department contracts with OIT for server and desktop support.

- **Institutions of Higher Education**: Each of the 28 public higher education institutions maintains its own IT department, which supports the IT needs of the campus, faculty, staff, and students.

- **Judicial Branch**: The Judicial Business Integrated with Technology Services (JBITS) division manages the Judicial Branch's IT needs and is overseen by the branch's Chief Information Officer. JBITS provides five services: executive services, application development services, court services, e-filing services, and technical services.

- **Legislative Branc**h: Legislative Information Services (LIS) under the Colorado Legislative Council handles IT services for the Legislative Branch. LIS provides IT support and services for all legislators and their staff, the Office of Legislative Legal Services, Colorado Legislative Council, the Joint Budget Committee staff, and the Office of the State Auditor.

Information Security

The governance structure over information security in Colorado state government is slightly different and more expansive than the structure in place for other types of IT funding and operations. Specifically, the General Assembly enacted House Bill 06-1157, better known as the Colorado Cyber Security Program, during the 2006 Legislative Session. That legislation was codified in Sections 24-37.5-401 through 406, C.R.S. The law also created the position of State Chief Information Security Officer (CISO) to oversee the Colorado Cyber Security Program. The program, which is now referred to as the Colorado Information Security Program, includes governance, risk management, and compliance. Most of the law's requirements apply to public agencies that are defined in the law as "every state office, whether executive or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions." In addition to Executive and Judicial Branch agencies, the institutions of higher education and the General Assembly, although not directly accountable for the Colorado Information Security Program requirements, have specific reporting and coordination requirements.

The goal of the Colorado Information Security Program is to improve Colorado's information security posture by establishing a statewide information security framework and governance model. The program forms the foundation of the State's information security control structure and reflects the General Assembly's

commitment to address the information security risks facing public agencies with a coordinated and risk-based approach.

Large IT Projects

Prior to 2007, the Commission on Information Management (the Commission) presided over IT projects in the state. The Commission comprised both private and public sector members appointed by the Governor. Senate Bill 07-254 dissolved the Commission and directed the State's Chief Information Officer to coordinate and direct the development of policies and procedures for the effective management of technology investments throughout their entire life cycle, including, but not limited to, project definition, procurement, development, implementation, operation, performance evaluation, and enhancement or retirement. Under this direction, OIT established the Enterprise Portfolio Project Management Office (EPPMO) and hired a Director for EPPMO to provide project management oversight, direction, and best practices. EPPMO created eight Executive Governance Committees (EGCs), which are logically grouped by department/office to help achieve the goals of improving cross-departmental collaboration and to better manage the existing major IT project portfolio. Each EGC includes members designated by departmental executive directors and is chaired by the EPPMO Director.

The EGCs serve as advisory boards for making recommendations to OIT regarding changes to project funding, scheduling, release plans, staffing, and other issues that could impact a project. Projects under the oversight of an EGC are often the State's largest IT investments. Currently, projects that have an estimated cost of $5 million or greater, regardless of funding source, are automatically referred to an EGC committee. Projects can also be referred to the EGC committees by the Governor, the State's Chief Information Officer, or the EPPMO Director. Projects can also be reviewed for consideration as an EGC project if they meet one of the following established criteria: (1) the project development or acquisition timeline exceeds 1 year, (2) the project spans state agencies or government jurisdictions or is considered an "enterprise-level" project, or (3) the project has high visibility or the project is a recovery from a failed project.

Currently, the EGCs oversee 30 projects, spread out over 13 agencies. The committees meet monthly and are presented with what is known as a project dashboard for each project assigned to the committee. The project dashboard includes how far along in the timeline the project has progressed, where the budget stands at that point, and an overall rating for the project. Each of these categories is given one of the following ratings:

- *Red*: The project is not on track, and a plan is required to get the project back on track.

- *Yellow*: The project is not on track to deliver the committed scope by the committed deadline with committed resources, but there is a plan to remediate the issues.

- *Green*: The project is on track to deliver the committed scope on time and on budget.

A list of the 30 projects and their related rating can be found in Appendix A.

This page intentionally left blank.

Fiscal Year 2013 in Review

Chapter 2

This chapter reviews the State's information technology (IT) landscape during Fiscal Year 2013. Specifically, we discuss trends in IT funding and expenditures, IT strategic planning, state legislation that impacted IT in Fiscal Year 2013, major state IT projects in progress, and Fiscal Year 2013 IT audits and reports.

IT Funding

All of the Colorado branches of government and the departments under those branches have specific and varied daily business needs that require various information technology solutions. Further, many of the departments also provide public services—such as e-filing of tax returns, tax remittance, unemployment and welfare benefits, and licensing of professionals in certain occupations—that require the use of IT applications that range from small to large in size. Accordingly, department and branch IT budgets since Fiscal Year 2009 ranged from approximately $13,000 to $138 million.

Annually, the state branches and departments must request an appropriation for their IT needs, ranging from IT personnel services, multiuse network payments, and management and administration of the Governor's Office of Information Technology (OIT) to communication expenses and the building of new applications. For those departments that rely on OIT for their technology needs, a common policy line item is included in their appropriations, which are then transferred to OIT. Specifically, the following were the common policy line items that all departments under OIT authority were appropriated:

- **Multiuse Network Payments**: Each department's share of the State's data, voice, video, text, and graphics communications needs. Costs for the network include OIT's overhead, Internet access, and contractual obligations that provide the State with a reserved amount of bandwidth at each network access point. For Fiscal Year 2013, $19.5 million was appropriated across the departments, in comparison to $17.6 million for Fiscal Year 2012, an increase of 11 percent.

- **Communication Services Payments**: Each department's share of the overhead related to the State's public safety communications infrastructure. This line item funds personal services, operating expenses, and indirect costs for the Communication Services program in OIT. For

Fiscal Year 2013, $5.3 million was appropriated across the departments, in comparison to $4.9 million for Fiscal Year 2012, an increase of 8 percent.

- **Management and Administration of OIT**: Each department's share of the division-level management of OIT and back-office functions as authorized by Senate Bill 08-155. For Fiscal Year 2013, $3.4 million was appropriated across the departments, in comparison to $7.5 million for Fiscal Year 2012, a 55 percent decrease in funding.

In the table below, we provide a high-level overview of major IT-related line items that were appropriated to state agencies for Fiscal Year 2013.

Appropriated Line Items Impacting State Government IT
Fiscal Year 2013

Agency	Dollar Amount	Description
OIT and the Departments of Health Care Policy and Financing and Human Services	$14.3 million	For the Colorado Benefits Management System (CBMS) modernization project
OIT and the Department of Personnel & Administration	$8.6 million	For the Colorado Financial Reporting System (COFRS), the State's accounting system modernization project
OIT	$1.9 million	To facilitate the consolidation of the remaining agency data centers into OIT's two enterprise data centers
OIT and the Departments of Health Care Policy and Financing and Human Services	$1.3 million	For the creation of a system that can scan and store documents in the CBMS database and index each file for retrieval
OIT	$0.4 million	To support the hardware, software, maintenance, and hosting costs associated with the development of a system to electronically validate the identity and attributes of individuals responding to emergency incidents

Source: HB12-1335 Long Appropriations Bill

IT Expenditures

We analyzed the total amounts that Colorado state agencies spent on IT operations and initiatives during Fiscal Years 2009 through 2013. Due to the manner in which IT spending is tracked in the state, we were unable to easily

determine the IT expenditures for the Department of Transportation and each institution of higher education. These agencies utilize separate financial accounting systems and only report summarized data to the Colorado Financial Reporting System (COFRS), the State's accounting system. As such, the IT expenditure data contained in the rest of this section is limited to the Executive Branch (excluding the Department of Transportation), Judicial Branch, Legislative Branch, and statewide elected offices.

During Fiscal Year 2013, Colorado state agencies spent a total of $353 million on IT operations and initiatives. This represents about a 0.19 percent decrease from Fiscal Year 2012 and is about 1 percent of all state expenditures for Fiscal Year 2013.

The table below shows the five departments that were the largest consumers of IT in the state, in terms of dollars spent, during Fiscal Years 2012 and 2013.

State of Colorado
Largest IT Consumers by Dollars Spent
Fiscal Years 2012 and 2013

Largest IT Consumers in Fiscal Year 2012	Largest IT Consumers in Fiscal Year 2013
1. Governor's Office (which includes OIT)	1. Governor's Office (which includes OIT)
2. Department of Human Services	2. Department of Human Services
3. Department of Health Care Policy and Financing	3. Department of Health Care Policy and Financing
4. Department of Revenue	4. Department of Revenue
5. Department of Public Safety	5. Department of Public Safety

Source: Office of the State Auditor's analysis of IT expenditure data from the Colorado Financial Reporting System for Fiscal Years 2012 and 2013.

During Fiscal Years 2012 and 2013, the five agencies that were the largest IT consumers were responsible for approximately 78 percent of the State's total IT expenditures.

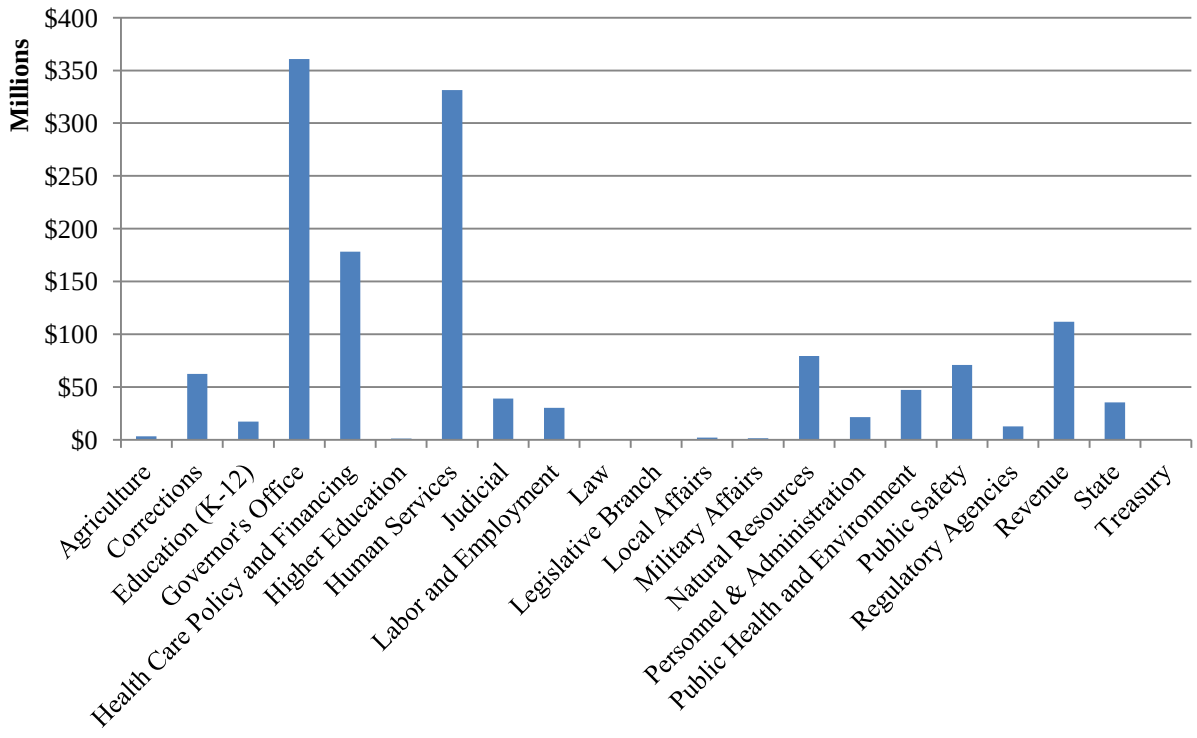
Trends in State IT Expenditures

In addition to Fiscal Year 2013 data, we obtained and analyzed state government IT expenditures for Fiscal Years 2009 through 2012. Again, these expenditure data do not include IT expenditures for either the Department of Transportation or institutions of higher education. Over the 5-year period, agencies spent a total of $1.4 billion on IT services and initiatives. In Appendix B, we provide a table of IT

expenditures for Fiscal Years 2009 through 2013, excluding the Department of Transportation and the institutions of higher education.

The chart below shows the total expenditures for Fiscal Years 2009 through 2013 by state agency and the Judicial and Legislative Branches.

Total IT Expenditures
16 of the Executive Branch Agencies,
the Legislative and Judicial Branches, and the Statewide Elected Offices
Fiscal Year 2009 through June 30, 2013

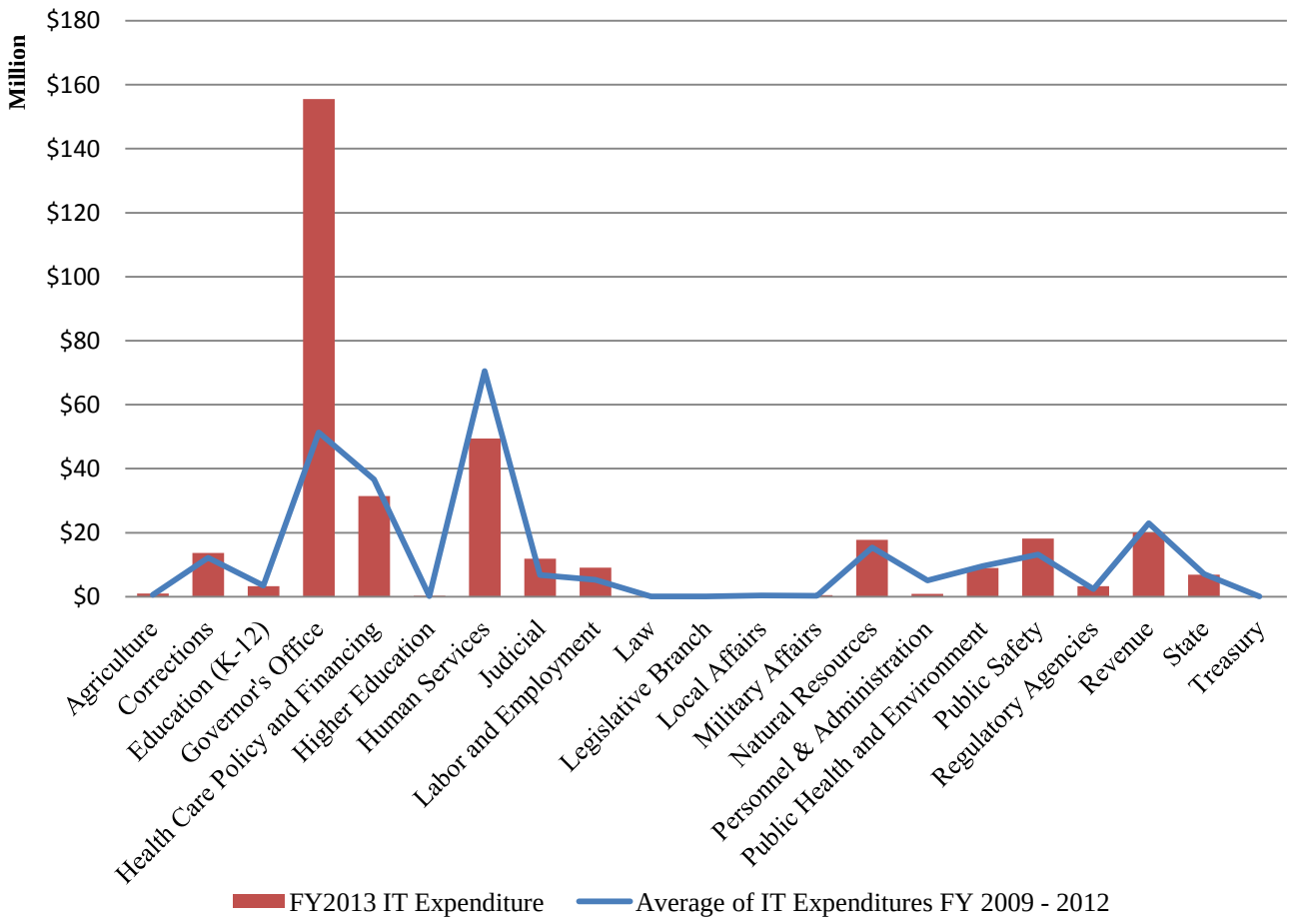


Source: Office of the State Auditor's analysis of Fiscal Year 2009 through June 30, 2013 data from the Colorado Financial Reporting System. Expenditure data were pulled as of June 30, 2013 and do not include period 13, the final closing period, for Fiscal Year 2013.

Finally, we compared Fiscal Year 2013 IT expenditures for each of the state branches, agencies, and offices with their respective average IT expenditures for the 4 prior years, Fiscal Years 2009 through 2012. Averaging the prior 4 years normalizes the data to reduce the effect of large, one-time investments. As shown in the following chart, several of the agencies' Fiscal Year 2013 expenditures

slightly exceeded the average spent during the prior 4 years, with one office, the Governor's Office, exceeding the average significantly.

IT Expenditures
16 Executive Branch Agencies,
the Legislative and Judicial Branches, and the Statewide Elected Offices
Fiscal Year 2013 and Average IT Expenditures
From Fiscal Years 2009 through 2012



Source: Office of the State Auditor's analysis of Fiscal Year 2009 through June 30, 2013 data from the Colorado Financial Reporting System. Expenditure data were pulled as of June 30, 2013 and do not include period 13, the final closing period, for Fiscal Year 2013.

IT Strategic Planning

The strategic planning process is one of the fundamental ways in which an organization creates its unique sense of identity and purpose. Through defining their mission, goals, and methods of measuring success, agencies develop the foundation for making policy decisions and prioritizing the use of limited resources. Performance-based goals are broad policy-oriented goals that indicate to the public and members of the General Assembly the intended purposes of an agency and its programs and services. Agencies should develop corresponding performance measures, either quantitative or qualitative, that can be used to assess their progress toward achieving their goals. Annually, OIT develops a strategic plan, known as the "OIT Playbook," which defines OIT's value proposition, top strategic priorities, and key initiatives. The OIT Playbook also shows an assessment of the current status of each of its state priorities, as well as its future goals. House Bill 10-1119, which was enacted on August 11, 2010, requires each Department to publish annually on its official website their strategic plan and performance measures. However, OIT is not included under this House Bill requirement. Nevertheless, as a matter of good management and best practices, OIT has created its own performance management system.

Governor's Office of Information Technology
Key Operational Performance Measures
Fiscal Year 2013

Performance Measure	FY 2013 Target	FY 2013 Actual	Description
Cost Savings / Cost Avoidance	$3.00 million	$4.01 million	Tracks savings and cost avoidance achieved as a result of IT consolidation and other initiatives and seeks to identify and define measurable outcomes related to the benefits of consolidation. The data reported are focused on professional services and operating expenses and do not consider the impact of ongoing base personal services reductions. Data are tracked on a monthly basis.
Contracting (Days to Complete Contract)	< 45 Business Days	128 Business Days	Measures the average number of business days from the solicitation award or internal procurement request to final contract execution. The metric is tracked on a monthly basis.
First Contact Resolution	60%	67%	Assesses the percentage of customers' issues that are resolved within the first point of contact. Data are tracked on a monthly basis.

Governor's Office of Information Technology
Key Operational Performance Measures
Fiscal Year 2013

Performance Measure	FY 2013 Target	FY 2013 Actual	Description
Mean Time to Total Resolution	90%	87%	Calculates the average resolution time of service requests that were closed within the given period that aligns with the priority of the request. Data are currently being captured for priority 1 targeted at less than 4 hours, priority 2 less than 3 days, and priority 3 at less than 2 weeks. Data are tracked on a monthly basis.
Project Health Index for Major IT Projects	<8.3	8.0	Assesses the progress of IT projects within the Executive Governance Committee structure. Based on the following criteria: project scope, available resources, project budget, overall risk, project schedule, and expected deliverables. This is intended to measure the overall health of Executive Governance Committee technology projects. The target measures reflect the numeric value measuring the overall health of current EGC IT related projects. Data are tracked on a monthly basis.
Application / System Availability	99.50%	99.72%	Measures the overall application availability percentage (excluding planned downtime) for critical and essential systems, as identified by the business owners, and business applications. Data are tracked on a monthly basis.
Security Awareness Trainings Completed	90%	98%	Identifies the percentage of state employees who complete the required annual statewide security awareness training. Data are tracked on an annual basis.
Broadband Availability by Household	94%	98.39%	Tracks the household broadband availability percentage (wireline and fixed wireless) across Colorado (where broadband is defined as a download speed of 3 megabits per second and an upload speed of 1 megabit per second). The objective is to understand the current broadband landscape in Colorado and how we are improving. Data are tracked biannually through contracted services. Note that this metric is currently based on provider-reported data.
Rural Broadband Availability by Households	90%	92.79%	Focuses on broadband availability in rural areas only and is similar to the previous measurement. Data are tracked biannually, through contracted services, and this metric is currently based on provider-reported data.

Source: Governor's Office of Information Technology.

Legislation Impacting IT

As technology in state government continues to change and expand rapidly, and as IT applications continue to grow larger in scale and become increasingly pervasive and critical to the citizens of Colorado, more and more legislation has been crafted around IT areas of concern. In our *Information Technology in Colorado State Government* (August 2012) report, we highlighted eight bills that were passed and would have a significant impact to IT for the State in Fiscal Year 2013. Most notably were the appropriations made for three large IT projects: the Colorado Benefits Management System Modernization project with an appropriation of $12.3 million, the Colorado Financial Reporting System Modernization project with an appropriation of $8.6 million, and the Data Center Consolidation 2.0 project with an appropriation of $1.9 million. Also of note was the passage of House Bill 12-1288, which calls for enhanced governance of all projects with an IT component. Specifically, risk, long-term sustainability, and the eventual retirement of the system must be considered when determining project success.

Shown in the table below is a list of legislation impacting IT operations in state government that passed during the 2012 Legislative Session and became effective during Fiscal Year 2013 (or earlier). As shown, most of the legislation pertains to system implementation and appropriations.

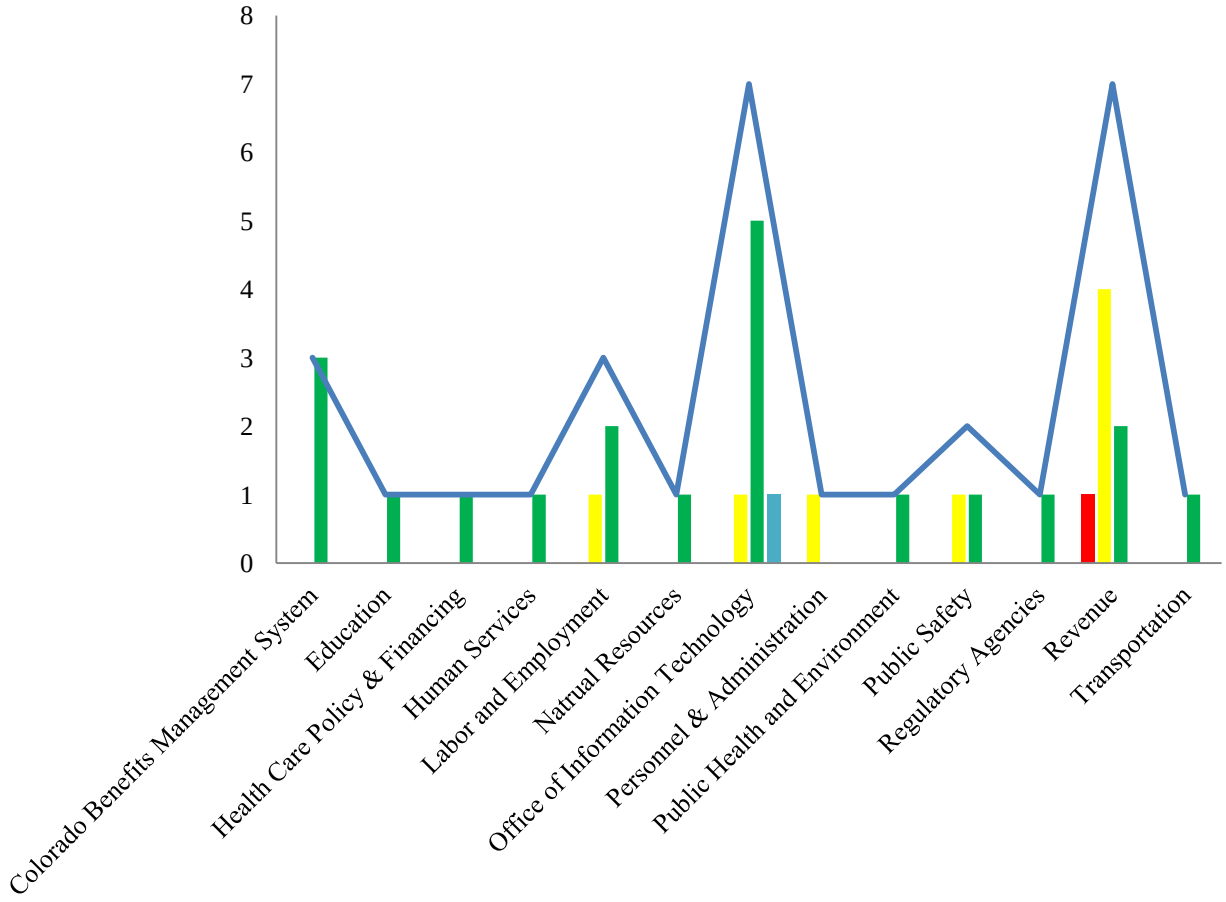
Legislation Impacting State Government IT 2012 Legislative Session Effective in Fiscal Year 2013			
Bill	**Agency**	**Effective date**	**Description**
H.B. 12-1339	Departments of Health Care Policy and Financing and Human Services	May 3, 2012	Authorized the General Assembly to appropriate monies for the CBMS improvement and modernization project. Required the Chief Information Officer to submit a written report to the Joint Budget Committee on a quarterly basis concerning the project. The bill provided $12.3 million in appropriations for Fiscal Year 2013 for major CBMS system improvements.
H.B. 12-1335	State of Colorado's General Appropriation – Long Bill	May 7, 2012	General Appropriation -- Long Bill. For Fiscal Year 2013, the bill included two major IT capital construction projects: $8,626,790 was appropriated for COFRS modernization, and $1,900,000 was appropriated for the data center consolidation.
H.B. 12-1052	Department of Regulatory Agencies	July 1, 2012	Requires the Director of the Division of Registrations to implement a system to collect health care workforce data from health care professionals who are eligible for the Colorado Health Service Corps, practical and professional nurses, and pharmacists. The bill appropriated $36,745 from the Division of Registrations Cash Fund to the Department of Regulatory Agencies.
H.B. 12-1041	Department of Public Health and Environment	August 8, 2012	Created an electronic death registration system for the purposes of allowing persons responsible for reporting death information to the Office of the State Registrar of Vital Statistics to do so electronically. Within 2 years after the bill takes effect, the Department of Public Health and Environment is to submit a report to the Health and Environment Committee of the House of Representatives, and the Health and Human Services Committee of the Senate, or their successor committees, regarding the development and implementation of the electronic death registration system, detailing staffing level and fee modifications since implementation. The bill appropriated $743,940 in Fiscal Year 2013.
H.B. 12-1288	Governor's Office of Information Technology	August 8, 2012	Developed a comprehensive risk assessment process that will be applied to every new IT project to assess risk levels related to the project and determine whether the project should be classified as a major IT project. Requires OIT to establish project budgets for projects of all sizes, including major IT projects. Requires a state agency to consult with and obtain the approval of OIT in connection with any major IT project that it plans to undertake. Requires the State's Chief Information Officer to develop a staged review process for IT projects that ensures a project meets specific requirements and complies with the project plan approved by OIT. Expanded the definition of "capital construction" to include the purchase of services from OIT on the condition that the use of such services is the most cost-beneficial option or falls within the duties and responsibilities of OIT or the State's Chief Information Officer.
Source: Office of the State Auditor staff review of 2012 Legislative Session information.			

IT Projects

The Enterprise Portfolio Project Management Office currently oversees 271 IT projects at 16 Executive Branch agencies. Of these 271 projects, 30 (11 percent) have been identified as Executive Governance Committee projects based on the criteria discussed in the previous Large IT Projects section. Monthly, the Enterprise Portfolio Project Management Office reviews and rates IT projects to determine the health of each project. Each project is reviewed to determine if the project is on track to remain within the established budget, is in compliance with the project schedule, and is adhering to the project scope, and each project is given a rating of red, yellow, or green in each of those areas. Based on the combined ratings of these areas, the project is then given an overall rating of red, yellow, or green. As of the end of Fiscal Year 2013, 222 (82 percent) of the 271 projects had an overall health rating of green, indicating that, overall, the projects were on track to deliver the committed scope, on time and on budget. Further, 42 (15 percent) projects had a health rating of yellow, indicating that the projects were not on track to deliver the committed scope by the committed deadline with the available resources, but there was a plan to remediate the issues. Lastly, only seven (3 percent) projects were given a red rating, indicating that the projects were not on track and will require a plan to get back on track. In Appendix A, we provide a snapshot view of the 30 Executive Governance Committee (EGC) projects showing the start and projected end dates, the planned and the actual budgets to date, overall project status, and descriptions of the projects. Below is a pie chart that illustrates the overall health of the Executive Branch IT projects using the red, yellow, and green rating color scheme.

Of the 30 EGC projects, seven (23 percent) belong to the Department of Revenue and seven (23 percent) are OIT projects. Combined, they make up 46 percent of all EGC projects. Of these 14 projects, 50 percent of them have been given a rating of yellow status for the project schedules, indicating that the schedules are not on track to deliver the committed scope by the committed deadline with committed resources, but there are plans to remediate the issues. Two of the 14 projects have a schedule rated as red, indicating that the projects are not on track, and plans are required to get the projects back on track. Of these 14 projects, five (36 percent) have an overall project rating of yellow, and one has an overall project rating of red. The chart below shows the total number of EGC projects by agency and the number of projects by rating for each agency.

Total Number of Executive Governance Committee Projects by Agency or Project Name
As of June 30, 2013



Red: the project is not on track, and a plan is required to get the project back on track.
Yellow: the project is not on track to deliver the committed scope by the committed deadline with committed resources, but there is a plan to remediate the issues.
Green: the project is on track to deliver the committed scope on time and on budget.
Not Rated: The project status has not been rated at this time.

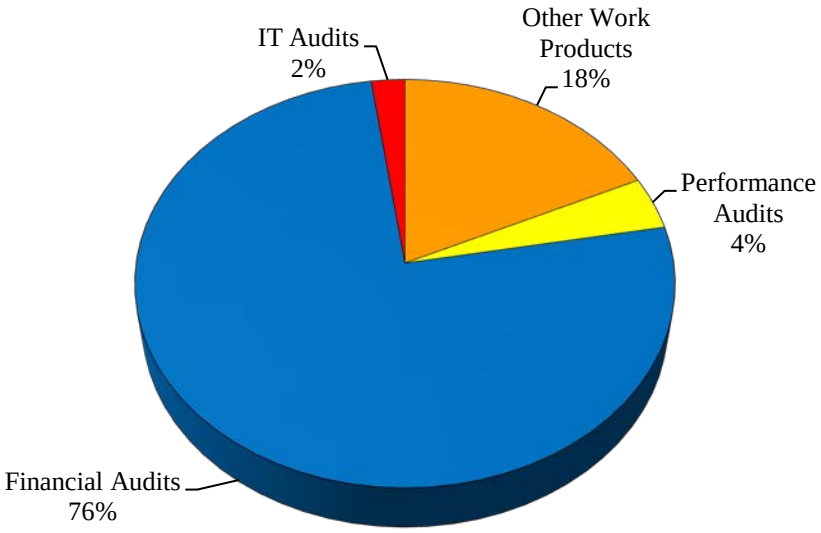
Source: Office of the State Auditor's analysis of data provided by the Governor's Office of Information Technology.
Note: Blue line represents the total number of projects.

IT Audits and Reports

The Office of the State Auditor (OSA) employs a risk-based approach whereby we allocate our IT audit staff resources to assess the State's highest IT risk areas. As shown in the following chart, during Fiscal Year 2013, the largest use of the IT resources was to support the financial audits, at 76 percent. Other work products, such as the Information Technology in Colorado State Government

report and the Legislative Audit Recommendation database used 18 percent of the resources. The remaining 6 percent was allocated between performance (4 percent) and IT (2 percent) audits.

Office of the State Auditor
IT Audit Resource Allocation by Audit Area[1]



Source: Office of the State Auditor's analysis of timekeeping data, as of April 23, 2013.
[1]The chart does not reflect time spent on management and other operational duties.

Based on the risks identified at the time, during Fiscal Year 2013, OSA conducted and presented to the Legislative Audit Committee the following IT audit-related work:

IT Audits

Independent Verification and Validation Review of the Judicial Department's Integrated Colorado Courts E-Filing and Judicial Paper on Demand Systems July 2012	
Purpose:	To evaluate the Judicial Department's Integrated Colorado Courts E-Filing and Judicial Paper on Demand systems and identify any problems early enough in the development process, thereby enhancing the quality of ongoing development efforts.
Overall Conclusion:	Overall, the audit concluded that the Judicial Department's Integrated Colorado Courts E-Filing and Judicial Paper on Demand projects were following best practices to ensure successful outcomes managerially, financially, and technically and that the projects faced a low to medium risk of failure.

IT Components of Performance Audits

Statewide Internet Portal Authority November 2012	
Purpose:	To determine whether there were effective internal controls in place at the Statewide Internet Portal Authority (SIPA) over contracts, financial activities, and information systems.
IT-Related Conclusion:	The audit concluded that SIPA's contract administration does not provide assurance that government entity or consumer data are secure and that services will continue in the event of a disaster. Additionally, the audit found that SIPA had not established a comprehensive system of control to manage its risks.

Medicaid Hospital Provider Fee Program September 2012	
Purpose:	To evaluate the Medicaid Hospital Provider Fee Program to determine the Program's compliance with federal and state laws and to assess the reliability of data used in the Hospital Provider Fee Model to calculate the fees paid by hospitals and supplemental payments made to hospitals.
IT-Related Conclusion:	The audit concluded that the Department of Health Care Policy and Financing should improve the information security of the Hospital Provider Fee Model spreadsheet by restricting access to only those users with a business need and by developing a method to track changes in the spreadsheet over time.

Further, IT audit staff performed IT general computer controls testing for the *Medical Marijuana Regulatory System Part I* (March 2013) performance audit, and this testing did not result in formal findings.

IT Components of Statewide Single and Financial Audits

In addition to the standalone IT audit and performance audit projects discussed above, OSA's IT Audit Division performed audit work in Fiscal Year 2013 in support of the Statewide Single and Financial Audits for Fiscal Year Ended June 30, 2012 report (released February 2013). The following table provides the results of the general computer controls audit work performed for this review. The table does not include follow-up testing performed on prior year audit recommendations.

State of Colorado Statewide Single Audit For Fiscal Year Ended June 30, 2012		
Purpose:	To determine whether the State of Colorado's IT control activities, individually or in combination with others, are properly designed, in place, and operating effectively to prevent, or detect and correct, material misstatements in Colorado's Comprehensive Annual Financial Report and the Schedule of Expenditures of Federal Awards.	
Agency	**Application**	**IT-Related Conclusion**
Governor's Office of Information Technology	Access control software (Top Secret) for mainframe applications	No findings were noted for Top Secret in the Fiscal Year 2012 Statewide Single Audit.
Health Care Policy and Financing	Medicaid Management Information System (MMIS), SSAE 16 review	No findings were noted for MMIS in the Fiscal Year 2012 Statewide Single Audit.
Department of Human Services	JP Morgan Electronic Benefits System (EBT), Statement on Standards for Attestation Engagements (SSAE) 16 review	The Department of Human Services should work with its fiscal agent to ensure that the SSAE 16 report is available in a timely manner and that the fiscal agent is being held accountable for information system controls over the EBT System.
Department of Human Services	Childcare Automated Tracking System (CHATS)	No findings were noted for CHATS in the Fiscal Year 2012 Statewide Single Audit.

State of Colorado Statewide Single Audit For Fiscal Year Ended June 30, 2012		
Purpose:	To determine whether the State of Colorado's IT control activities, individually or in combination with others, are properly designed, in place, and operating effectively to prevent, or detect and correct, material misstatements in Colorado's Comprehensive Annual Financial Report and the Schedule of Expenditures of Federal Awards.	
Agency	**Application**	**IT-Related Conclusion**
Department of Human Services, Department of Health Care Policy and Financing, and Governor's Office of Information Technology	Colorado Benefits Management System (CBMS), SSAE 16 review	The departments and OIT should work together to ensure that the CBMS service provider adequately mitigates risks associated with the 18 exceptions listed in the SSAE 16 report.
Department of Personnel & Administration	Colorado Financial Reporting System (COFRS)	No findings were noted for COFRS in the Fiscal Year 2012 Statewide Single Audit.
Department of Personnel & Administration and OIT	Colorado Personnel Payroll System (CPPS)	The Department of Personnel & Administration and OIT should work together to implement adequate controls related to access management, network controls, disaster recovery and backups, and succession planning.
Department of Public Health and Environment and OIT	Women, Infants, and Children system (Compass)	The Department of Public Health and Environment and OIT should work together to ensure that all U.S. Department of Agriculture rules and regulations and Colorado Information Security Policies related to security assessments, business continuity, physical inventory, service-level agreements, and access controls are adequately implemented.
Department of Revenue	GenTax	No findings were noted for GenTax in the Fiscal Year 2012 Statewide Single Audit.
Department of Revenue and OIT	Revenue Accounting System	Prior year audit recommendations were not implemented by the Department of Revenue and OIT. However, due to the retirement of the Revenue Accounting System, OSA did not make any further recommendations for the system.

In total, OSA made 75 recommendations, including subparts, in the Fiscal Year 2012 Statewide Single Audit report pertaining to the areas of IT security, change management, IT operations, and work done on prior year audit recommendations.

In addition to the Statewide Single Audit work (which was performed independently by OSA) OSA also provided IT audit programs to contractors who performed audit work pertaining to the annual financial audit of the State in Fiscal Year 2012.

Information Technology for Fiscal Year 2014

Chapter 3

This chapter reviews the State's information technology (IT) landscape anticipated for Fiscal Year 2014. Specifically, we discuss trends in IT funding and new state legislation that was enacted that will affect IT in Fiscal Year 2014. In addition, this chapter focuses on the areas of risk for which the Office of the State Auditor (OSA) has made IT audit recommendations over the past 6 fiscal years (Fiscal Years 2008 through 2013) and the IT audits and reviews planned for Fiscal Year 2014.

IT Funding

Below are the common policy line items that all departments under the Governor's Office of Information Technology (OIT) authority were appropriated for Fiscal Year 2014:

- **Colorado State Network (formerly Multiuse Network Payments)**: For Fiscal Year 2014, $20.9 million was appropriated across the departments, in comparison to $19.5 million for Fiscal Year 2013, an increase of 7 percent.

- **Communication Services Payments**: For Fiscal Year 2014, $5.4 million was appropriated across the departments, in comparison to $5.3 million for Fiscal Year 2013, an increase of 2 percent.

- **Management and Administration of OIT**: For Fiscal Year 2014, $3.7 million was appropriated across the departments, in comparison to $3.4 million for Fiscal Year 2013, an increase of 9 percent.

In the following table, we provide a high-level overview of major IT-related line items that were appropriated to state agencies for Fiscal Year 2014.

Appropriated Line Items Impacting State Government IT Fiscal Year 2014		
Agency	**Dollar Amount**	**Description**
OIT and the Departments of Health Care Policy and Financing and Human Services	$14.6 million	For the continuation of the Colorado Benefits Management System modernization project.
Department of Personnel & Administration	$3.3 million	For the Department of Personnel & Administration to purchase specialized equipment (e.g., scanners and letter openers) and for OIT to purchase supporting IT infrastructure (e.g., servers and routers), all of which will enable the State to more efficiently manage tax remittances submitted to the Department of Revenue, contracting with the Department of Personnel & Administration.
Department of Labor and Employment	$2.9 million	For services related to the multi-state WyCAN (Wyoming, Colorado, Arizona, and North Dakota) project to manage unemployment taxes and benefits.
Department of Human Services	$1.9 million	For the investment in mobile technology to be used by county child welfare workers performing administrative work in the field. The technology will give the child welfare workers remote access to Trails, the database used to manage child welfare cases.
OIT	$1.4 million	To meet the financial obligations of operating the State's Multi-Use Network concurrently with the new Colorado State Network while migration to the new network for all state agencies is completed.
The Colorado Office of Information Security	$1.1 million	To address the State's most pressing information security needs.
OIT and the Department of Health Care Policy and Financing	$500,000	For the provision of a behavioral health data system to track patient and provider performance data.
OIT	$400,000	For the implementation of an IT asset tracking system.
Office of State Planning and Budgeting	$300,000	To conduct an IT billing study.
Source: SB13-230 Long Appropriations Bill		

Legislation Impacting IT

Similar to the 2012 Legislative Session, numerous bills impacting IT in state government were introduced during the 2013 Legislative Session. The most

significant 2013 bill impacting IT was House Bill 13-1079, which created the Joint Technology Committee. This committee will provide oversight of all IT issues in the State, including projects, security technology, policies and concerns, IT infrastructure, and short-term and long-term changes in state IT.

Shown in the table below is a list of legislation that passed in Fiscal Year 2013 impacting OIT or IT operations in state government and will be effective in Fiscal Year 2014.

Legislation Impacting State Government IT
2013 Legislative Session
Effective in Fiscal Year 2014

Bill	Agency	Effective date	Description
S.B. 13-137	Department of Health Care Policy and Financing	February 19, 2013	Authorizes the Department of Health Care Policy and Financing to issue a request for information to seek input from potential contractors on capabilities to perform advanced predictive modeling and analytics using technology to provide a comprehensive and accurate view across all providers, recipients, and geographic locations within the Medicaid program in order to identify fraud.
S.B. 13-053	Departments of Education and Higher Education	April 8, 2013	Requires the departments to establish a procedure that will allow for the direct, electronic exchange of student unit record data for students enrolled in Colorado public high schools to Colorado institutions of higher education.
S.B. 13-231	Department of Human Services	May 14, 2013	The statute creates a demonstration project in CDHS allowing counties to enter into performance agreements with the Department and to test interventions that will best increase permanency, positive outcomes, safety, and well-being of children and their families. OIT will serve as a consultant on the project and is not mentioned in the statute.
H.B. 13-1079	OIT	May 18, 2013	Creates a Joint Technology Committee, with the responsibility of oversight for OIT, including all of the following: a review of the state of IT, any general IT needs, any anticipated short- or long-term IT changes for IT, OIT's responsibilities related to the statewide communications and information infrastructure, and OIT's responsibilities for statewide geographic information system coordination. The Joint Technology Committee will

Legislation Impacting State Government IT 2013 Legislative Session Effective in Fiscal Year 2014			
Bill	**Agency**	**Effective date**	**Description**
			also have oversight of the State's Chief Information Security Office and its duties; any telecommunications coordination in the state performed by the State's Chief Information Officer; the General Government Computer Center and state agencies regarding any IT purchased or implemented that is not managed or approved through OIT, any IT that a state agency purchased or implemented that does not follow the standards set by OIT, and any IT that a state agency purchased or implemented that has the same function as IT already created, purchased, or implemented by OIT.
H.B. 13-1292	All Departments	May 24, 2013	Sets a 90 percent level of in-state employment for projects where the budget includes appropriated state monies. As such, OIT will monitor the rate at which out-of-state or out-of-country staff and companies are hired. If the established threshold is violated, OIT must post the violation information on its website.
H.B. 13-1241	OIT and the Department of Public Safety	May 28, 2013	Allows for the appropriation of monies from the General Fund to the Department of Public Safety and OIT for the operation of the statewide automated victim information and notification system. In addition to General Fund appropriations, the Department of Public Safety and OIT were appropriated $434,720 for the creation of the system.
S.B. 13-004	Department of Revenue	August 7, 2013	The statute allows state-issued ID cards to be authorized via electronic means. This will impact IT systems at the Dept of Revenue and OIT will serve as a consultant. OIT is not mentioned in the bill. Allows for the renewal of state identification cards by mail and provides an appropriation of $4,588 to the Department of Revenue and OIT for the implementation of the bill.
Source: Office of the State Auditor staff review of 2013 Legislative Session information.			

IT Projects

Below we provide a list of the current Executive Governance Committee projects that are scheduled to continue throughout or complete in Fiscal Year 2014. For more detailed information about each of the projects listed below see Appendix A.

Governor's Office of Information Technology
Fiscal Year 2014 Executive Governance Committee
Projects In Progress as of June 30, 2013

No.	Project	Estimated Completion Date
Colorado Benefits Management System (CBMS)		
1	CBMS Convert Rules to New Engine (Department of Human Resources)	June 2014
2	CBMS New Rules Engine (Health Care Policy and Financing) Modified Adjusted Gross Income (MAGI) Calculations	September 2013
3	CBMS New Rules Engine (Health Care Policy and Financing) Non- Modified Gross Adjusted Income (MAGI) Calculations	September 2014
Department of Education		
4	Statewide Longitudinal Data System (SLDS) - Capture	June 2014
Department of Health Care Policy and Financing		
5	Medicaid Information Technology Architecture Management Information System (MMIS) Reprocurement Phase 1 – Solicitations	July 2014
Department of Human Services		
6	Automated Child Support Enforcement System (ACSES) Migration – Master	September 2013
Department of Labor and Employment		
7	OPS AMANDA System Implementation Strategy (OASIS)	June 2014
8	Unemployment Insurance Internet Self Service	September 2013
9	Wyoming, Colorado, Arizona, North Dakota Consortium Phase 1	September 2013
Department of Natural Resources		
10	Integrated Parks and Wildlife System (IPAWS)	May 2015
Department of Public Health and Environment		
11	Mountain Plains State Consortium's Women, Infant, & Children System	October 2013

Governor's Office of Information Technology
Fiscal Year 2014 Executive Governance Committee
Projects In Progress as of June 30, 2013

No.	Project	Estimated Completion Date
Department of Public Safety		
12	Colorado Bureau of Investigation Automated Fingerprint Identification System Replacement	June 2013
13	Multi-Purpose Public Safety Solution: Premier One Computer-Aided Dispatch Migration and Maintenance	June 2014
Department of Regulatory Agencies		
14	Licensing System Replacement	March 2013
Department of Revenue		
15	Amendment 64 Implementation	December 2014
16	Colorado State Title and Registration System – Colorado State Network Upgrade	August 2013
17	Tax Pipeline Imaging Project	March 2014
18	System Infrastructure Refresh Phase 1	June 2013
19	Marijuana Enforcement Division Inventory Tracking System	September 2013
20	Office of Information Technology - Viper database Upgrade	October 2013
21	Tax Pipeline and Imaging Phase 3	January 2014
Department of Transportation		
22	Procurement for Public Sector Supplier Relationship Management Phases 2 & 3	December 2014
Department of Personnel & Administration		
23	The Colorado Financial Reporting System (COFRS) - Modernization of the State's accounting system	September 2014
Office of Information Technology		
24	Colorado Complex Local Area Network Upgrade / Migration	November 2013
25	Colorado Broadband Data & Development Program	June 2016
26	Colorado State Network Implementation	December 2013
27	Data Center Consolidation 2.0	July 2013
28	Data Center Consolidation Enterprise Refresh	March 2014
29	Managed Internet Protocol Communication	October 2013
30	Statewide Longitudinal Data System (SLDS) Link	October 2013

Source: Governor's Office of Information Technology

IT Risk Areas

In any business operation today, risk plays a critical role. Almost every business decision an executive director, department or division head, or manager has to make requires that he or she balance risk and reward. Effectively managing that risk is essential to an enterprise's success. However, all too often IT risk (the business risk related to the use of IT) is overlooked and is relegated to a technical specialist who is outside of the decision-making circle. If the risk is left unmanaged, significant financial and data losses may result; however, if risk is managed effectively, benefits to productivity can be achieved.

At OSA, we spent Fiscal Years 2008 through 2013 auditing state agencies, large IT projects, application systems, and the overall governance of IT in the State of Colorado. Based on our audit experience and the more than 630 IT recommendations we have made to the 16 Executive Branch departments, the institutions of higher education, and the Judicial Branch, we have determined the significant areas of IT risk in state government. The 632 recommendations we made do not include 179 recommendations made under separate cover as a part of the *Office of Cyber Security Performance Audit* (November 2010).

The following sections provide an overview of IT risk areas OSA has identified and recommendations we have made in those areas.

Account Monitoring and Control

Inactive user login accounts that have not been disabled give attackers and employees looking to commit fraud the opportunity to impersonate legitimate users, making discovery of the malicious behavior difficult. According to the SANS Institute, a private U.S. company that specializes in Internet and computer security training, accounts of contractors and employees who have been terminated have been misused in this way. Additionally, the SANS Institute found instances of current and former employees who have maliciously accessed user accounts left in a system long after the user’s contract expiration or termination of employment. These accounts allow continued access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes. Of the total 632 IT recommendations OSA made from Fiscal Years 2008 through 2013, 144 (23 percent) addressed account monitoring and control and the need to control access based on the account users’ need to know.

Secure Configurations for Hardware, Software, and Network Devices

Computer hardware, software, and network devices that are installed with default security settings that are geared to ease of deployment and ease of use are vulnerable to exploitation. In addition, updates to software are not always applied in a timely manner and can introduce unknown weaknesses, leaving a computing device vulnerable to attack. Further, attackers take advantage of the fact that network devices may become less secure over time as users demand exceptions to security settings for specific business needs. These exceptions to settings are not removed when the business need is no longer applicable.

Network ports can also provide access to sensitive data—specifically to services and utilities that are running on a server. Colorado Information Security Policies, industry best practices, and the Center for Internet Security standards specify that only those network ports, services, and utilities necessary to conduct business should be available and running. Of the 632 recommendations OSA made from Fiscal Years 2008 through 2013, 118 (19 percent) were related to the security configuration of computer hardware, software, and network devices.

IT Governance

Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-upon enterprise objectives to be achieved. Further, governance ensures direction is set through prioritization and decision making, and performance and compliance are monitored against the agreed-upon direction and objectives. For the purposes of categorizing OSA's audit recommendations, we have included vendor contract management, service-level agreements, business process, project management, and OIT consolidation-related findings in this category. From Fiscal Years 2008 through 2013, we have made 101 recommendations (16 percent of the 632 recommendations) in the area of IT governance.

Continuous Vulnerability Assessment, Remediation, and Incident Response Management

Organizations that do not scan for computer vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised. Finding and addressing computer software vulnerabilities reduce the opportunity for persistent attackers to gain access to sensitive data. Vulnerabilities must also be tied to threat intelligence and be properly prioritized. Organizations that do not have effective incident response to exploited

vulnerabilities can experience considerable damage to their reputations and loss of information. Without an incident response plan, attacks may never be discovered in the first place, or, if the attack is detected, proper procedures that would help to contain damage, eradicate the attacker's presence, and recover in a secure fashion may never be implemented. Of the 632 IT recommendations OSA made between Fiscal Years 2008 and 2013, 73 (12 percent) have addressed the need for continuous vulnerability assessments and remediation and incident response management. Of the 73 recommendations, 23 (32 percent) were made as a result of the network and computer systems penetration testing performed from February through November 2010 as part of the *Office of Cyber Security Performance Audit* (November 2010).

Disaster Recovery and Data Backup

The ability to recover lost or damaged data is critical to most departments' ability to continue doing business after an incident of data loss. To help ensure that systems can be brought up after a data loss or system failure, a backup copy of the operating system, application software, and data on a computer should be included in the overall backup procedures, and the backup procedures should be performed regularly. All backup policies should be compliant with regulatory and organizational requirements. Further, as required by Colorado Information Security Policies, systems should be tested regularly to ensure that the systems can be effectively recovered in an emergency, that staff is aware of the restore procedures, that all necessary backup procedures have been followed, and that the appropriate hardware is available. Since Fiscal Year 2008, OSA has seen a steady increase in the number of findings in the areas of data backup and disaster recovery for a total of 72 (11 percent) of the total 632 recommendations made.

Information Security Policy, Training, and Awareness

A constantly updated information security awareness and education program for all users is important. Policies tell staff what they should do: training provides staff with the knowledge and skills to implement the policies; and awareness can change behaviors so that people follow the policies. If, after training, users are still not following policies, the policies should be augmented with heightened efforts to ensure user awareness and understanding. Insufficient information security awareness and training puts the State at greater risk for theft of critical data; corruption of sensitive information; major system outages; and, increasingly, actual destruction of systems. Since Fiscal Year 2008, 49 (8 percent) of OSA's 632 recommendations were related to the need to address information security training, adequate information security policy creation and oversight, and assessment of information security knowledge and skills of IT and business staff.

Maintenance and Monitoring of Audit Logs

Sometimes log records are the only evidence of a successful attack against a computer application or system. We have found that many of the systems in the state are not programmed or configured to generate or retain audit logs. Further, for many systems that do generate and retain audit logs, there is no regular log review to identify and respond to abnormal system events. In this way, many system attackers rely on the likelihood that many organizations do not consistently review audit logs and therefore do not know whether their systems have been compromised. Due to this, attackers can retain unauthorized access and control of computer systems for months or years without anyone in the organization knowing, despite evidence of such attacks being recorded in log files that are being generated appropriately. Of the 632 total IT recommendations between Fiscal Years 2008 and 2013, 42 (7 percent) have addressed the need to maintain audit logs and monitor them for anomalies that could indicate attacks or fraud on the application or system.

Control of Administrative Privileges

A common technique used by attackers, including employees committing fraud, is the elevation of privileges to an application by guessing, cracking, or otherwise obtaining an administrative password, which then allows access to sensitive information or financial systems that could ultimately result in financial loss.

From Fiscal Years 2008 through 2013, OSA made 28 recommendations (4 percent of the total 632 recommendations) around the need to control and limit the use of administrative privileges.

Inventory of Computing Devices

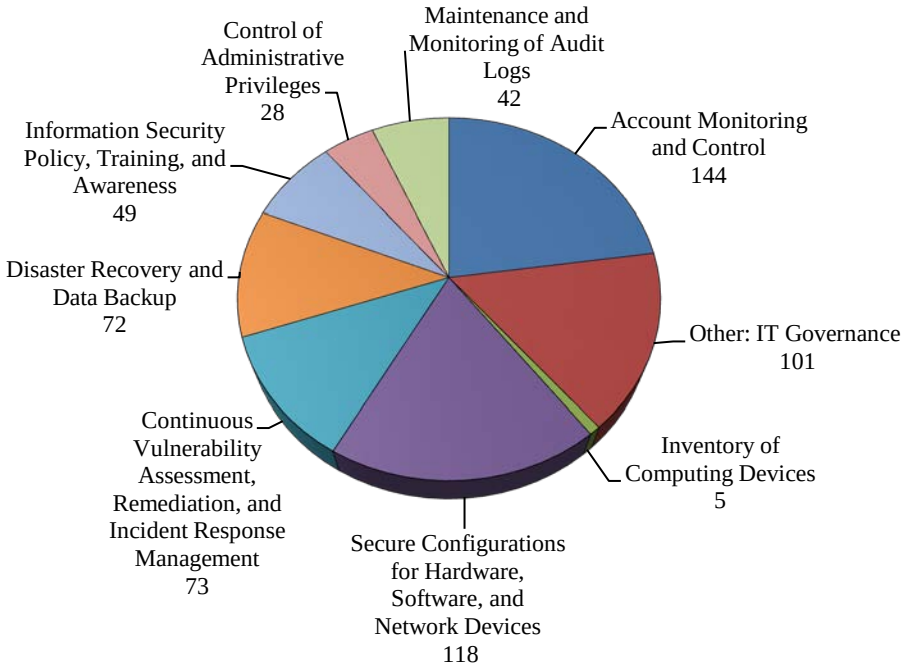
According to the SANS Institute, a private U.S. company that specializes in Internet and computer security training, inventorying authorized and unauthorized devices is one of the top critical security controls that when performed can help to reduce security risk. Without an accurate inventory of what is deployed, OIT security services cannot guarantee that all computing hardware and software are secured, thus leaving the network open to attacks and a potential loss of data. From Fiscal Years 2008 through 2013, five (1 percent) of OSA's 632 recommendations pertained to the inventory of devices.

Over the years, OIT has struggled to get a handle on the number of authorized and unauthorized devices connecting to the state network. This difficulty is, in part, due to the inability to get an accurate inventory of all of the hardware and

software already deployed in the field. Further, as we see departments and counties implement mobile device technology with the goal of improving efficiency and effectiveness, we can expect there to be a rise in risks that are specific to these devices.

The chart below shows the number of IT recommendations OSA made in each of the above categories between Fiscal Years 2008 and 2013.

Office of the State Auditor IT Recommendations
By Category
Fiscal Years 2008 through 2013



Source: Office of the State Auditor's analysis of audit reports and reviews performed from Fiscal Years 2008 through 2013.

Fiscal Year 2014 IT Audits and Reviews

Based on the risks discussed above, OSA has identified IT audits and reviews that will be important to conduct and follow up on during Fiscal Year 2014.

OSA plans to conduct audits and reviews during the remainder of Fiscal Year 2014 to include the following risk areas:

- **Network and System Security:** OSA intends to address the risks associated with insufficient controls that may allow unauthorized network

access to the State's critical IT systems, including those at higher education institutions.

- **Management of IT Processes and Services:** OSA plans to evaluate the risks associated with management processes, which may not fully ensure that key IT processes and services meet the key business objectives of the units being served. This review may also include the oversight of IT projects whose success is critical to the State.

Fiscal Year 2014 Statewide Single Audit

The State uses several key computer applications to record financial activity and administer state operations. The annual statewide single audit includes testing IT controls over these key applications in order to evaluate the State's IT effectiveness associated with preventing and detecting potential material misstatements in financial records and to verify that the IT infrastructure that supports key applications is secure.

Appendices

Appendix A

EGC Projects as of June 30, 2013

No.	Project	Start Date	End Date	Planned Budget	Actual to Date	Status		Description
	Colorado Benefits Management System							
1	CBMS Convert Rules to New Engine (Department of Human Resources)	10-Jun-13	30-Jun-14	$1,000,000	$0	3% complete		The purpose of this project is to migrate the older rules engine of the CDHS eligibility programs to the Corticon rules engine. The advantages of this project include modernizing the rules engine with a more current product, reducing dependencies in the code, more efficient processing and improved development tools.
2	CBMS New Rules Engine (Health Care Policy and Financing) MAGI	21-May-12	27-Sep-13	$3,000,000	$0	75% complete		On March 16, 2012, the US Department of Health and Human Services (HHS) issued final and interim final rules ("the Medicaid final rule") codifying Medicaid eligibility and enrollment provisions of the Patient Protection and Affordable Care Act (ACA). As a result, CBMS needs to be upgraded and the new way of eligibility determination Modified Adjusted Gross Income (MAGI) needs to be put in place.

No.	Project	Start Date	End Date	Planned Budget	Actual to Date	Status		Description
3	CBMS New Rules Engine (Health Care Policy and Financing) Non-MAGI	1-Dec-12	22-Sep-14	$1,696,464	$0	65% complete		Currently CBMS uses a proprietary rules engine which supports all the Medicaid programs. This project migrates the Non-MAGI Medical programs (LTC, AM, MSP and LIS) to the new rules engine and will rewrite some of the decision table logic.
	Department of Education							
4	SLDS - Capture	1-Jul-10	30-Jun-14	$8,561,800	$4,729,685	81% complete		To facilitate capture of timely and reliable data that can then be linked for purposes of making P-20 educational decisions. This falls under the CAPTURE initiative of the 2009 SLDS Grant.
	Department of Health Care Policy and Financing							
5	MITA MMIS Reprocurement Phase 1 - Solicitations	1-Jun-11	1-Jul-14	$2,145,377	$2,072,877	90% complete		To conduct an assessment of the Medicaid Information Technology Architecture (MITA), the Medicaid Management Information System (MMIS) and Fiscal Agent services procurements in other states in preparation for the upcoming MMIS procurement.
	Department of Human Services							
6	ACSES Migration - Master	1-Aug-11	6-Sept-13	$7,875,000	$4,362,022	89% complete		To migrate the ACSES (Automated Child Support Enforcement System) from a older mainframe operating system to a state-of-the-art operating platform.

No.	Project	Start Date	End Date	Planned Budget	Actual to Date	Status		Description
	Department of Labor and Employment							
7	CDLE OASIS	14-Sep-11	30-Jun-14	$4,188,221	$1,763,396	62% complete		New application software implementation of the AMANDA system, for the Division of Oil and Public Safety at the Department.
8	UI Internet Self Service - ISS	1-Apr-09	30-Sep-13	$8,708,512	$7,826,912	88% complete		To modernize the current Internet Self Service (ISS) applications, develop, implement and maintain the functionality of new applications and integrate these elements into an Internet Self-Service Suite.
9	WyCAN Phase 1	11-Aug-11	30-Sep-13	$2,204,646	$1,012,381	93% complete		The WyCAN Consortium consists of the Unemployment Insurance (UI) programs of the States of Arizona, Colorado, North Dakota, and Wyoming. The Consortium is seeking information about procuring a combined UI Tax and Benefits system that is extensible and configurable and will be cost-effective for development, operations, and support.
	Department of Natural Resources							
10	Integrated Parks and Wildlife System (IPAWS)	2-Nov-10	21-May-15	$4,258,961	$1,281,682	65% complete		To replace the Colorado Parks and Wildlife (CPW) Total Licensing System (TLS). The new system will be a cloud based solution.

No.	Project	Start Date	End Date	Planned Budget	Actual to Date	Status		Description
	Department of Public Health and Environment							
11	MPSC Women, Infant, & Children (WIC)	7-Feb-06	13-Oct-13	$19,239,020	$18,406,582	97% complete		To develop a new web enabled WIC system that will replace existing legacy system and will be used for case management and payment control. The project is in partnership through a consortium that includes the states of Wyoming and Utah, the Mountain Plains Consortium (MPSC). The project is 100% federally funded and is under the gated process of the USDA.
	Department of Public Safety							
12	CBI Automated Fingerprint Identification System (AFIS) Replacement	14-Apr-11	25-Jun-13	$7,656,019	$1,709,352	85% complete		To support criminal fingerprint identification, applicant and licensee background checks, and to process latent fingerprints from crime scenes in support of criminal investigations. AFIS is used by CBI
13	MAPSS: Premier One CAD Migration and Maintenance	7-Dec-10	30-Jun-14	$2,000,000	$1,988,143	30% complete		To upgrade Colorado State Patrol's (CSP) three critical communication systems to enable CSP to upgrade its Computer Aided Dispatch (CAD), Records Management System (RMS) and Mobile Data Computers (MDC) hardware and software.
	Department of Regulatory Agencies							
14	DORA Licensing System Replacement	2-Mar-10	31-Mar-13	$3,054,903	$2,277,600	97% complete		To improve overall licensing service. The new system will support approximately 175,000 licenses annually that comprise over 40 occupations.

No.	Project	Start Date	End Date	Planned Budget	Actual to Date	Status		Description
	Department of Revenue							
15	Amendment 64 Implementation	2-May-13	31-Dec-14	$0	$0	1% complete		This project is focused on the business implementation of Amendment 64 at the Department level. The implementation or business plan is broken down into three distinct phases. The business plan will require the involvement of various work units and businesses groups of the Department in order for the successful implementation.
16	CSTARS – CSN Upgrade	3-Jan-12	21-Aug-13	$464,214	$223,100	84% complete		The CSN Migration Project is the technology refresh of the existing MNT (Multi-Use Network) network. The CSN is a fully managed network and predominantly Multi Protocol Label Switching (MPLS) and Ethernet infrastructure which include network, supporting WAN termination hardware and associated maintenance, custom billing, and CSN network management. The CSTARS CSN Upgrade is a sub-project of the OIT CSN Implementation project.

No.	Project	Start Date	End Date	Planned Budget	Actual to Date	Status		Description
17	Tax Pipeline Imaging Project	6-Mar-12	31-Mar-14	$0	$0	20% complete		In the Department of Revenue Tax processing Performance Audit, issued September 2011, audit report#2157, State Auditors recommended that DOR and DPA needs to streamline the tax remittance process. A Lean project team was established to evaluate current processes, identify inefficiencies and recommend solutions (Phase 1). As a result, the decision was made to implement the recommended process improvements across both agencies.
18	System Infrastructure Refresh (SIR) Phase 1	1-Jan-13	25-Jun-13	$91,000	$31,050	74% complete		The DOR Enterprise Computing Environment (ECE) will be moved to and upgraded in a virtual environment. Scope of the project will include systems, storage and application analysis by Business Group, in addition to the configuration, migration and testing of applications in their new environment.
19	MED Inventory Tracking System	25-Jan-11	30-Sep-13	$0	$0	25% complete		The MED web-based tracking and product inventory system will be utilized by the MED, centers, grow facilities and infused product manufacturers as an employee and product tracking system.
20	OIT - Viper Upgrade	15-Aug-12	31-Oct-13	$307,515	$0	56% complete		To put new computer hardware in place that will upgrade the Viper database software.

No.	Project	Start Date	End Date	Planned Budget	Actual to Date	Status		Description
21	Tax Pipeline and Imaging Phase 3	6-Mar-13	24-Jan-14	$1,266,900	$0	19% complete		Send incoming taxation funds directly to Pueblo to be processed by IDS. An OCR system will be purchased to process Electronic images sent from Pueblo to Denver, and be uploaded into Gentax. Payments to the bank will become electronic.
	Department of Transportation							
22	CDOT SAP SRM PPS Phases 2 & 3	1-May-12	31-Dec-14	$3,497,494	$639,262	30% complete		Install and setup Procurement for Public Sector Supplier Relationship Management. This is a five phase project.
	Department of Personnel & Administration							
23	COFRS Modernization	1-Jul-12	30-Sep-14	$11,450,180	$4,977,833	13% complete		Update the Colorado Financial Reporting System (COFRS) to the current 3.9 cloud based version of the application. The existing version was implemented over 20 years ago.
	Office of Information Technology							
24	CCLAN/Internet DPA – OIT Migration	4-Mar-13	12-Nov-13	$0	$0	18% complete	Not Rated	To install and configure new networking equipment at 1525 Sherman and at the Lakewood Data Center to enable a new MPLS Core (Multiple Protocol Label Switching) and to increase network bandwidth and redundancy for state office buildings in the Capitol Complex area.

No.	Project	Start Date	End Date	Planned Budget	Actual to Date	Status		Description
25	Colorado Broadband Data & Development Program (CBDDP)	1-Jan-10	29-Jun-16	$5,361,506	$3,110,431	32% complete		To map the availability of broadband at community anchor institutions such as schools, hospitals, public safety entities and non-federal government agencies. This project is funded by a grant from the National Telecommunications and Information Administration (NTIA)
26	CSN Implementation	19-Mar-11	31-Dec-13	$0	$0	75% complete		Upgrade the existing MNT (Multi-Use Network) network. The CSN will be a fully managed network and predominantly Multi Protocol Label Switching (MPLS) and Ethernet infrastructure which will include network, supporting WAN termination hardware and associated maintenance, custom billing, and CSN network management by Century Link.
27	Data Center Consolidation (DCC) 2.0	3-Oct-11	13-July-13	$0	$0	75% complete		To initiate a fresh approach to the original DCC project started in 2009. With an upgraded network and an enterprise virtual environment, DCC 2.0 has the tools necessary to move forward with consolidating the remaining "agency" data center into OIT's two enterprise data centers.

No.	Project	Start Date	End Date	Planned Budget	Actual to Date	Status		Description
28	Data Center Consolidation CO Cloud	20-May-13	3-Mar-14	$0	$0	4% complete		The project will refresh the enterprise virtual environments and network infrastructure at our two enterprise data center locations – eFOR3T and the Lakewood Data Center; physical moves and virtual migrations of the remaining servers from CDLE, CDOT and CDPHE to the two enterprise data centers, and will include establishing/upgrading the Internet Edge at eFOR3T and the Lakewood Data Center.
29	MIPC – Managed IP Communication	30-Mar-12	15-Oct-13	$897,277	$538,383	78%		The installation and configuration of a new Cisco Unified Communications (UC) solution for the State of Colorado. The State's existing phone/network environments will be migrated to the CenturyLink managed platform.
30	SLDS - LINK	3-Jan-11	22-Oct-13	$5,290,342	$4,202,007	45% complete		To integrate and deploy an identity master data management/identity access and authentication management solution for the executive branch. To enable the integration of information from multiple state and local agencies.

Source: Governor's Office of Information Technology

This page intentionally left blank.

Appendix B

Fiscal Years 2009 through June 30, 2013
IT Expenditures

Below are the Fiscal Years 2009 through June 30, 2013 IT expenditures for each state department or branch of government.

Department/ Agency/ Branch	FY2009	FY2010	FY2011	FY2012	FY2013	Total
Agriculture	$ 203,005	$ 199,561	$ 813,800	$ 1,005,608	$ 1,006,266	$ 3,228,240
Corrections	$ 11,462,745	$ 11,333,985	$ 12,638,483	$ 13,184,154	$ 13,685,863	$ 62,305,229
Education	$ 4,033,811	$ 3,124,361	$ 3,138,975	$ 3,784,621	$ 3,246,633	$ 17,328,401
Governor's Office	$ 2,869,658	$ 25,104,799	$ 39,418,487	$137,754,540	$155,536,941	$ 360,684,426
Health Care Policy and Financing	$ 35,231,521	$ 32,788,975	$ 34,816,292	$ 43,822,219	$ 31,469,712	$ 178,128,720
Higher Education	$ 80,009	$ 89,561	$ 358,888	$ 280,204	$ 272,949	$ 1,081,611
Human Services	$121,231,180	$ 51,590,936	$ 53,780,506	$ 55,272,279	$ 49,392,873	$ 331,267,775
Judicial	$ 8,887,895	$ 7,609,914	$ 4,973,922	$ 5,805,543	$ 11,837,489	$ 39,114,763
Labor and Employment	$ 3,044,665	$ 1,992,290	$ 7,503,802	$ 8,592,308	$ 9,075,775	$ 30,208,839
Law (Attorney General)	$ 60,456	$ 68,003	$ 37,522	$ 73,188	$ 145,050	$ 384,219
Legislature	$ 58,228	$ 55,870	$ 60,711	$ 52,068	$ 68,255	$ 295,132
Local Affairs	$ 179,243	$ 167,344	$ 511,462	$ 571,355	$ 616,237	$ 2,045,641
Military Affairs	$ 252,618	$ 194,093	$ 366,597	$ 326,583	$ 455,917	$ 1,595,808
Natural Resources	$ 13,788,671	$ 12,570,700	$ 17,436,623	$ 17,834,355	$ 17,764,493	$ 79,394,841
Personnel & Administration	$ 9,166,134	$ 3,453,433	$ 4,957,705	$ 2,903,859	$ 849,023	$ 21,330,154
Public Health	$ 7,642,778	$ 7,622,233	$ 11,152,500	$ 11,956,883	$ 8,995,341	$ 47,369,734
Public Safety	$ 13,285,070	$ 13,477,336	$ 8,154,807	$ 17,966,504	$ 18,168,608	$ 71,052,326
Regulatory Agencies	$ 1,304,369	$ 1,496,940	$ 3,110,140	$ 3,474,050	$ 3,266,980	$ 12,652,479
Revenue	$ 20,746,773	$ 26,208,855	$ 22,407,760	$ 22,385,237	$ 20,081,276	$ 111,829,900
Secretary of State	$ 7,542,789	$ 7,024,437	$ 7,431,499	$ 6,478,836	$ 6,931,741	$ 35,409303
Treasury	$ 30,515	$ 31,505	$ 12,753	$ 137,191	$ 112,619	$ 324,583
Total						$ 1,407,032,124

Source: Appropriated amounts were obtained from the Fiscal Years 2009 through 2013 Long Bills. Expenditure data were obtained from the Colorado Financial Reporting System and are up through June 30, 2013. Reporting System expenditure data does not include period 13, the final closing period for Fiscal Year 2013.

The electronic version of this report is available on the website of the
Office of the State Auditor
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 1339-I

Report Control Number 1339-I