Statewide Internet Portal Authority

Performance Audit
November 2012

OFFICE OF THE
STATE AUDITOR

LEGISLATIVE AUDIT COMMITTEE
2012 MEMBERS

Representative Cindy Acree
Chair

Representative Angela Williams
Vice-Chair

Senator Lucia Guzman
Representative Jim Kerr
Senator Steve King
Senator Scott Renfroe
Representative Su Ryden
Senator Lois Tochtrop

OFFICE OF THE STATE AUDITOR

Dianne E. Ray
State Auditor

Monica Bowers
Deputy State Auditor

Sarah Aurich
Manjula Udeshi
Legislative Audit Managers

Rosa Olveda
Scott Reid
Kate Shiroff
Kara Trim
Legislative Auditors

The mission of the Office of the State Auditor is to improve the efficiency, effectiveness, and transparency of government for the people of Colorado by providing objective information, quality services, and solution-based recommendations.

Office of the State Auditor

Dianne E. Ray, CPA
State Auditor

November 15, 2012

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of the Statewide Internet Portal Authority (SIPA). The audit was conducted pursuant to Section 2-3-103(1)(b), C.R.S., which authorizes the State Auditor to conduct audits of special purpose authorities. The report presents our findings, conclusions, and recommendations, and the responses of SIPA and the SIPA Board.

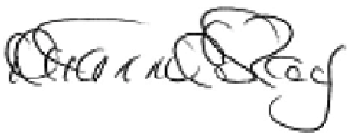

TABLE OF CONTENTS

Glossary of Terms and Abbreviations

AICPA – American Institute of Certified Public Accountants

Board/SIPA Board – SIPA Board of Directors established by Section 24-37.7-102, C.R.S.

CHFA– Colorado Housing and Finance Authority

COSO – The Committee of Sponsoring Organizations of the Treadway Commission

E-government – State or local government service provided electronically through the State Internet Portal

EFT – Electronic Funds Transfer

EGC – Executive Governance Committee

FTE – Full-time equivalent staff

Government entity– A state or local government entity, collectively government entities

IT – Information Technology

OIT – Governor's Office of Information Technology

PCI – Payment Card Industry

SAS – Statement on Auditing Standards

Statewide Internet Portal – The State's website, Colorado.gov

SIPA – Statewide Internet Portal Authority

Transaction payment engine – A system operated by Colorado Interactive that processes payments made online for government services

STATEWIDE INTERNET PORTAL AUTHORITY
Performance Audit, November 2012
Report Highlights

Dianne E. Ray, CPA
State Auditor

Statewide Internet Portal Authority

PURPOSE
To determine whether there are effective internal controls in place at the Statewide Internet Portal Authority (SIPA) over contracts, financial activities, and information systems.

BACKGROUND
- SIPA, a political subdivision of the State, was created to bring e-government solutions to government entities and the public they serve. SIPA contracts with third-party vendors to provide the statewide internet portal, "Colorado.gov" and to provide services to its clients (i.e., government entities), including website hosting, payment processing, custom application development, and software applications such as Google Apps.
- SIPA provides services to more than 260 government entities and through its contract with Colorado Interactive processed $252 million in payments for government service transactions in Fiscal Year 2011.

OUR RECOMMENDATIONS
SIPA and the SIPA Board should:
- Improve provisions in its contract with Colorado Interactive to better ensure that sensitive data is protected and that there is a comprehensive disaster recovery plan that ensures continuity of operations and appropriate notifications in the event of a breach.
- Develop contract monitoring policies, train staff on the policies, document contract monitoring efforts, and include measures in staff performance evaluations for contract monitoring efforts.
- Develop a comprehensive system of internal controls over its financial activities.
- Improve controls over expenses to ensure that expenses are reasonable, necessary, and supported by adequate documentation.

SIPA *agreed with most of the audit recommendations.*

AUDIT CONCERN
SIPA's contract administration does not provide assurance that government entity or consumer data are secure, that services will continue in the event of a disaster, or that the government entities are receiving high-quality services. Additionally, SIPA has not established a comprehensive system of controls, limitations on expenditures, or management of its risk. As a result, SIPA cannot ensure that its financial statements are accurate and complete or protect the organization from fraud and abuse.

KEY FACTS AND FINDINGS
- SIPA does not have sufficient contract provisions requiring Colorado Interactive to protect the security of the data or to develop and design a disaster recovery plan that will reduce the impact of a major disruption of key business functions and processes. Further, SIPA is not adequately monitoring the services provided by its vendors.
- SIPA has not developed a comprehensive system of internal controls to: (1) prevent financial reporting errors; (2) ensure that expenses are reasonable and necessary; and (3) prevent fraud, abuse, and noncompliance with laws and regulations. For example: the Executive Director approves his own expenses; SIPA could not document review and approval of 40 percent of the expenses we sampled totaling $100,700; SIPA's bank reconciliations are not identifying critical errors, such as $391,800 in deposits made to the wrong bank account; and SIPA lacks a centralized filing system for contracting and financial documentation.
- 272 expenses totaling $13,700 do not appear reasonable or necessary. These included $9,500 in meals charged by SIPA employees while not on travel status, and $4,200 in other expenses such as a holiday party costing $80 per person, alcohol, and over-limit and late payment fees on credit cards. Further, 69 expenses, totaling about $21,700, did not have adequate documentation to support the expense.
- SIPA has accumulated a $1.7 million fund balance, and has not established a formal policy that identifies the optimal amount of reserves needed or how to use any excess reserves to further SIPA's mission and goals.
- SIPA has not developed a comprehensive risk management plan to protect SIPA in the event of a criminal act (e.g., theft, fraud, harassment, etc.), natural disaster, or other lawsuit.

This page intentionally left blank.

RECOMMENDATION LOCATOR
Agency Addressed: Statewide Internet Portal Authority and the Board of Directors

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
1	24	Incorporate provisions into its written agreements requiring Colorado Interactive to: (a) establish a written policy for notifying affected parties in the event of a systems breach or disaster, (b) conduct regular risk assessments of its information systems and report to SIPA on identified risks and plans for mitigating the risks, and (c) implement manual and automated controls for identifying and disabling unused IDs on the transaction payment engine system and provide SIPA with quarterly reports demonstrating its management processes for user IDs.	Agree	a. February 2013 b. June 2013 c. June 2013
2	25	Incorporate provisions into its written agreement requiring Colorado Interactive's disaster recovery plan to include: (a) a business impact analysis that identifies the potential impacts to key business processes and allows Colorado Interactive to formulate and prioritize its disaster recovery efforts, (b) alternative processing plans detailing how Colorado Interactive will ensure that portal transactions can continue to be processed and that hosted websites will remain available, (c) detailed recovery steps, including identifying time frames for each step and for each disaster scenario, (d) a current list of customers and a detailed communication plan for how to contact customers in the event of an emergency, and (e) a schedule for regularly reviewing and updating the disaster recovery plan.	a. Agree b. Agree c. Agree d. Disagree e. Agree	a. September 2013 b. June 2013 c. September 2013 d. N/A e. March 2013

RECOMMENDATION LOCATOR
Agency Addressed: Statewide Internet Portal Authority and the Board of Directors

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
3	31	Develop a formal, documented, contract monitoring process that includes: (a) written policies and procedures that outline the frequency of contact with contractors and government entities, the topics to be discussed at each meeting, and a requirement for verifying the accuracy of contractor invoices prior to paying the invoices or billing government entities for the services; (b) including in the policies requirements for documenting contract monitoring activities; (c) training staff on the new contract monitoring policies and procedures; and (d) incorporating contract management outcome measures into the annual performance evaluation of any staff responsible for monitoring contracts.	Agree	a. June 2013 b. June 2013 c. September 2013 d. July 2013
4	44	Implement a system of internal controls over its financial accounting processes including: (a) establishing segregation of duties within accounts payable, accounts receivable, and journal entries; (b) limiting SIPA's access to the joint bank account to review-only access; (c) conducting monthly reconciliations of bank statements to accounting records, reviewing the reconciliations, and taking appropriate action to address concerns identified; (d) improving accounting system controls to ensure that only employees with a business need can access the accounting system; the same individual cannot enter, approve, and modify accounting transactions; user passwords are changed every 90 days; and accounting system data is archived and retained; (e) implementing a centralized record keeping system that organizes and tracks documentation of financial transactions and approvals, and retains data for at least 3 years; and (f) using additional resources to provide the financial accounting expertise needed to develop a comprehensive system of internal controls and train SIPA staff and the SIPA Board on monitoring the effectiveness of the controls.	Agree	a. March 2013 b. January 2013 c. January 2013 d. January 2013 e. July 2013 f. June 2013

RECOMMENDATION LOCATOR
Agency Addressed: Statewide Internet Portal Authority and the Board of Directors

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
5	51	Improve controls over its expenses by developing written policies and procedures that ensure SIPA expenses are reasonable, necessary, and documented. Controls should include developing written policies that: (a) define allowable and unallowable expenditures, including allowable meals and clear limitations to prevent excessive or unnecessary expenses; (b) identify documentation requirements for all types of expenses; and (c) ensure staff do not exceed credit card limits and that credit card balances are paid timely.	Agree	a. August 2013 b. August 2013 c. Implemented
6	52	Establish a policy that ensures compliance with IRS regulations for reporting taxable fringe benefits. Additionally, SIPA should contracting with a tax expert, if needed, to ensure that employees' taxable income for the past 3 years was reported accurately and to determine whether employees' taxable income for the past 3 years needs to be adjusted.	Partially Agree	August 2013
7	56	Better manage its fund balance by: (a) identifying written fund balance policy that establishes a reasonable target fund balance that aligns with SIPA's mission and goals and identifies priorities for how any monies in excess of the optimal fund balance (if applicable) should be reinvested; (b) making the fund balance policy publically available; (c) periodically evaluating SIPA's fee structure to determine whether if it can reduce fees for its services; and (d) transferring fund balance not needed to meet the monthly cash flow needs to an interest-bearing savings account.	Agree	Implemented

RECOMMENDATION LOCATOR
Agency Addressed: Statewide Internet Portal Authority and the Board of Directors

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
8	61	Develop a comprehensive risk management program for SIPA including: (a) working with an insurance broker to evaluate how much risk SIPA can afford to finance itself through self-insurance and how much risk SIPA should finance through the purchase of commercial insurance policies; (b) establishing written policies that include terms of its self-insurance policy and the amount that should be reserved for self-insurance, in the event that SIPA decides to continue self-insuring; and (c) creating a separate self-insurance fund to pay for any claims, in the event that SIPA decides to continue self-insuring.	a. Agree b. Not Applicable c. Not Applicable	a. February 2013 b. Not Applicable c. Not Applicable

Overview of the Statewide Internet Portal Authority

Chapter 1

In 2003, the General Assembly enacted Senate Bill 336 recognizing that the goal of state government should be to do more with less and provide efficient and effective services for citizens through the use of innovative technology solutions. In Senate Bill 03-336, the General Assembly recognized the need for a statewide internet portal to serve as a place where citizens can electronically access state government information, products, and services (collectively referred to as e-government services). The bill authorized the Commission on Information Management, a State commission assigned to preside over all information technology (IT) projects in the State prior to 2007, to develop a plan for implementing the statewide internet portal. To capitalize on the potential of e-government services and facilitate their implementation by public entities throughout the State, in 2004 the General Assembly enacted Senate Bill 04-244 creating the Statewide Internet Portal Authority (SIPA) [24-37.7-101 et seq., C.R.S.].

Section 24-37.7-105, C.R.S., created SIPA to bring e-government solutions to government entities and the members of the public they serve. Under statute, SIPA oversees a statewide internet portal that enables the citizens of Colorado to more easily interact and transact business with both state and local government entities. Specifically, statute requires SIPA to: (1) develop the statewide internet portal; (2) provide electronic access for members of the public, state agencies, and local governments to such information and services and explore ways to improve access to electronic information, products, and services; and (3) explore options for expanding the statewide internet portal by providing add-on services such as providing email and electronic calendaring to subscribers.

SIPA's mission is "to provide efficient and effective services for citizens through the use of modern business practices and innovative technology solutions." SIPA's 2011 business plan provides further detail about SIPA's goals, including that SIPA plans to:

- Continue developing a statewide internet portal that provides a single access point to state and local government information, products, and services and that gives members of the public an effective and efficient way to transact business.

- Increase the number of applications developed, integrated, and made publicly available by government entities on the internet portal.

- Create a grant program for government entities to accelerate their adoption of SIPA's services.

- Increase the number of eligible government entities that use the services provided by SIPA through promotion and education.

- Explore and expand the type of enterprise services and solutions offered to government entities through SIPA.

In 2007, the Commission on Information Management was dissolved and replaced with eight Executive Governance Committees (EGCs) that now serve as the advisory boards for the Governor's Office of Information Technology (OIT). OIT manages all state agency IT projects, including any projects that state agencies work with SIPA to procure, such as the recent move of all executive branch agencies to Google Apps software which includes Google email, calendar, chat, and document processing software solutions. OIT contracted with SIPA to provide Google Apps.

Administration and Operations

Section 24-37.7-102, C.R.S., establishes SIPA as a political subdivision of the State, not under the jurisdiction of any state agency. Statute creates a 13-member Board of Directors (Board) to oversee SIPA and ensure that SIPA's statutory responsibilities are met. The Board consists of three members from executive branch state agencies, one member from the judicial branch, one member from the State Senate, one member from the State House of Representatives, the Secretary of State, the Chief Information Officer from OIT, one member representing local governments, the head of one of the offices of the Governor, and three members from the private sector with backgrounds in information management and technology. The Board appoints SIPA's Executive Director, who is responsible for SIPA's daily operations and ensuring that the goals of the organization are met.

SIPA primarily carries out its mission and goals by partnering with government entities to provide them with services, including website hosting, payment transaction processing, custom application development, and software applications such as Google Apps. SIPA contracts with the following third-party vendors to provide all of these services.

- **Colorado Interactive—**manages the statewide internet portal, "Colorado.gov". It also provides content management services for government entities to help them manage their websites, designs custom websites, provides IT project management services, and develops custom applications for government entities. Colorado Interactive's primary service is processing credit card payments received from government entity customers. This payment processing is accomplished through the use of the transaction payment engine system, which receives payment information through interaction with SIPA's front-end Web applications on Colorado.gov. For each transaction, Colorado Interactive collects the fee charged for the government service plus a portal fee of $.75 and a credit card service charge of about 2.25 percent of the transaction total. Every three days, Colorado Interactive distributes the government service fees to the appropriate government entity. Colorado Interactive retains the rest of the fee revenues, pays expenses associated with processing the transactions, such as the credit card vendor fees, and distributes 7 percent of the net revenue after paying expenses, plus $37,500 per month, to SIPA. Colorado Interactive retains the rest of the fee revenues collected through the transaction payment engine. Currently, there are more than 300 users for the transaction payment engine, composed of multiple users from each of the government entities.

- **Tempus Nova—**provides Software as a Service, or a suite of Web-based software applications, hosted in the cloud, that aid businesses with collaboration and productivity. These Web-based solutions allow coworkers to: share and work on documents simultaneously even when they are working from different locations; schedule meetings for one another and check on each other's calendars from any location; and provide chat services so that coworkers can communicate at any time in different locations to resolve issues. Tempus Nova provides Google Apps software, which include Gmail, Google Talk, Google Calendar, Google Docs, and Google Videos. In Fiscal Year 2012, government entities paid about $333,300 for Tempus Nova's services and software.

- **Vertiba—**provides professional services to help government entities implement Salesforce. Salesforce is cloud-based client relationship management software that SIPA sells to government entities. A local government entity may use this software to keep track of constituents and constituent contacts or interactions. In Fiscal Year 2012, government entities paid about $177,500 for Vertiba's services and software.

It is not mandatory for government entities to procure these services through SIPA. Therefore, SIPA must compete with other vendors of similar services in the

private sector to attract clients. As a result, SIPA and its Board are focused on providing quality services at competitive prices.

SIPA is an important entity to state and local governments. Through its contractors, SIPA provides e-government services to more than 260 government entities. In Fiscal Year 2011, SIPA processed more than $252 million in payments for government service transactions.

Funding and Expenses

Section 24-37.7-107 to 108, C.R.S., requires SIPA to be self-funded and, as such, it is not appropriated any general fund revenue. Instead, SIPA funds its operations using proceeds from the sale of products, services, or information; donations; federal grants; and the issuance of bonds. Currently, SIPA's largest funding source is a percentage of the net revenue Colorado Interactive generates from the fees it charges on transactions processed through the statewide internet portal. SIPA also receives revenue from the sale of software licenses. It is important to note that SIPA pays contractors directly for all services provided to the government entities and then bills the government entities for the services provided. As a result, much of SIPA's revenues and expenses are pass-through funds. The following table shows the revenues and expenses for SIPA for Fiscal Years 2008 through 2012.

The Statewide Internet Portal Authority
Revenues and Expenses by Source and State Fiscal Year

Revenue and Expense Category	2008	2009	2010	2011	2012 (unaudited)	Percentage Change 2008-2012
Revenues						
Colorado Interactive Revenue Share	$596,300	$647,000	$710,500	$1,185,800	$1,207,000	102%
Pass-Through Revenue[1]	0	0	377,200	1,324,000	825,700	119[2]
Software License Revenue[3]	0	0	0	183,600	419,500	128[2]
Other Revenue[4]	0	0	0	63,400	0	NA
Total Revenue	**$596,300**	**$647,000**	**$1,087,700**	**$2,756,800**	**$2,452,200**	**311%**
Expenses						
Operating[5]	($338,300)	($370,200)	($348,800)	($868,400)	($523,800)[6]	55%
Professional Fees[7]	(261,000)	(300,200)	(593,600)	(1,580,500)	(1,329,300)	409
Total Expenses	**($599,300)**	**($670,400)**	**($942,400)**	**($2,448,900)**	**($1,853,100)**	**209%**
Fund Balance—Beginning of Year	**$720,900**	**$717,900**	**$694,500**	**$839,800**	**$1,147,700**	**59%**
Net Revenue	**($3,000)**	**($23,400)**	**$145,300**	**$307,900**	**$599,100**	**20,070%**
Fund Balance—End of Year	**$717,900**	**$694,500**	**$839,800**	**$1,147,700**	**$1,746,800**	**143%**

Source: Office of the State Auditor's analysis of SIPA audited financial statements for Fiscal Years 2008 through 2011, and of unaudited reports from SIPA's accounting system for Fiscal Year 2012.

[1] SIPA pays its contractors directly and bills the government entity, thus this revenue is passing through SIPA from the government entity to the contractors.

[2] The percentages for pass-through revenue and software license revenue are calculated from 2010 to 2012 and 2011 to 2012, respectively, because the category did not exist prior to 2010 and 2011, respectively.

[3] Software license revenue includes both pass-through revenue (funds received from government entities for software licenses that SIPA pays to its contractors) and SIPA revenue share (revenue earned by SIPA on each software sale).

[4] Other revenue includes a grant SIPA received from the Colorado Trust to create a health provider locator website for the Department of Health Care Policy and Financing as well as funding from a sponsorship SIPA received for an event it held in Fiscal Year 2011.

[5] Operating expenses include employee wages and benefits, parking, business meals, travel, office functions, board expenses, training, marketing, office equipment and supplies, bank charges, and depreciation for Fiscal Years 2008 through 2011.

[6] Depreciation and amortization expenses are calculated by the financial auditors and have not been released for Fiscal Year 2012. In Fiscal Year 2011, depreciation was about $27,000 and amortization was $46,000.

[7] Professional fees include: charges to SIPA for its annual financial audit, consulting services for both SIPA and the government entities, contractor charges for services to the government entities, and legal and accounting services for SIPA.

As shown in the above table, SIPA increased its revenue by 311 percent between Fiscal Years 2008 and 2012. Additionally, between Fiscal Years 2008 and 2012, SIPA's total expenses increased by 209 percent. In each of the past 5 years SIPA

has carried a fund balance of nearly $700,000 or more. We discuss concerns with the increasing fund balance and SIPA's lack of a comprehensive fund balance policy in Recommendation No. 7.

Audit Scope and Methodology

We conducted this performance audit pursuant to Section 2-3-103(1)(b), C.R.S., which authorizes the State Auditor to conduct audits of special purpose authorities. Audit work was performed from December 2011 through October 2012.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of our audit were to review SIPA's contract administration practices, system of internal controls over financial activities, information technology controls, and the cost-effectiveness of SIPA services. We planned our audit work to assess the effectiveness of those internal controls that were significant to our audit objectives. Our conclusions on the effectiveness of those internal controls are described in the audit findings and recommendations. Specifically, our objectives were to determine whether:

- SIPA has controls in place to ensure that SIPA's contract with Colorado Interactive has the provisions necessary to protect sensitive data and ensure proper disaster recovery planning.

- SIPA adequately monitors its contracts with third-party vendors to ensure that high-quality services are delivered on time and within the contract budget.

- SIPA has sufficient internal controls in place, including policies and procedures that govern financial reporting, protect against fraud and misappropriation, and give the public reasonable assurance that the organization is operating efficiently, effectively, ethically, and equitably. Additionally, we evaluated whether SIPA took action to correct significant deficiencies and material weaknesses noted during its Fiscal Year 2008 through 2011 financial audits.

- SIPA expenses are reasonable and necessary and supported by sufficient documentation.

- SIPA's services and portal fees are reasonably priced and whether SIPA's fund balance and business uses of those funds align with best practices.

- SIPA is adequately managing and financing the risks to the organization.

To accomplish the audit objectives identified above, we interviewed SIPA staff and the Board and reviewed: SIPA's policies and procedures and documentation of financial transactions, electronic transaction data from Colorado Interactive, prior financial audits, Board meeting minutes, and SIPA's strategic plan. Because we found that SIPA has very limited policies and procedures governing its contract administration activities, system of internal controls, financial activities, or other business operations, we looked to nationally recognized standards bodies for guidance on internal controls, information system controls, and accounting standards. We also looked to state resources such as the State Fiscal Rules, the State Procurement Manual, and the State Cyber Security Policy for guidance against which to evaluate SIPA's business activities.

In addition, we reviewed information in three areas to provide sufficient, appropriate evidence for the purpose of evaluating SIPA's contract administration practices based on our audit objectives. Specifically, we:

- Reviewed controls over access to the transaction payment engine by reviewing 100 percent of the active user IDs to determine if all the IDs were valid and that only authorized individuals had access to the system.

- Sent three customer satisfaction surveys to government entities that use one or more of the services offered by SIPA. In total, 446 government entities received a survey, with some entities receiving more than one survey because they currently use more than one of SIPA's services.

- Evaluated the entire population of user IDs for SIPA's internal accounting system to determine if there were sufficient access controls to protect against fraud and abuse and reviewed SIPA's archiving procedures for financial data within the system.

- Evaluated the contract terms and conditions in Colorado Interactive's contract, one of SIPA's three vendors, to determine whether the contract contained provisions necessary to protect sensitive data and ensure proper disaster recovery planning.

- Reviewed SIPA's contract monitoring practices for all three of its vendor contracts to determine whether SIPA adequately oversees its contracts and ensures that contractors complete high quality work, on time, and within the contract budget.

Finally, we relied on sampling techniques to support our audit work in the areas described below. Unless otherwise indicated, we selected non-statistical judgmental samples to provide sufficient, appropriate evidence for the purpose of evaluating SIPA's system of internal controls based on our audit objectives. Specifically, we reviewed:

- A sample of 3 months of SIPA revenue from Colorado Interactive during Fiscal Year 2012 to determine if SIPA received the correct amount of revenue as specified by contract.

- A sample of data from Colorado Interactive for three state entities using the transaction payment engine to determine whether revenues paid to the state entities appeared accurate.

- A sample of 6 months of bank account statements for SIPA's joint account with Colorado Interactive for January through June 2012 to determine what type of transactions occurred, the purpose of the transactions, and the authorization for the transactions.

- A sample of expenses occurring in 2 months, December 2011 and April 2012, to determine if the 72 expenses occurring during those months were properly approved. Our sample totaled $349,100 for the 2 months.

- A sample of 176 expenses between July 1, 2010 and February 29, 2012 to evaluate whether expenses were reasonable, necessary, and supported by sufficient documentation. Our sample included expenses from the following categories: marketing, professional dues and training, Board expenses, office supplies and equipment, travel expenses, and meals. The 176 expenses totaled $186,300.

- A sample of 217 contract expenses totaling $2.8 million between July 1, 2010 and February 29, 2012 to evaluate whether contract expenses were supported by an invoice, substantiated by a contract or task order, and properly billed to the government entity.

- All adjusting entries made by SIPA for Fiscal Year 2011 to determine if the entries were properly reviewed and approved.

- All checks written by SIPA in Fiscal Years 2011 and 2012 to determine if checks were properly authorized by the appropriate SIPA signature authority.

- All of SIPA's credit card statements for the period July 1, 2010 through April 15, 2012 for each of the three active credit cards at SIPA to

determine whether credit card expenses overall appeared to be reasonable and necessary and to identify any trends in credit card expenses that could indicate potential fraud or abuse. SIPA's credit card expenses during this period totaled about $99,200. SIPA did not have credit card statements or supporting documentation from before July 1, 2010.

Additional detail about audit samples and testing results is discussed in each of the individual audit findings and recommendations.

This page intentionally left blank.

Contract Administration

Chapter 2

The Statewide Internet Portal Authority (SIPA) was created to provide electronic access for members of the public, state agencies, and local governments to information, products, and services through the statewide internet portal [Section 24-37.7.105(1)(b), C.R.S.]. Statute specifically allows SIPA to contract with outside vendors to provide internet portal services, and SIPA and its Board implemented a business structure in which SIPA does not provide any direct services. Instead, SIPA contracts with outside vendors to provide all of its services. As a result, SIPA's primary role in carrying out its statutory duties is to enter into and monitor contracts with its vendors to ensure that the state and local government entities it serves (collectively referred to in this report as "government entities") are getting high-quality services at a competitive price. As discussed in Chapter 1, SIPA currently oversees contracts with three private contractors as follows:

- **Colorado Interactive—**manages the statewide internet portal, "Colorado.gov," and works with government entities to help them manage their websites, design custom websites, provide IT project management services, and develop custom applications. Colorado Interactive collects all payments processed through Colorado.gov and distributes revenues for government service fees to the appropriate government entity. SIPA's contract with Colorado Interactive expires in May 2014.

- **Tempus Nova—**provides Google Apps software including Gmail, Google Talk, Google Calendar, Google Docs, and Google Videos. Tempus Nova sells licenses for these products to SIPA, which SIPA then resells to government entities for a set price, which is below market value yet higher than what SIPA pays to Tempus Nova. Tempus Nova also provides professional support services to help government entities migrate their current email systems to Gmail. SIPA's contract with Tempus Nova expires in May 2015.

- **Vertiba—**works with government entities to implement Salesforce software that they purchase from SIPA. Salesforce enables government entities to keep track of constituents and constituent contacts or interactions. SIPA's contract with Vertiba is open-ended and does not have a specific expiration date.

Statute facilitates the contracting process for state agencies wishing to use SIPA's services. Specifically, Section 24-37.7-102(1), C.R.S., creates SIPA as a political subdivision of the State and Section 24-101-105(1)(a)(II), C.R.S., allows state entities to contract directly with political subdivisions of the State without having to follow the State Procurement Code. As a result, agencies can enter into a contract with SIPA without going through the request for proposal and bid selection processes typically required by the Procurement Code. It is important to note that although SIPA was required by statute to obtain bids for its contract with the vendor to provide the state internet portal, it is not required to obtain bids for all types of services. SIPA, however, reports that because government entities are not required to use its services, SIPA must be able to compete with other organizations offering similar services. As a result, SIPA reports that it elected to obtain bids when it sought a contractor to provide Google Apps software.

SIPA serves about 100 state government entities (including divisions, agencies, and offices within departments) and 160 local government entities. Collectively, these entities have about 115 websites provided through the state web portal, Colorado.gov. Colorado Interactive, through Colorado.gov and its transaction payment engine, processed more than $252 million in payments for government service transactions in Fiscal Year 2011. Both taxpayers and government entities rely on the ongoing availability of SIPA's service offerings to conduct government business.

According to the United States Office of Federal Procurement Policy's *Guide to Best Practices for Contract Administration*, effective contract administration includes developing a clear, concise statement of work, preparing a plan to cost-effectively measure the contractor's performance, maintaining documentation to pay according to the contractor's performance, and processing invoices quickly and effectively. We reviewed SIPA's contract administration practices and found that SIPA could make improvements in two key areas. First, SIPA needs to ensure that the terms in its contract with Colorado Interactive are clear and contain requirements to ensure the security of data and ongoing availability of key systems. Second, SIPA needs to monitor its contracts to ensure that contractors are complying with the contract terms and providing quality services on time.

Contract Terms

As described above, SIPA currently maintains master contracts with three private contractors to make e-government solutions available to government entities. These contracts do not have specified prices or deliverables; instead, pricing and deliverables are determined in specific task orders executed between SIPA and individual government entities. SIPA acts as the middleman between its private contractors and the government entities. Specifically, once a government entity decides to procure an e-government service offered by SIPA, it enters into an

agreement with SIPA. These agreements outline the general terms of the relationship between SIPA and the government entity, such as establishing the relationship between SIPA and the government entity and SIPA's ability to provide services, if desired, in the future. The agreements also allow either entity to terminate the agreement with 60 days' notice and establish that neither SIPA nor its contractors has any responsibility for the accuracy or completeness of electronic information contained within the government entity's databases. For each specific project or deliverable, the government entity must then complete a task order with SIPA that describes the project, project deliverables, and project deadlines; identifies the contractor; and specifies the payment terms and amount. SIPA must approve each task order. SIPA's master contract with the private providers is written to automatically incorporate all task orders that SIPA executes with government entities, thereby making the contractor responsible for completing the work outlined in each task order.

What audit work was performed and what was the purpose?

SIPA contracts with three different private providers for the majority of its services. Of these, Colorado Interactive's contract is the highest risk because Colorado Interactive processes financial transactions on behalf of government entities, collects the majority of the funds that are the main source of funding for SIPA, and deals with sensitive information such as taxpayer-identifying information and credit card information. As a result, we focused our review on SIPA's contract with Colorado Interactive.

The purpose of the audit work was to determine whether SIPA's contract with Colorado Interactive contained provisions necessary to protect sensitive data and ensure proper disaster recovery planning. We reviewed SIPA's contract with Colorado Interactive and interviewed staff from SIPA and Colorado Interactive. Additionally, we reviewed controls over access to the transaction processing engine system operated by Colorado Interactive by reviewing the 327 active user IDs to determine if all IDs were valid and that only authorized individuals had access to the system.

How were results of the audit work measured?

The first step in effective contract administration is to identify a clear scope of work, including clearly stated deliverables, time frames, benchmarks, and performance standards. We compared the Colorado Interactive contract to the following guidance for information technology contracts. Although SIPA is not required to comply with the standards cited below, the standards can serve as guidance to SIPA in strengthening its contract provisions with Colorado Interactive.

- **Maintaining data security.** State Cyber Security Policy P-CISP-005 on vendor management requires all state agencies to ensure that any entity they contract with to provide IT services, including other public entities through an intra-agency agreement, meets the security requirements set forth in the Cyber Security Policy. Some of the requirements in the Cyber Security Policy include:

  - All contracts with vendors providing IT services must clearly hold the vendor responsible for maintaining the security of sensitive data and require the vendor to notify affected parties (e.g., the agency and affected Colorado residents) in the event of a breach of the security of the sensitive data.

  - Contracts with vendors must include requirements for the vendor to produce regular reports to the state agency focusing on potential risk areas such as unauthorized systems access, compromised data, loss of data integrity, inability to transmit or process data, and exception reporting.

- **Limiting user access to secure systems.** State Cyber Security Policy P-CISP-008 states that entities should provide users with the least amount of access necessary to perform their job duties. Additionally, entities should establish procedures to immediately notify IT security administrators when an employee resigns or is terminated so they can immediately remove that person's access. It is also a best practice to monitor IDs so that those that are inactive after a predetermined period of time are removed. In September 2006, American Express, Discover Financial Services, JCB MasterCard Worldwide, and Visa International formed the Payment Card Industry (PCI) Security Standards Council to manage security standards related to credit and other payment cards. The PCI Security Standards Council developed a body of standards collectively referred to as "PCI standards" that apply to all entities processing credit card transactions. One of the PCI standards requires all entities that process, store, or transmit credit card information to remove or disable all user IDs that have been inactive for more than 90 days.

- **Disaster recovery planning.** State Cyber Security Policy P-CISP-004 on Disaster Recovery states that disaster recovery plans are to be developed and designed to reduce the impact of a major disruption of key business functions and processes. The disaster recovery plan must include the following elements:

  - Alternative processing and recovery capability for all major IT services and systems. The plan must be developed and designed to

reduce the impact of a major disruption on key business functions and processes.

- Usage guidelines, such as who implements the disaster recovery plan and when, and an explanation of the roles and responsibilities of each party involved in implementing the plan.

- Contact information for parties affected by a disaster, procedures for implementing the communication process in the event of a disaster, and a process for testing the communications approach to ensure communications operate effectively.

- Specified response and recovery requirements for each time frame relative to the disaster (e.g., within the first 24 hours, we will take X action and within the next 48 hours we will take Y action).

The policy also states that disaster recovery plans should be tested regularly and revised and maintained to account for any changes in personnel, systems, or documentation updates.

The Colorado Consumer Protection Act, Section 6-1-716(2), C.R.S., requires that all entities operating in Colorado investigate possible breaches of security related to personal information of any Colorado resident and, if founded, notify the affected party of the breach. The Consumer Protection Act focuses on the issue of a security breach, which is only one component of overall data security. To provide more comprehensive protections over data, the Governor's Office of Information Technology (OIT) has established specific cyber security policies, including those noted above, that all state agencies must adhere to when contracting for IT services. The policies provide additional security over sensitive information in the State's IT systems. It is important to note that if the state agencies currently contracting with SIPA for Colorado Interactive's services had been contracting with Colorado Interactive directly, those state agencies would have been required to include these provisions in the contract, as a condition of doing business with Colorado Interactive. Therefore it is reasonable to expect SIPA to include similar security requirements in its contract with Colorado Interactive to provide the same level of security that state agencies would have if they contracted directly with the vendor.

What problem did the audit work identify?

We identified the following two concerns related to Colorado Interactive's responsibilities under its contract with SIPA.

- **Colorado Interactive has not taken some of the steps needed to protect sensitive data.** First, Colorado Interactive does not report the results of regular risk assessments it conducts on its information systems to SIPA. As a result, SIPA does not know what risks Colorado Interactive believes exist relative to its duties under the contract. Second, Colorado Interactive does not effectively manage user access to the system. We reviewed Colorado Interactive's controls over user access to the transaction payment engine system and found problems with 198 (61 percent) of the 327 user IDs we reviewed. Specifically, 170 of the IDs had been activated but never used. The remaining 28 IDs had not been used in more than 90 days, and the time since the users' last access for these IDs ranged from 113 to 371 days. IDs that are never used or not used for long periods provide attackers an unnecessary avenue for compromising systems. Finally, Colorado Interactive does not have written policies describing its methods for investigating a breach or the type of breach that would warrant notification of affected parties.

- **Colorado Interactive's disaster recovery plan is not adequate.** First, Colorado Interactive could not demonstrate that it had conducted any analysis of the potential business impacts of various disasters when developing its disaster recovery plan. Second, Colorado Interactive's disaster recovery plan does not have the following key elements: (1) alternative processing plans detailing how it will ensure that portal transactions can continue to be processed and that hosted websites will remain available; (2) detailed recovery steps, including identifying time frames for each step and for each disaster scenario; (3) a current list of customers or end users (e.g., government entities) and a detailed communication plan for how to contact customers in the event of a disaster or emergency; and (4) a schedule to regularly review, update or revise the disaster recovery plan. While SIPA staff reported that Colorado Interactive does have some of these processes in place, neither SIPA nor Colorado Interactive provided documentation that there are written plans in place that address these issues. All disaster recovery related processes and procedures should be in writing and included or at least referenced by the entity's disaster recovery plan to ensure that there is a comprehensive, centralized plan that can be accessed and implemented in the event of a disaster.

Why did the problem occur?

SIPA's contract with Colorado Interactive does not have sufficient provisions requiring Colorado Interactive to protect the security of the data. Neither SIPA's master contract, nor the individual task orders, specifically cite the Consumer Protection Act and do not have other, more specific data security requirements

with which Colorado Interactive must expressly comply. Specifically, neither SIPA's master contract nor the individual task orders expressly hold Colorado Interactive responsible for protecting sensitive data; managing user access to the system; or providing regular reports to SIPA on potential risk areas such as unauthorized systems access, compromised data, loss of data integrity, inability to transmit or process data, and exception reporting. Specifically stated contract provisions and reparations, in the event of the vendor's failure to comply with such provisions, could provide immediate and effective recourse in the event of a security breach that causes harm to a government entity or the members of the public using SIPA's services.

Further, while SIPA's contract requires Colorado Interactive to have a disaster recovery plan, SIPA's contract does not expressly require Colorado Interactive to develop and design the plan in such a way as to reduce the impact of a major disruption of key business functions and processes or to ensure that recovery efforts can be prioritized in order to minimize major disruptions. SIPA's contract with Colorado Interactive requires Colorado Interactive to "have a disaster recovery plan and this plan shall be shared with the Executive Director of SIPA (a) on a yearly basis and (b) as changes are made to the plan. The disaster recovery plan should be tested by the contractor at least once a year. The results shall be discussed with the Executive Director of SIPA." There is no further description of the disaster recovery plan in SIPA's contract with Colorado Interactive. In particular, SIPA's contract does not specify that Colorado Interactive's disaster recovery plan must include provisions for alternative processing and recovery capability for all major IT services and systems; guidelines as to who will implement which parts of the plan; a communications protocol that includes maintenance of a list of current contact information for customers or end users of the system, as well as a means for ensuring that all affected parties can be contacted in the event of a disaster; or specific response and recovery time lines for each phase in the disaster recovery process.

Why does this problem matter?

Through its contractor, Colorado Interactive, SIPA provides critical services to about 260 government entities, including processing more than $252 million in government service transactions in Fiscal Year 2011 and supporting 115 websites. A significant security breach or disaster in Colorado Interactive's systems could result in service interruptions, unintended release of sensitive taxpayer information, or loss of revenue. It is important that SIPA require Colorado Interactive to protect sensitive data and take appropriate actions to notify parties if sensitive data is breached.

Additionally, ineffective user ID management increases the risk that an attacker could obtain sensitive data within the transaction payment engine. Further, credit

card vendors such as Visa, MasterCard, or Discover could fine Colorado Interactive $50 to $90 per cardholder record that was compromised in a security breach and suspend Colorado Interactive's ability to accept credit cards because Colorado Interactive is not effectively removing and disabling user IDs. In Fiscal Year 2011, Colorado Interactive processed about 1.7 million transactions, including 1.2 million credit card transactions. If Colorado Interactive's ability to process credit cards is suspended, more than 70 government entities that use the transaction payment engine would lose their ability to accept credit card payments for services until a new credit card processor could be identified.

It is also important that Colorado Interactive have a comprehensive disaster recovery plan that includes actions that would occur in the event of a disaster, such as notifications that would need to be made, steps that would need to be taken to minimize the loss or breach of any sensitive data, and actions to undertake to get the system back online as quickly as possible. Without clearly stated requirements in the contract concerning the disaster recovery plan, it is difficult for SIPA to hold Colorado Interactive responsible for any incidents to which Colorado Interactive does not appropriately respond. Further, government entities, because they have not contracted directly with Colorado Interactive, would have limited recourse to be compensated for any losses. Additionally, without a complete list of client contact information, Colorado Interactive would be unable to quickly and efficiently notify customers of a breach or disaster.

Recommendation No. 1:

The Statewide Internet Portal Authority (SIPA) and the SIPA Board should incorporate a data protection section into the written agreements with Colorado Interactive to make it clear that Colorado Interactive is responsible for the security of data in its systems. The agreements should include specific provisions requiring Colorado Interactive to:

a. Establish a written policy discussing the circumstances under which Colorado Interactive will notify affected parties in the event of a breach or disaster related to its systems.

b. Conduct regular risk assessments for its information systems involved in providing services to SIPA clients and report to SIPA on identified risks and Colorado Interactive's plans for mitigating the risks.

c. Implement a combination of manual and automated controls for identifying and disabling unused IDs on the transaction payment engine system. The written agreements should also require Colorado Interactive to provide SIPA with quarterly reports demonstrating its management

processes for user IDs for the transaction payment engine. The reports should include, but not be limited to, user ID listings and access reports and provide documentation of Colorado Interactive's monitoring activities related to user IDs.

Statewide Internet Portal Authority and Board of Directors Response:

a. Agree. Implementation date: February 2013.

SIPA agrees with part "a" of this recommendation and will work with its contractors to develop a breach notification policy. As part of this policy SIPA will review the Colorado Consumer Protection Act.

b. Agree. Implementation date: June 2013.

SIPA agrees with part "b" of this recommendation. SIPA agrees that regular risk assessments are a good practice and it will work with Colorado Interactive to increase their regularity.

c. Agree. Implementation date: June 2013.

SIPA agrees with part "c" of this recommendation. SIPA agrees that implementing both manual and automated controls for disabling unused IDs is a warranted control and will work with its contractor to improve these controls.

Recommendation No. 2:

The Statewide Internet Portal Authority (SIPA) and the SIPA Board should incorporate into the written agreements with Colorado Interactive more specific requirements related to Colorado Interactive's disaster recovery plan. Specifically, SIPA should have a written agreement requiring Colorado Interactive's disaster recovery plan to include:

a. A thorough business impact analysis that helps Colorado Interactive identify the potential impacts to the various business processes in the event of a disaster and allows it to formulate and prioritize its disaster recovery efforts.

b. Alternative processing plans detailing how Colorado Interactive will ensure that portal transactions can continue to be processed and that hosted websites will remain available.

c. Detailed recovery steps, including identifying time frames for each step and for each disaster scenario.

d. A current list of customers or end users (government entities) and a detailed communication plan for how to contact customers and end users in the event of an emergency.

e. A schedule for regularly reviewing and updating the disaster recovery plan.

Statewide Internet Portal Authority and Board of Directors Response:

a. Agree. Implementation date: September 2013.

SIPA agrees with part "a" of this recommendation. SIPA will work with its contractor on a thorough business analysis that identifies the potential impacts to its business processes in the event of a disaster.

b. Agree. Implementation date: June 2013.

SIPA agrees with part "b" of this recommendation. SIPA will work with its contractor to incorporate the standing practices into the written disaster plan. The current plan is not sufficiently documented, however standing practices do allow for payment processing to take alternate paths within 5 minutes and allow for a mirrored image of all websites to be put in place within 15 minutes.

c. Agree. Implementation date: September 2013.

SIPA agrees with part "c" of this recommendation. SIPA agrees that a detailed document should exist which outlines the steps and timeframes necessary for recovery. SIPA will work with its contractor to document the recovery process more fully.

d. Disagree.

SIPA and its contractor have in place a notification system. Accordingly, SIPA does not feel the proposed recommendation is necessary. Utilizing a commercial notification system, customers are able to sign up to receive notifications related to outages, maintenance, upgrades, or other important announcements. This system is utilized often and allows users to easily sign up for notifications as well as to be removed quickly and efficiently. Using a commercial system is an

improved process over keeping a manual list that will quickly become dated and would require constant administration.

Auditor's Addendum:

The commercial notification system referenced in SIPA's response is not a sufficient source of contact information for all customers or end users. According to SIPA's response, customers are "able to sign up for notification…," which indicates that if users fail to sign up or to update their contact information, they will not receive notifications from the system. We were unable to determine whether this system contains contact information for all SIPA customers because SIPA did not provide us with a complete list of its customers as we requested during the course of the audit. Further, because SIPA did not disclose the existence of this system until after our audit work was completed, we were not able to assess the adequacy of the system to notify all affected users in the event of a disaster.

e. Agree. Implementation date: March 2013.

SIPA agrees with part "e" of this recommendation. SIPA agrees and will work with its contractor to create a schedule for regular reviews of its disaster recovery plan.

Contract Monitoring

The second step in an effective system of contract administration is to monitor contractors to ensure that they provide all services agreed to in the contract, that the services are high quality, and that the services are delivered on time and within budget. Because SIPA serves as the middleman between the government entity and the third party contractor, SIPA, and not the government entity, is responsible for ensuring that the contractor provides the services specified in the contract, on time, and for the agreed-upon price. Further, government entities are not billed directly by the service providers. Instead, SIPA's contractors bill SIPA for the services rendered to a government entity and SIPA pays the contractor directly. SIPA then bills the government entity for the cost of the services the entity received.

What audit work was performed and what was the purpose?

We reviewed SIPA's contract monitoring processes for its three contracts with Colorado Interactive, Vertiba, and Tempus Nova to determine whether SIPA

adequately oversees its contracts and ensures that the contractors complete high-quality work, on time, and within the contract budget. Specifically, we interviewed SIPA staff and reviewed documentation provided by contractors during update meetings and tested a sample of 217 payments totaling $2.8 million that SIPA made to contractors to determine whether the payment was supported by an invoice, could be tied back to an executed task order, and had been properly billed to the government entity. Additionally, because of concerns with SIPA's contract monitoring practices, and one instance identified during our expenditure testing of SIPA paying a contractor's invoice twice, we conducted additional analysis of SIPA's payments to contractors and corresponding billing of government entities. Specifically, we used information in SIPA's accounting system to compare the total amount paid by SIPA to contractors with the total amounts that SIPA billed to the government entities to determine whether there was a risk that SIPA had over- or under-billed the government entities for services contractors provided.

Finally, we sent three customer satisfaction surveys to government entities that used one or more of the services offered by SIPA. In total, 446 government entities received a survey, with some entities receiving more than one survey because they currently use more than one of SIPA's services. The surveys were intended to measure customer satisfaction with the following three types of services: (1) transaction processing services (provided by Colorado Interactive), (2) website services and content management software (provided by Colorado Interactive), and (3) software as a service (provided by Tempus Nova and Vertiba). We received 60 responses (13 percent) across the three surveys. On average, the majority of respondents (67 percent) indicated that they are satisfied with SIPA's services and the work conducted by Colorado Interactive, Tempus Nova, and Vertiba. However, about 33 percent of the respondents expressed some level of dissatisfaction with services. In conjunction with our audit work, these results may indicate that SIPA could increase efforts to ensure that its contractors are providing quality, timely, and cost-effective services to its customers.

How were results of the audit work measured?

Statute specifically requires SIPA to oversee the portal integrator, Colorado Interactive. Because SIPA's business model is to outsource all services SIPA offers, contract monitoring is an important activity that SIPA must perform to carry out its statutory duties and ensure that its clients are getting high-quality services at a competitive price. Further, because SIPA acts as a middleman between government entities and the contractor, SIPA needs to be in contact with both the government entity and the contractor to effectively monitor contracted work.

The United States Office of Federal Procurement Policy's *Guide to Best Practices for Contract Administration* and the State Procurement Manual offer best-practice guidance for contract monitoring. These sources suggest that contract monitors: (1) develop written policies and procedures for contract monitoring, (2) establish clear documentation requirements for monitoring activities, (3) implement processes to ensure satisfactory deliverables were provided, and (4) ensure the contractor is paid according to the contract terms.

What problem did the audit work identify?

We found that SIPA does not have formal, documented, contract monitoring practices. Specifically, SIPA does not:

- **Identify work not completed.** Although Colorado Interactive is required by contract to test the disaster recovery plan and report to SIPA on the results of the tests, we found that neither the testing nor the reporting is occurring. Further, as discussed previously, we found that Colorado Interactive is not adequately managing access to the system by deleting inactive user IDs. SIPA's monitoring efforts were not sufficient to identify that Colorado Interactive was not complying with either of these contractual security requirements.

- **Document contract monitoring activities.** SIPA staff report that they monitor their contracts by: (1) conducting biweekly meetings and receiving project report outlines from Colorado Interactive that indicate whether a project is experiencing any problems, including running late; (2) conducting weekly meetings with Tempus Nova; and (3) meeting as needed with Vertiba. We found SIPA does not maintain notes related to the meetings with Tempus Nova or Vertiba, and does not document any discussions with Colorado Interactive about how problems identified in the project outlines will be resolved. Because of the lack of documentation, we were unable to evaluate the adequacy of SIPA's monitoring of the contracts.

- **Include regular meetings with government entities concerning contracted work.** Although SIPA acts as middleman between the government entity and the contractor for all contracted services, we found SIPA does not meet regularly with the government entities related to the progress and quality of contracted work to ensure that any problems with the contractor's work can be identified and rectified.

- **Monitor the timeliness of project completion.** Although each task order contains a specific deadline for completion of the work to be performed by the contractor, SIPA does not document when projects are completed.

SIPA staff specifically reported that they do not monitor the timeliness of project completion because it would be too difficult to determine whether the delays were the result of contractor negligence or government entity irresponsiveness.

- **Consistently ensure government entities are billed correctly for services.** SIPA does not always compare the invoices received from its contractors to the payment terms and project budgets contained in the task order prior to paying a contractor. SIPA staff said that they sometimes review the invoices and compare them with the task orders prior to payment, however, staff report that they have a pretty good understanding of the outstanding task orders and amounts, and therefore do not believe formal review is always needed. After paying the contractor's invoice, SIPA then bills the government entity, relying primarily on the government entity to identify any billing discrepancies for the services provided by the contractor. Because SIPA staff do not have a formal or documented process of reviewing contractor billing, we could not verify the adequacy of SIPA's review process.

We did not find any exceptions with respect to the sample of contractor payments we tested. We do have concerns related to the total amount SIPA paid to contractors as compared with the amounts that it billed to government entities. For Fiscal Years 2010 through 2012 SIPA's accounting records indicate that, in aggregate, SIPA billed government entities approximately $262,400 more for services than SIPA paid its contractors. This could indicate that SIPA may have over-billed government entities for contractual services. During the same period, SIPA paid approximately $230,400 more for software licenses than it has received in payments from government entities, indicating SIPA may have under-billed government entities for licenses. Alternatively, these discrepancies could be the result of errors in SIPA's accounting system or a combination of billing and accounting issues. To identify the cause of the discrepancy, SIPA would need to tie each contractor invoice it paid and each invoice it sent to a government entity back to the accounting system entries to ensure all payments and receivables were categorized correctly and that government entities were billed the appropriate amount for services rendered.

Why did the problem occur?

While the Executive Director's job description specifically requires him to monitor contracts, SIPA does not have any written policies concerning how contracts should be monitored. The SIPA Board does include contract monitoring as one of the components of the Executive Director's performance evaluation; however, there was no evidence in the Board meeting minutes that the Executive Director provides formal updates to the Board on his contract monitoring

activities, or that the Board has specific measures or criteria for evaluating the Executive Director's contract monitoring activities.

Why does this problem matter?

Without a well-documented, consistent process for contract monitoring, SIPA cannot demonstrate that its contractors' work is completed on time, within budget, or according to contract terms. Without documented contract monitoring efforts, including tracking project completion and documenting discussions with contractors and government entities regarding any performance issues, SIPA could have difficulty determining the root cause of any project delays or difficulties or building a case for breach of contract in the event a contractor does not perform.

Further, the lack of a comprehensive system of monitoring contractors, including a system that always matches contractor bills with task orders and work completion deadlines, can result in over- or under-billing and projects that are not completed timely. SIPA will need to review its invoicing and task orders for this period to determine whether any entities were over- or under-billed for services.

Recommendation No. 3:

The Statewide Internet Portal Authority (SIPA) should work with the SIPA Board to develop a formal and documented process for contract monitoring that ensures that contractors are completing quality work on time and within budget. At a minimum, this process should include:

a. Developing written policies and procedures that outline the frequency of contact with contractors and government entities; the topics to be discussed at each meeting, such as checking on project deliverables, deadlines, and outstanding problems; and a requirement for verifying the accuracy of contractor invoices prior to paying the invoices or billing government entities for the services. The verification should include a comparison of contractor invoices to the associated task order, information obtained during monitoring meetings on work completed, and previously paid invoices.

b. Including requirements in the written policies and procedures for documenting contract monitoring activities. Documentation requirements should include creating a file for each contract that includes the executed contract; all task orders; all contractor invoices and government entity bills; spreadsheets or other mechanisms to track ongoing monitoring of contractors; and notes from meetings with contractors and government

entities that discuss the contractor's adherence to all contract provisions, and resolution of any outstanding problems.

c. Providing training to all staff responsible for monitoring contracts on the new policies and procedures.

d. Incorporating contract management outcome measures, including adhering to the contract monitoring policies, into the annual performance evaluation of any staff responsible for monitoring contracts.

Statewide Internet Portal Authority and Board of Directors Response:

a. Agree. Implementation date: June 2013.

SIPA agrees with part "a" of this recommendation and will work with the necessary stakeholders to develop policies and procedures which will outline the frequency of contact with contractors and government entities.

b. Agree. Implementation date: June 2013.

SIPA agrees with part "b" of this recommendation and will work with the necessary stakeholders to develop a formal and documented contract monitoring process and policy.

c. Agree. Implementation date: September 2013.

SIPA agrees with part "c" of this recommendation and will train any responsible parties on the policies and procedures that are implemented.

d. Agree. Implementation date: July 2013.

SIPA agrees with part "d" of this recommendation and will incorporate contract monitoring outcome measures in the evaluation of responsible staff members.

Internal Controls

Chapter 3

The Statewide Internet Portal Authority (SIPA) was created under Section 24-37.7-101, et. seq., C.R.S., to provide one-stop access to electronic information, products, and services so that members of the public can conduct business online with state agencies and local governments (government entities). In Fiscal Year 2011, SIPA, through its contractor Colorado Interactive, processed more than $252 million in transactions on behalf of more than 70 different government entities (including individual agencies, divisions, and programs). Further, SIPA, through its contractors, provides website development and hosting to approximately 100 government entities and software applications to 55 government entities.

SIPA's operating revenue primarily comes from a percentage of the net revenue Colorado Interactive generates from the fees it charges on transactions processed through the statewide internet portal. SIPA determines the fees that Colorado Interactive charges in addition to the fee for the government service, including a portal fee of $.75 per transaction, and a credit card service charge of 2.25 percent on each transaction. As such, SIPA is funded with a portion of the fees paid by taxpayers when purchasing government services electronically through the state portal. SIPA is responsible for how those funds are spent, for operating efficiently and effectively, and for charging fees that are reasonable. Additionally, SIPA and its contractor are responsible for the collection and distribution of hundreds of millions of dollars belonging to government entities and, as a result, it is critical that SIPA and its contractor make every effort to ensure that those funds are safeguarded and distributed to the appropriate government entity.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 1992 issued *Internal Control – Integrated Framework* to help businesses and other entities assess and enhance their internal control systems. Internal controls help provide assurance that risks to the organization such as errors, fraud, abuse, or noncompliance with laws and regulations will not prevent the organization from meeting its goals and objectives. Additionally, an effective system of internal controls helps to ensure that the organization's financial statements are presented accurately. The COSO internal control framework identifies five key components to an effective system of internal controls, including:

- **Control Environment—**The culture of accountability and "tone at the top" of an organization, including the expectations surrounding the integrity, ethical values, and competence of the organization's people.

- **Risk Assessment—**The identification and analysis of relevant internal or external risks to the organization that could prevent the organization from achieving its objectives.

- **Control Activities—**The policies and procedures that help ensure management directives are carried out. Control activities may include approvals of various transactions and activities, reconciliation of key accounts, review of operating performance, security of assets, and segregation of duties.

- **Information and Communication—**Information about the internal control structure must be identified, captured and communicated to the organization's staff in a form and time frame that enable people to carry out their responsibilities. All personnel must understand their role in the internal control system and receive a clear message from top management that control responsibilities must be taken seriously. Further, information about the organization's internal controls structure should be communicated with key external parties, such as the board of directors.

- **Monitoring—**Internal control systems should be monitored to assess the quality of the system's performance over time. Ongoing monitoring, including regular management and supervisory activities, is needed as well as periodic formal review of internal control processes as the organization changes.

According to COSO, everyone in an organization shares responsibility for the internal control environment. The responsibilities of each level of the organization include:

- **Management—**The chief executive officer is ultimately responsible for the system of internal controls, and more than any other individual, sets the "tone at the top" that affects integrity and ethics throughout the system of internal controls.

- **Board of Directors—**Provides governance, guidance, and oversight. Effective board members are objective, capable, and inquisitive and have knowledge of the entity's activities and control environment, and commit the time necessary to fulfill their board responsibilities. A strong, active board is often best able to identify and correct weaknesses in the internal controls system.

- **Other Personnel—**Internal control is the responsibility of everyone in an organization and therefore should be part of everyone's job description.

The COSO Internal Control framework guided our review of SIPA's internal control structure.

Sound financial management is a fundamental responsibility of any business and especially for entities primarily funded with public funds or critical to governments' conduct of business. Financial management is comprised of a number of factors, including a comprehensive system of internal controls, effective and efficient management and investment of resources, and mitigation of risk. We reviewed financial management practices at SIPA and found that SIPA needs to improve its financial management practices by: (1) developing a comprehensive system of financial controls, (2) improving management of its expenses, (3) developing a fund balance policy that aligns with SIPA's organizational objectives, and (4) evaluating its risks and identifying an appropriate risk management (insurance) program to mitigate SIPA's risk of loss.

Financial Controls

In 2010 and 2011, SIPA significantly expanded its service offerings and marketing and outreach efforts to state and local governments. As a result, SIPA's revenues have increased by more than 300 percent, expenses have increased by more than 200 percent, full-time-equivalent (FTE) staff have increased from two to three and SIPA added a part-time contract accountant. SIPA's three FTE are responsible for generating new business through outreach efforts aimed at generating contracts with government entities; identifying and making new services available to government entities; carrying out personnel and administrative processes; and overseeing the contractors that provide government entities with Web portal and website development and hosting services, transaction payment processing services, and Google and other software applications. Additionally, these three FTE, along with the contract accountant are responsible for conducting all accounting functions.

The payments collected by Colorado Interactive, including the transaction fees mentioned previously, are deposited into a bank account owned jointly by SIPA and Colorado Interactive. This account is known as the "joint bank account." Of these payments, the fee charged for the government service (e.g., vehicle license renewal) is distributed to the government entity, and the remaining amount goes to Colorado Interactive. The joint bank account is a "clearing" account, and Colorado Interactive uses an internal computer program to calculate the amounts that go to each government entity. The program clears the account every 3 days, distributing revenues to the government entities via electronic funds transfer (EFT) and to Colorado Interactive's bank account, held by its parent company

National Information Consortium. Colorado Interactive later sends an EFT payment to SIPA for its share of the revenue. Specifically, Colorado Interactive distributes 7 percent of net revenue [gross revenue after payment of government entities and Colorado Interactive's operating expenses] plus $37,500 per month to SIPA, per the contract between SIPA and Colorado Interactive. About $252 million flowed through this account in Fiscal Year 2011.

What audit work was performed and what was the purpose?

The purpose of our audit work was to determine whether SIPA has sufficient internal controls in place, including policies and procedures that govern financial reporting, protect against fraud and misappropriation, and give the public reasonable assurance that the organization is operating efficiently, effectively, ethically, and equitably. We reviewed SIPA's system of internal controls, including SIPA's financial policies and procedures related to processing the receipt of payments and the approval of expenses. Our review included:

- A judgmentally selected, non-statistically valid sample of 3 months of SIPA revenue from Colorado Interactive during Fiscal Year 2012 to determine if SIPA received the correct amount of revenue as specified in its contract with Colorado Interactive.

- The joint bank account between SIPA and Colorado Interactive including: (1) identifying the individuals with access to the joint bank account; (2) reviewing the type of access each individual has; and (3) reviewing all joint bank account statements for January through June 2012 to determine if there had been any transfers or withdrawals from the account, the purpose of the transfers/withdrawals, and the authorization for each transfer/withdrawal.

- A sample of expenses occurring in 2 months, December 2011 and April 2012, to determine if the 72 expenses occurring during those months were properly approved. Our sample totaled $349,100 for the 2 months sampled.

- All adjusting entries made by SIPA for Fiscal Year 2011 to determine if the entries were properly reviewed and approved.

- SIPA's financial audits, conducted by Clifton Gunderson, for Fiscal Years 2008 through 2011 to evaluate whether SIPA had addressed the material weaknesses and significant deficiencies identified in these audits. When a financial statement audit identifies deficiencies in the system of internal controls, the auditors are required by the Statement on Auditing Standards

(SAS) 115 to classify each deficiency based on its severity. According to SAS 115, material weaknesses in internal controls are the most serious; they represent deficiencies that create a reasonable possibility that a material misstatement of SIPA's financial statements will not be prevented, detected, or corrected on a timely basis. Significant deficiencies are less severe, but according to SAS 115 are important enough to merit attention by those charged with governance.

How were the results of the audit work measured?

We used the following criteria in evaluating SIPA's system of internal controls. According to the COSO framework, a key component of an effective system of control activities is the appropriate segregation of duties. According to the American Institute of Certified Public Accountants (AICPA), segregation of duties is intended to prevent and detect fraud by requiring more than one person to be involved in the: (1) custody of assets, (2) authorization or approval of related transactions affecting those assets, and (3) recording or reporting of related transactions. Specifically:

- For **Accounts Receivable,** the standards indicate that a single person should not receive and log payments, record the payments into the accounting system, and make the deposit for payments received into the bank account. When a payment is received, the payment should be checked and credited against the appropriate outstanding receivable and recorded as a cash receipt. If paid by check, the check should then be deposited into the appropriate bank account. Giving the same individual access to receive checks, record payments received in the organization's accounting system, and make deposits increases the risk that fraud and abuse can occur and go undetected.

- For **Accounts Payable,** the standards indicate that a single person should not create new vendors, approve invoices or credit card statements for payment, write checks, enter the payment, and credit accounts payable in the accounting system. To ensure that expenses are reasonable, necessary, and supported by appropriate documentation, it is important for someone other than the person making the expense (or paying the invoice) to review and approve the expense.

- For **adjusting entries,** the standards indicate that a single person should not enter and approve an adjusting entry in the accounting system. Adjusting entries can be used to significantly change how transactions are shown in the financial statements, and as a result, it is important that the entry and approval functions for adjusting entries be properly segregated to retain the integrity of the financial statements.

- For **access to bank accounts or the accounting system,** the standards indicate that only individuals that have a business need to access the system or bank account should be given access privileges. Allowing individuals to access bank accounts when there is no business need for them to do so increases the risk of theft, fraud, or misappropriation of assets in the account.

In addition, AICPA Internal Control Guidance (based on Statements on Auditing Standards 109 and 110) dictates that entities should perform periodic reconciliations of asset and liability accounts. Reconciling bank statements to cash receipts and accounts receivables on a routine basis helps to ensure that payments received are recorded properly in the accounting records and deposited into the correct bank account in a timely manner. To ensure proper segregation of duties, the person who approves transactions or handles cash receipts should not be the person who performs the reconciliation. Reconciliations should be documented and approved by management.

Finally, the system of internal controls should be documented. The September 2009 edition of the Journal of Accountancy issued an article titled *Understanding Internal Control and Internal Control Services* which stated that all controls and their operation need some documentation. Maintaining records is an organization's primary mechanism of documenting and monitoring its internal control structure and documenting its business activities to provide transparency and accountability to stakeholders and oversight bodies. SIPA is not subject to state archiving rules. However, the Colorado Records Management Manual provides guidance that SIPA could look to when determining the appropriate retention period for documentation of financial activities. Specifically, the Colorado Records Management Manual, Schedule 7: Financial Records, Part D, Cash Management, states that documentation of transactions with external bank accounts, including deposit slips, cancelled checks, debit/credit memos, bank statements, bank reconciliations, and cash and credit card receipts should all be retained for a minimum of 3 years. Retaining records also helps to ensure accountability to present and future stakeholders.

What problems did the audit work identify and why do the problems matter?

SIPA has not addressed significant deficiencies and material weaknesses in internal controls noted in financial audits for Fiscal Years 2008, 2009, 2010, and 2011 and has not yet developed a comprehensive system of internal controls. During this audit, we identified deficiencies in internal controls in four areas: (1) segregation of duties, (2) reconciliation, (3) accounting system controls, and (4) record keeping. We outline our concerns below.

Segregation of Duties

- **Accounts Payable**—We found problems in two areas related to accounts payable: (1) SIPA does not have a system of review and approval of the Executive Director's credit card expenses; SIPA's Executive Director approves his own credit card statements for payment. Between July 2010 and April 2012, the Executive Director made about 480 credit card expenses totaling about $69,400. (2) SIPA does not have written policies in place to document the review process over payment of other invoices. However, according to SIPA staff, the administrative assistant receives the invoice from the contractor and emails the Director to seek approval for payment of the invoice. The Executive Director reviews the email and responds with an approval of the invoice. Finally, the Executive Director stated that his signature on the check was additional evidence of approval of the expense. We reviewed a sample of 72 invoices totaling about $349,100 to determine whether SIPA could document this approval process. We found that SIPA could not provide documentation that this review and approval process had occurred for 29 (40 percent) of the 72 invoices we sampled. These 29 invoices totaled $100,700, or about 29 percent of the dollar amount we tested. Further, we reviewed all 557 checks written in Fiscal Years 2011 and 2012 to determine if the Executive Director had signed the checks. We found three checks, totaling about $41,300 that had not been signed at all before being mailed out and cashed by the payee. These three checks occurred in a two-month period, representing 13 percent of all checks issued in those 2 months. Two of the three checks were for more than $18,000 each and without a signature; SIPA has no documentation that these payments were approved. Together, these findings indicate that SIPA's reported process for reviewing and approving expenses is not working effectively.

- **Accounts Receivable**—We found that the same SIPA employee receives checks, prepares and executes batch deposits for checks received, and enters receipt of payment into SIPA's accounting system. In total, this employee deposited approximately $756,000 in checks between January and June 2012. Additionally, we found that the batch deposits are not reviewed by a third party or compared with bank deposit records to ensure the deposit was made.

- **Adjusting Entries**—SIPA does not have appropriate controls over adjusting entries. Specifically, adjusting entries can be made in the accounting system without review or approval by a person other than the person making the entry. We reviewed all 12 of the adjusting entries in SIPA's accounting system for Fiscal Year 2011. These 12 entries totaled $405,600. Four of the adjusting entries, totaling nearly $24,700, were

made with no documentation of why the adjustment was necessary or evidence of review or approval by someone other than the person that made the adjusting entry. The remaining 8 entries, totaling $380,900, were made appropriately because they were recommended by the external auditor and entered into the system by SIPA staff to correct errors made in the accounting system.

- **Access to Joint Bank Account—**We found that two SIPA employees have unlimited access to withdraw funds from the joint bank account with no business purpose for having that access. The funds in the joint bank account primarily belong to the government entities and Colorado Interactive. Under its contract with SIPA, Colorado Interactive is responsible for disbursing all funds from the account. We found one instance in which SIPA staff transferred $109,800 from the joint account to SIPA's bank account by mistake. The SIPA employee corrected the mistake on the same day. However, the error could have been avoided entirely if SIPA staff had no access to withdraw funds from the account and instead had review-only access. On average, SIPA carries a balance of about $2 million in the joint bank account each month.

Reconciliation

As discussed, Colorado Interactive is responsible for managing the joint bank account that receives all payments for transactions processed through the transaction payment engine. SIPA is responsible for managing its operating account, which is the bank account that SIPA uses to deposit its revenues and pay its expenses. During our review of SIPA's financial management practices, we found that SIPA's reconciliation of bank statements to accounts receivables or cash receipts shown in the accounting system are not effective.

SIPA provided some documentation of reconciling its operating account bank statements to its accounting records, including the balance of cash in its operating account and cleared checks, deposits, and other withdrawals. However, we found several accounting errors resulting in SIPA's accounts receivables or cash being improperly stated in its financial accounting system that indicate that SIPA's reconciliation processes are ineffective. Specifically, we found the following errors that would have been identified by SIPA staff if they had followed up on errors or questionable items identified in the reconciliations.

- **SIPA did not routinely identify or address incorrect deposits.** We identified a total of $391,800 for seven deposits that were mistakenly deposited into the joint bank account rather than SIPA's operating bank account between August 2011 and February 2012. These incorrect deposits occurred because the bank erroneously linked SIPA's lockbox and ATM card for its operating account with the joint bank account. As a

result, when SIPA made a deposit using its operating account lockbox or ATM card, or if a government entity sent a payment directly to SIPA's operating account lockbox, the funds were deposited by the bank into the joint bank account.

We found that although SIPA had prepared reconciliations of the operating bank account with its accounting records during the time these errors were occurring, SIPA did not take any action to investigate or correct potential problems identified in the reconciliations. For example, one of SIPA's reconciliations indicated an uncleared deposit of about $125,800. Uncleared deposits could be a sign of a serious problem, such as a payment being drawn on an account with insufficient funds or accounting errors at the bank. However, SIPA staff did not follow up on the uncleared deposit and only corrected the erroneous deposits after Colorado Interactive notified SIPA of the problems. Ultimately SIPA staff made seven transfers from the joint bank account to the operating bank account to correct these errors, but not for 2 to 6 months after the original deposits were made. As a result, the funds remained in the wrong bank account for more than 2 months and SIPA's cash receipts in its accounting system were overstated for the same period. We found an additional $42,500 in uncleared deposits reflected in SIPA's bank reconciliations for 3 months before SIPA resolved them.

SIPA has since worked with Colorado Interactive and the bank to correct the problem with the lockbox and ATM card, and therefore should not have further need to withdraw or transfer funds from the joint account.

- **SIPA did not record receipts timely.** We found that SIPA did not record an electronic payment of $110,900 as cash received in the accounting system for 45 days after receipt of the funds. As a result of not recording this transaction timely, SIPA's accounting records for cash and accounts receivable were not accurate and could result in: (1) SIPA double-billing for a receivable that was not recorded as paid, or (2) SIPA's financial statements being inaccurate.

Accounting System Controls

SIPA has not properly secured access to its accounting system or ensured the safety of historical data in its accounting system. We identified problems in two areas. First, SIPA has not restricted user access to ensure that the same person cannot enter, approve, and modify entries in the accounting system. We found that all four user IDs in SIPA's accounting system have unrestricted access to the system, meaning that all staff that can access the system are allowed to enter, approve, and modify transactions in the system. Second, we found that SIPA is not properly managing user IDs for the accounting system. Specifically, we

found: (1) one of the four active IDs to access the system belonged to an employee that terminated employment about 5 months prior to our review, (2) passwords for all four user IDs have not been changed since the system's implementation in 2009, and (3) financial data within the system has never been archived. The lack of effective ID management within the accounting system could result in improper access, unauthorized modification of financial data, or shutting down the accounting system. Finally, not archiving data can result in the loss of transaction-level details from prior accounting periods and the inability to review older data if needed.

Record Keeping

During our review of SIPA's financial management practices, we found that SIPA does not have a comprehensive system of record keeping for its key business activities. Specifically, we found:

- **SIPA does not retain financial records for a sufficient period of time.** SIPA keeps most of its financial records, such as documentation of expenses including invoices and some receipts, for 2 fiscal years. Other financial information, such as documentation of its batch deposits, including a record of each check that was included in the batch deposit, is maintained only through bank records, which the bank keeps on file for only 90 days. As a result, once that period expires, without other documentation retained by SIPA it is difficult to determine what payments were included in which deposits. Typically, financial records should be maintained for a minimum of 3 years to ensure adequate documentation is available to address these needs.

- **SIPA does not maintain a central filing system for records pertaining to accounts receivable, accounts payable, contracts, or contract monitoring files.** For example, SIPA reported that it could not provide information on the total number of task orders that have been executed during Fiscal Year 2012 without going through a highly labor intensive, manual process. Additionally, SIPA's financial records are scattered throughout its accounting system and individual staff email accounts, making it difficult for oversight entities to review transaction-level detail or for SIPA to pull together historical documentation should an issue arise with a client or contractor. Further, maintaining important business documents in employee email records can be problematic when it comes to reconstructing documentation of business activities by anyone in management that needs to access those records. Email is not a sufficient or reliable system of record keeping and in the event something happens to an employee, using an informal system of maintaining key records in various employee email files could cause management or another oversight body difficulty in rebuilding any financial information lost.

Without an effective system of internal controls, SIPA cannot ensure that its financial statements are accurate and complete or protect the organization from fraud and abuse. Further, an effective system of internal controls helps the organization to ensure expenses are reasonable and necessary and supported by sufficient documentation. SIPA provides the internet portal for more than 260 government entities, provides more than 100 websites, and processed more than $252 million in transactions for government services for Fiscal Year 2011. If SIPA were to fail or experience a significant disruption in service, many government entities would struggle to find a new service provider to accept payments for services online. Further, a fraud affecting the joint bank account could result in government entities losing significant amounts of money.

Why did the problem occur?

SIPA staff and the SIPA Board report that the financial auditors minimized the seriousness of the deficiencies cited in the financial statement audits for Fiscal Years 2008 through 2011. As a result, neither SIPA staff nor the Board has taken significant action to address material weaknesses in internal controls. Additionally, SIPA management has indicated that SIPA's limited staff resources prohibit the implementation of effective controls and that these resources are better directed toward activities that are more directly aligned with accomplishing SIPA's mission, such as increasing the applications and IT solutions it makes available to SIPA clients and increasing the number of government entities using SIPA's services. We understand that SIPA must prioritize the use of its resources, but addressing material weaknesses in SIPA's internal controls is an activity that can help both management and the SIPA Board to ensure that the organization's objectives are not undermined by fraud, abuse, noncompliance with laws, or mismanagement of the organization's assets.

At an operational level, SIPA does not have sufficient written policies or procedures establishing a comprehensive system of internal controls. First, SIPA has not developed written policies that establish clear processes for segregating duties for key financial processes, including accounts receivable, accounts payable, or adjusting entries. Second, SIPA does not have a written policy requiring periodic reconciliation of its accounting records to bank statements for the operating account or describing how those reconciliations should be done, who should review the reconciliation, and how any anomalies identified through the reconciliations should be addressed. Third, SIPA has not established a written policy for how it will review revenue it receives from Colorado Interactive to ensure it is accurate. Finally, SIPA has not developed policies and taken action to properly limit access to either its financial accounting system or to the joint bank account to only those individuals with a business need to access those systems and accounts.

Neither SIPA management nor SIPA staff have financial accounting backgrounds and do not have the expertise necessary to establish a comprehensive system of internal controls or proper accounting and record keeping practices. Further, the contract accountant primarily performs bookkeeping functions and has not conducted a thorough review of SIPA's internal control structure.

Although SIPA has a small staff and currently lacks the expertise to identify and implement a comprehensive system of internal controls, among the three staff and the Board, SIPA should be able to implement controls related to: (1) custody of assets, (2) authorization or approval of related transactions affecting those assets, and (3) recording and reporting of related transactions. First, the Board should review and approve the Executive Director's expenses, including credit card statements for payment on a routine basis. Second, SIPA could separate certain duties among its three staff members. For example, once a Board member reviews and approves each of the Executive Director's expenses, prior to payment, the documented approval could be forwarded to a staff member who would enter the payment into the accounting system and prepare the check. The Executive Director could sign the check. The Board could periodically hire outside expertise to conduct a review of the internal control system to ensure that improvements have been implemented properly and that the system of controls is operating effectively.

Recommendation No. 4:

The Statewide Internet Portal Authority (SIPA) should work with the SIPA Board to implement a stronger system of internal controls over its financial accounting processes. The system of internal controls, at a minimum, should be documented within written policies and, at a minimum, accomplish the following:

a. Establishing proper segregation of duties within the following functions: (1) accounts payable; (2) accounts receivable; and (3) journal entries.

b. Limiting access to the joint bank account to review-only access in which SIPA can review deposits and withdrawals from the account, but SIPA staff should not have access to withdraw funds from the account.

c. Conducting monthly reconciliations of bank statements to accounting records. Reconciliations should be performed by a person other than the individual recording the transactions or making the deposits and the reconciliation should be reviewed by a person that did not complete the reconciliation. SIPA should retain documentation of the reviewed reconciliation and establish a process for following up on any concerns identified by the reconciliation.

d. Immediately removing access in SIPA's accounting system when staff terminate employment with SIPA and ensuring that only employees with a business need can access the accounting system; ensuring proper segregation of duties within the accounting system so that the same individual cannot enter, approve, and modify accounting transactions; ensuring user passwords are changed at least every 90 days on the accounting system; and identifying and implementing an annual data archive process for information on the internal accounting application and identifying a data retention policy for archived data.

e. Developing and implementing a centralized, comprehensive record keeping system that organizes and tracks documentation of financial transactions, including documentation of expenses, approval of invoices and payments, documentation of deposits, and reconciliations of accounts. Additionally, SIPA should retain documentation for a minimum of 3 years.

f. Identifying and using additional resources, as needed, to provide financial accounting expertise to work with SIPA staff to develop a comprehensive system of internal controls and train SIPA staff and the SIPA Board on monitoring the effectiveness of the system of controls once it is in place.

Statewide Internet Portal Authority and Board of Directors Response:

a. Agree. Implementation date: March 2013.

   SIPA agrees that internal controls are a necessity and that continuous improvement in this area should always be a goal. SIPA will work with its Board and contract accountant to improve its internal controls and increase its segregation of duties.

b. Agree. Implementation date: January 2013.

   SIPA agrees that it should limit access to the joint bank account and will work expediently to make these adjustments to the account settings. It is important to note that while the settings or access rights are in need of revision the OSA reports no fraudulent activity with these accounts.

c. Agree. Implementation date: January 2013.

SIPA agrees with this recommendation and will work with its staff and contract accountant to design a different approach to how it is currently conducting reconciliations.

d. Agree. Implementation date: January 2013.

SIPA agrees with this part of the recommendation and will work with staff and its contract accountant to implement it immediately.

e. Agree. Implementation date: July 2013.

SIPA agrees with part "e" of this recommendation. SIPA currently utilizes several systems to perform its operations and is in the process of implementing a Client Relationship Management (CRM) system that can further aid it in organizing documentation. SIPA will continue to implement this system and will utilize its features and functions to organization and track necessary documentation.

f. Agree. Implementation date: June 2013.

SIPA agrees with part "f" of this recommendation. SIPA will work to develop a comprehensive system of internal controls and will seek the consultation of appropriate individuals throughout the process.

Expenses

SIPA spent about $1.9 million in Fiscal Year 2012. About $1.3 million of these expenses were for professional services, including pass-through expenses that SIPA incurred to pay for services provided to government entities by one of the three contractors with whom SIPA contracts. SIPA then recoups these expenses by billing the government entity for the services SIPA paid the contractor to provide. Additionally, in Fiscal Year 2012 SIPA spent about $523,800 on operating expenses, including staff salaries and benefits, training, office supplies, and other expenses.

What audit work was performed and what was the purpose?

The purpose of the audit work was to determine if SIPA expenses are reasonable and necessary and supported by sufficient documentation. We reviewed two sets

of documentation related to SIPA's expenses. First, we reviewed supporting documentation for a sample of 176 expenses, totaling about $186,300 incurred by SIPA between July 1, 2010 and February 29, 2012. Our sample included 35 transactions paid by check and 141 credit card transactions for expenses such as marketing, professional fees, professional dues and training, board expenses, office supplies and equipment, travel expenses, and meals. We did not test lease payments. For the sample of 176 expenses, we tested each expense for the following attributes: (1) is the expense reasonable, (2) is there supporting documentation, including an itemized receipt, for the expense, (3) does supporting documentation agree to the amount of the purchase, (4) was the expense coded to the correct object code and the correct fiscal year, (5) do travel expenses include expenses for overnight travel only, and (6) can the check used to pay for the expense be tied to SIPA's operating bank account statement?

Second, during our review of these 176 expenses we became aware that SIPA does not require staff to retain receipts to support credit card expenses. Because this practice increases the risk that credit card expenses could be inappropriate or inaccurate, we reviewed the credit card statements to determine whether the credit card expenses overall appeared to be reasonable and necessary and to identify any trends that could indicate potential fraud or abuse. We reviewed SIPA's credit card statements between July 1, 2010 and April 15, 2012 for each of the three active credit cards in use at SIPA. In total, there were 759 credit card transactions, not already included in our sample of 176 expenses, during this 22-month period totaling about $57,100.

How were the results of the audit work measured?

Organizational spending practices should be representative of behavior that a prudent person would consider a reasonable or necessary business practice, given the facts and circumstances. We used the following criteria to evaluate SIPA's expenses:

- SIPA has only two policies related to expenses: (1) SIPA employees must submit receipts for all reimbursements of expenses directly related to the business of SIPA, except that a receipt is not needed for incidental expenses less than $10, and (2) for expenses exceeding $25,000 for contracts, personnel services, credit commitments, and capital purchases, authorization must be by a majority vote of the seated voting members of the Board.

- Because SIPA's financial policies are so limited, we used other sources as guidance in evaluating the reasonableness of the expenses as well as the sufficiency of SIPA's controls over the expenses we tested, as described below:

- **Reasonable and Necessary.** State Fiscal Rule 2-1 requires that all state expenditures be only for state business purposes and reasonable and necessary under the circumstances.

- **Meals.** State Fiscal Rule 5-1, Section 11.1, and the State Controller's Technical Guidance on the Taxability of State Travel Reimbursements allow reimbursement for employee meals only when traveling and only for a period extending longer than a single day. If an employee is not on travel status, or travel concludes within a single day, and the meal is paid for by the State, the meal becomes reportable as taxable income to the employee. This Fiscal Rule is based on IRS regulations regarding the taxability of meals paid for by an employer. IRS regulations identify meals provided to employees as fringe benefits, reportable in the employee's taxable income if the meal does not occur as part of overnight, business-related travel. IRS regulations allow a meal provided to an employee that is not related to travel to be excluded from taxable income if the meal is a "business meal" and it is adequately documented, including the specific business purpose of the meal and the list of attendees. State Fiscal Rule 5-1, Appendices A1 and A2 allow a per diem of $66 per day for meals while on travel status, including $11 for breakfast, $16 for lunch, $34 for dinner, and $5 for incidental expenses such as tips for taxi cab drivers, hotel maids, or bellhops.

- **Supporting Documentation.** State Fiscal Rule 2-2 Section 2.14 requires state agencies to maintain supporting documentation, including an invoice, billing, or receipt that provides a description of goods or services purchased and the amount to be paid. This requirement applies to small purchases of less than $5,000.

While SIPA is not subject to State Fiscal Rules, these rules provide guidance that SIPA could look to in developing a comprehensive set of policies and procedures governing its expenses.

Additionally, is not uncommon for quasi-governmental entities created to provide a public service, such as Pinnacol or the University of Colorado Foundation, to have written policies allowing the organization to pay for "business meals" for staff and business partners. These policies contain specific limitations about the types of allowable meal expenses that will be reimbursed to employees or Board members or that can be charged to credit cards as business expenses. The policies also specify the type of documentation that must be retained to support the meal expense.

What problem did the audit work identify?

We reviewed a combined 935 expense transactions, including reviewing supporting documentation for 176 expenses from Fiscal Years 2011 and 2012 and reviewing credit card statements containing 759 transactions during the 22-month period from July 1, 2010 to April 15, 2012. The total value of transactions we reviewed was about $243,400. Our review identified problems in two areas:

Unreasonable and unnecessary expenses. We identified 272 SIPA expenses totaling about $13,700 (about 6 percent of the total amount reviewed), including meals, travel, and miscellaneous expenses for which we question either the reasonableness or necessity of the expense or both. We did not question any meals that appear to have occurred while the employee was on travel status. Of the 272 expenses that we identified as unreasonable or unnecessary, 270 were made with SIPA credit cards, totaling about $13,000.

- **Meal Charges.** SIPA staff charged about $9,500 on SIPA credit cards for 248 meals that appeared to have occurred while the employee was not traveling. Of the meals we questioned, we have two concerns. First, we question the business purpose of frequent, small purchases at places like Starbucks or 7-Eleven. Second, we question the high cost and business purpose of meals at restaurants such as Earl's, Panzano, and The Broker, for which SIPA did not maintain documentation of the individuals attending the meal or the business purpose of the meal. Meal charges for these 248 meals ranged from about $1.50 to $470, and 31 meals (13 percent) were for an amount greater than the $66 State per diem for an entire day of meals. Although SIPA reports that all of the meals it paid for were necessary and in the pursuit of business, SIPA staff are not required to retain or submit for review and approval itemized receipts to document meal charges paid for by credit card. As a result, SIPA has no documentation of the business purpose of the meal, who attended the meal, (e.g., only SIPA staff, business partners, or Board members), or what was purchased. While SIPA staff stated that they have calendar entries to support these meals as business expenses, this documentation does not effectively tie the attendees to a specific, itemized meal receipt, and individuals reviewing meal expenses would not have access to individual calendar entries prior to approval. Further, a calendar entry alone is not sufficient to satisfy IRS requirements for documenting business meals. None of the undocumented meals charged by SIPA staff were reported as taxable fringe benefits in the employee's taxable income, as required by IRS regulations. In total, we found that the three employees using credit cards charged a total of about $7,100, $2,300, and $100, respectively, for meals. It is important to note that SIPA's financial auditors also cited SIPA in both the Fiscal Year 2010 and 2011 audits for

not properly documenting business expenses and recommended that SIPA document a detailed business purpose and list of attendees on the receipt for all business expenses.

- **Other Charges.** There were 24 other expenses, totaling about $4,200, that do not appear to be reasonable or necessary to the conduct of business for SIPA, including the following: (1) Three expenses that SIPA staff reports were for the SIPA holiday party. These expenses totaled $2,400 and the receipts indicate there were 30 attendees, for a cost of $80 per person. In comparison to the State's per diem rate for dinner of $34, this appears to be an excessive amount to spend on a meal for a holiday party. Additionally, because SIPA staff at the time included three FTE and one accountant, and the SIPA Board included 13 members, a party of 30 attendees clearly included a number of others. However, SIPA was unable to provide a list of attendees at the event. (2) Five expenses totaling about $500 for snacks, grocery items, and alcohol. (3) Two expenses, totaling about $600, for parking and light rail passes for each of two employees in the same month. (4) Fourteen expenses totaling $700 for late fees, over-limit fees and interest charges on credit cards.

Insufficiently documented expenses. Sixty-nine of the expenses we tested, totaling about $21,700, did not have adequate documentation to support the expense. Specifically, SIPA could not provide any receipt for 30 transactions and could not provide an itemized receipt for 39 transactions, including a description of the item purchased or the attendee and business purpose of a meal. One of these expenses was a reimbursement without accompanying documentation, in violation of SIPA financial policies.

Why did the problem occur?

SIPA does not currently have a written policy in place that: (1) defines appropriate business expenses including the circumstances when it is acceptable for employees to purchase meals, goods, or other services with the SIPA credit card; (2) defines upper limits on any expenses, including meals, travel, or office functions; or (3) makes it clear that undocumented meal expenses will be reported as taxable income to the employee. Additionally, SIPA's policy on employee reimbursements simply says that employees will be reimbursed for "necessary meals" but does not discuss what constitutes a necessary meal, such as whether the employee needs to be on travel status in order to have SIPA pay for a meal, and does not set a per diem limit on the cost of meals. Finally, as discussed in the prior recommendation concerning internal controls, we found that SIPA does not have sufficient segregation of duties over accounts payable, including processes to ensure that expenses are reviewed and approved by a party other than the person incurring the expense for both credit card and other purchases. In order to

facilitate a review and approval process for expenses and to successfully implement recommendations related to improving internal controls over accounts payable discussed in Recommendation No. 4, SIPA will need to ensure that it maintains documentation, including itemized receipts, to support the expense.

SIPA staff were not paying credit card bills timely or monitoring account balances closely to ensure that they did not pay late fees or over-limit fees. A more robust process for processing accounts payable could improve the timeliness of credit card payments.

SIPA staff do not have the tax expertise necessary to ensure that fringe benefits, such as meals, are reported in compliance with IRS regulations.

Why does this problem matter?

SIPA is funded with a percentage of the net revenue Colorado Interactive generates from the fees it charges on transactions processed through the statewide internet portal. These fees are paid by taxpayers when purchasing government services, electronically, through the state portal and therefore, SIPA is accountable for how those funds are spent. The fact that some meals appeared to be unreasonable or excessive and that we could not determine the business purpose or who attended 34 meals in our sample totaling about $7,300, particularly when combined with the deficient internal control structure discussed in Recommendation No. 4, raises serious concerns with respect to SIPA's financial management practices and increases the risk of fraud and abuse, including misappropriation of assets and unreasonable spending. Further, by not establishing any limits on the types or amount of expenses that are acceptable for staff to incur, and by not implementing a review and approval process, SIPA exerts no controls to ensure only expenses that are reasonable and necessary are being paid. Such limits and control procedures also communicate to staff the importance of responsible spending.

Finally, SIPA may be out of compliance with federal tax law regarding fringe benefits and as such employees could suffer fines and penalties for unreported income and underpayment of taxes.

Recommendation No. 5:

The Statewide Internet Portal Authority (SIPA) should work with the SIPA Board to improve controls over its expenses by developing written policies and procedures that better ensure SIPA expenses are reasonable and necessary and that expenses are fully supported by appropriate documentation. Specifically, SIPA and the SIPA Board should:

a. Clarify, in a written policy, the types of expenses that are allowable and unallowable. This should include explanation of the circumstances in which SIPA will pay for meals or snacks for SIPA employees when they are not traveling and establishing clear limitations to prevent excessive or unnecessary expenses, such as paying for alcohol or purchasing both parking and bus passes for an employee in the same month.

b. Develop specific documentation requirements for all types of expenses. Documentation that should be required includes itemized receipts, documentation of the business purpose of the expense, and a list of attendees at all meals.

c. Develop a process to ensure that staff do not exceed credit card limits and that ensures that credit card balances are paid timely in order to avoid over-limit and late payment fees related to credit cards.

Statewide Internet Portal Authority and Board of Directors Response:

a. Agree. Implementation date: August 2013.

   SIPA agrees with part "a" of this recommendation and will work with the SIPA Board to develop a written policy related to allowable expenses.

b. Agree. Implementation date: August 2013.

   SIPA agrees with part "b" of this recommendation and will work with the SIPA Board to develop a written policy related to documentation of expenses.

c. Agree. Implementation date: Implemented.

   SIPA agrees with part "c" of this recommendation and developed procedures in the summer of 2012 that include increasing the credit card limits of staff to appropriate levels and has implemented a procedure in the summer of 2012 to ensure timely payments.

Recommendation No. 6:

The Statewide Internet Portal Authority (SIPA) should establish a clear policy for ensuring compliance with IRS regulations for reporting taxable fringe benefits. The State Fiscal Rules and policies and procedures developed by other quasi-

governmental entities that could provide best-practice guidelines for SIPA and the Board to use in developing these policies. Additionally, SIPA should work with the SIPA Board to ensure that employees' taxable income for the past 3 years was reported accurately. Specifically, SIPA should consider contracting with a consultant to provide tax expertise to work with SIPA staff and the SIPA Board to review expense records for meals and determine whether employees' taxable income for the past 3 years needs to be adjusted.

Statewide Internet Portal Authority and Board of Directors Response:

Partially agree. Implementation date: August 2013.

SIPA agrees that it should establish an improved policy surrounding reimbursements and meals and will work with the SIPA board to update its existing practices and policies. SIPA does not agree that it needs to work with a consultant to determine whether employees' taxable income needs to be adjusted. If necessary, SIPA will review each meeting, research the meeting invites, and will work with the applicable businesses to acquire any receipts it may not have on file. SIPA believes that each of these meetings met the applicable IRS regulation and that it can demonstrate the business purpose for each meeting.

Auditor's Addendum:

The concern noted in the audit is that SIPA lacks adequate documentation to demonstrate compliance with IRS regulations and, as such, may be placing SIPA and its staff at risk for negative tax consequences. The documentation SIPA offered to the auditors consisted primarily of calendar entries and/or documentation created after the fact which does not satisfy IRS requirements. Consulting with a tax professional would provide SIPA assurance that it is complying with the IRS regulations for reporting employee income.

Fund Balance

As discussed, SIPA has increased its revenue by 311 percent between Fiscal Years 2008 and 2012. Primarily, this increase in revenue has resulted from SIPA expanding its menu of services and software solutions for government entities and, more specifically, to SIPA renegotiating its contract with Colorado Interactive to increase SIPA's margin share on the transactions processed from 2 to 7 percent. Additionally, SIPA's contract with Tempus Nova to make Google Apps software available to government entities greatly expanded SIPA's

revenues. The increase in revenues has somewhat outpaced SIPA's increase in expenses, resulting in a growing fund balance for the organization. The table below shows SIPA's revenues, expenses, and fund balance for Fiscal Years 2008 through 2012. Fiscal Year 2012 is currently an estimate, based on unaudited financial information from SIPA's accounting system.

The Statewide Internet Portal Authority
Revenues, Expenses, and Fund Balance
Fiscal Years 2008–2012

	Fiscal Year 2008	Fiscal Year 2009	Fiscal Year 2010	Fiscal Year 2011	Fiscal Year 2012 (Unaudited)
Fund Balance Beginning of the Year	$720,900	$717,900	$694,500	$839,800	$1,147,700
Operating Revenue	596,300	647,000	1,087,700	2,756,800[1]	2,452,200
Operating Expenses	(599,300)	(670,400)	(942,400)	(2,448,900)[2]	(1,853,100)
Fund Balance End of the Year	$717,900	$694,500	$839,800	$1,147,700	$1,746,800

Source: Statewide Internet Portal Authority Financial Statements.
[1] According to SIPA, the large increase in revenues is the result of SIPA launching Google Apps and increasing the number of local and state government entities it serves.
[2] SIPA reports that expenses increased due to SIPA purchasing Google Apps for the local and state government entities and passing on the revenue to the vendors.

What work was performed and what was the purpose?

We reviewed SIPA's fund balance and expected business uses of those funds for Fiscal Years 2008 through 2012 to determine whether SIPA's fund balance aligns with best practices. Because SIPA's fund balance has been growing, we reviewed SIPA's portal fees and its process for setting fees and compared them with other states' fees to determine if Colorado's portal fees appear reasonable.

How were the results of the audit work measured?

SIPA's policies and procedures state that "[SIPA] shall maintain a goal of retaining earnings in a fund balance. The use of such funds will be for the purpose of meeting future obligations, capital expenditures, and operational expenses when needed. The Executive Director shall include the use of any fund balance in the yearly budget and shall adequately plan for any future obligations."

Because SIPA has not yet developed a fund balance policy or plan, we looked to other nationally recognized sources for guidance on fund balance management. The National Advisory Council on State and Local Budgeting and the Government Finance Officers Association recommend that all governments

develop a formal, written fund balance policy that is made publicly available. The Government Finance Officers Association recently updated its best practice on unreserved general fund balances to recommend that general purpose governments maintain, **at a minimum,** an unrestricted general fund balance of no less than 2 months of regular general fund operating revenues or regular general fund operating expenses. The Government Finance Officers Association further states that for government entities that have widely fluctuating revenues or expenses, it may be wise to maintain a larger fund balance; entities with predictable revenues and expenses may be able to manage without maintaining a large reserve.

One of SIPA's largest sources of revenue is a percentage of the convenience fees charged to taxpayers when they pay for government services through the state web portal. The SIPA Board has discretion to set fees as they see fit to pay for SIPA's operations. As such, it is important that SIPA sets fees appropriately so that the fees cover the costs of operating the portal, but not so high as to result in excess revenue. We compared SIPA's fee structure with similar fee structures in the comparable states of Arkansas, Indiana, and Utah.

What problem did the audit work identify and why did the problem occur?

As of June 30, 2012, SIPA has accumulated a $1.7 million fund balance; which is 11 times the amount SIPA would typically spend in a given month. As shown in the table above, SIPA's fund balance began growing significantly in Fiscal Year 2011, after SIPA renegotiated its contract with Colorado Interactive and contracted with Tempus Nova to make Google Apps software available to government entities. In its 2010 business plan, SIPA stated that it would be working with the finance committee of the SIPA Board to identify a "detailed investment strategy" for the SIPA fund balance. However, at the time of our audit, neither SIPA management nor the SIPA Board could articulate their plans for use of the fund balance or what an appropriate or necessary balance of reserves would be to ensure continuity of operations for SIPA. Additionally, neither SIPA nor the SIPA Board has established a formal policy that identifies the optimal amount of reserves to maintain in its fund balance or how to use any excess reserves to further the mission and goals of SIPA. We found that SIPA's fund balance remained in its checking account, not earning any interest, until February 2012, when SIPA moved about $400,000 into an interest-bearing savings account. SIPA moved an additional $100,000 from its checking account to its savings account in March 2012. As of June 30, 2012, SIPA has earned about $180 in interest on these $500,000 in savings.

SIPA reports having numerous discussions with the Board about SIPA's fees, which have not changed since SIPA began operating in 2005. Our review of

SIPA's fees revealed that they appear comparable to those charged by other state portals. However, without an established fund balance target and plans for how to use monies in excess of the target, SIPA and the Board lack an important standard against which to evaluate the appropriateness of SIPA's fees. Additionally, as SIPA's service offerings become more diverse, such as with the offering of Google Apps software, SIPA's revenue structure becomes more complex and requires ongoing evaluation against a fund balance and investment policy to ensure that SIPA offers services in the most affordable manner and to ensure that SIPA does not build a fund balance that is greater than it needs.

Why does this problem matter?

Without a clear plan and stated business purpose for the fund balance, we could not evaluate—nor has SIPA been able to evaluate—whether its current fund balance is appropriate to meet SIPA's business objectives. SIPA's mission is to provide efficient and effective government service delivery through the use of technology, with the additional goals of continuing to develop and expand the products and services that enable members of the public to efficiently transact business with government entities, and to aide government entities to accelerate adoption of the services offered by SIPA. For example, SIPA currently operates a grant program in which it awards small grants to government entities to help them purchase software, hardware, or infrastructure needed to facilitate that entity's ability to conduct business electronically. In each of Fiscal Years 2011 and 2012 SIPA granted roughly $100,000 to a total of about 20 government entities for these purposes. If SIPA and its Board were to determine that it could retain a smaller fund balance, it is possible that SIPA could invest more in these types of grants to government entities, or find other infrastructure, hardware, or software in which it could invest its excess revenues to facilitate e-commerce for government entities.

Additionally, if SIPA were to hold a greater portion of its fund balance in an interest-bearing savings account, SIPA could generate interest earnings that could further be invested in achieving its mission and goals.

Recommendation No. 7:

The Statewide Internet Portal Authority (SIPA) should work with the SIPA Board to better manage its fund balance by:

a. Identifying a reasonable target fund balance to meet SIPA's needs and identifying priorities for how any monies in excess of the optimal fund balance (if applicable) should be reinvested to further the mission and goals of SIPA. Based on the target fund balance identified, SIPA should

develop a formal, written fund balance policy that aligns with SIPA's mission and goals.

b. Making the fund balance policy publically available.

c. Periodically evaluating SIPA's fee structure, in light of its fund balance policy and objectives, to determine whether SIPA may be able to reduce fees to taxpayers for its services.

d. Transferring all of its fund balance, except what is needed to meet the month-to-month cash flow needs, to an interest-bearing savings account.

Statewide Internet Portal Authority and Board of Directors Response:

a. Agree. Implementation date: Implemented.

SIPA agrees with part "a" of this recommendation and updated its financial policies in December 2012 to reflect what it believes is a reasonable fund balance.

SIPA continually evaluates its fee structure and fund balance against planned expenses and future obligations. SIPA accumulated a larger fund balance over recent years only because of SIPAs significant growth during that time and to ensure that SIPA had the resources to meet the expanded new demands on it, including the purchase of necessary insurance and/or to meet potential liabilities, and to ensure that SIPA had the resources to address a major service disruption. If a major disruption were to occur, more than 200 applications would cease to function, payment processing would be disrupted, and governments across Colorado would be impacted almost immediately. SIPA maintained a fund balance that it believed was adequate to address most emergencies. As noted, SIPA has now formalized its policy on fund balance per OSA's recommendation.

b. Agree. Implementation date: Implemented.

SIPA agrees with part "b" of this recommendation and updated its financial policies in December 2012 to reflect what it believes is a reasonable fund balance. All of SIPA's policies are publically available at this time and can be made available upon request.

c. Agree. Implementation date: Implemented.

SIPA agrees with part "c" of this recommendation and will continue to evaluate its fee structure. In the future SIPA will document this evaluation more thoroughly.

d. Agree. Implementation date: Implemented.

SIPA agrees with part "d" of this recommendation and believes that active management of its bank accounts is an important part of management's duties. SIPA staff monitors and makes decisions related to bank account balances on a weekly basis and this practice will continue.

Insurance

According to the Governmental Accounting, Auditing, and Financial Reporting manual, all governments face various risks that must be managed and ultimately financed. They can approach financing these risks in various ways, including: (1) insurance—transferring the risk of loss to a third party in exchange for a premium, (2) pooling of risk—entering into an agreement with other entities to share common risks, or (3) self-insurance—retaining risk while systematically accumulating resources to finance risk losses as they occur. As an entity primarily funded by convenience fees charged to taxpayers and as an entity that other government entities rely on to conduct business electronically, it is important that SIPA appropriately manage its risks and protect SIPA's ability to continue conducting business in the event of a lawsuit, disaster, or theft.

In the Fiscal Year 2009 financial audit of SIPA, the auditors recommended that SIPA obtain commercial insurance coverage to protect SIPA in the event of a criminal act (e.g., theft, fraud, or harassment), natural disaster, or lawsuit. According to the Executive Director, when it first began as an organization in Fiscal Year 2005, SIPA found that purchasing a commercial policy was cost prohibitive; and as a result, SIPA decided to be self-funded for the purposes of insurance coverage.

What audit work was performed and what was the purpose?

To review the method by which SIPA manages and finances its risk we reviewed documentation at SIPA, interviewed both SIPA staff and members of the SIPA Board, and reviewed Board meeting minutes for Fiscal Years 2010 through 2012

to determine if the SIPA Board has discussed or documented its decision to be self-insured. Further, we reviewed documentation to determine whether SIPA had evidence of periodic review or evaluation of its decision to be self-funded with respect to its insurance coverage. Finally, we interviewed a risk management expert at the Division of Risk Management to discuss the benefits and risks of self-funding.

How were the results of the audit work measured?

We used information from the Colorado Division of Risk Management and the Colorado Housing and Financing Authority (CHFA) in assessing SIPA's risk management efforts. The Division of Risk Management is the division responsible for providing a comprehensive risk management program that serves all state departments and selected institutions of higher education. The Division of Risk Management manages a risk portfolio totaling around $55 million and, as such, has significant expertise in the area of risk management. CHFA is similar to SIPA in that it is a political subdivision of the State and is primarily self-insured.

According to the Division of Risk Management, larger entities are more likely than smaller entities to elect self-insurance because they have adequate assets to cover the risks that they are susceptible to. The Division also said that, typically, entities are not 100 percent self-insured and that most hold umbrella or stop-loss policies that cover losses of more than a specified amount. The amount of stop-loss protection needed varies by entity, depending on the risks that entity faces and the resources that entity has at its disposal to cover any losses incurred. The amount of stop-loss protection is also typically identified by an insurance expert or actuary.

Additionally, CHFA provided us with information on its risk management approach. Specifically, CHFA told us that its insurance broker established a comprehensive risk management plan for CHFA that includes self-insurance up to a specific stop-loss point at which another commercial policy takes over coverage. As part of this risk management plan, the insurance broker determines how much CHFA must maintain, in a separate account, for the purposes of funding insurance claims.

What problem did the audit work identify?

SIPA reports that it has been self-insured since 2005. We identified three concerns related to SIPA's management of its risk. We found that SIPA: (1) has no written policy citing the terms of its self-insurance, such as the amount of funds that it should set aside to cover losses, the amount it would pay out in the event of a loss, or a policy that defines how frequently SIPA should reevaluate its decision to self-insure; (2) could not provide any documentation that either SIPA

or the Board evaluated the decision to self-insure against other insurance options, or that the Board made a decision for SIPA to be self-insured; and (3) has not established a separate fund for the express purpose of funding losses.

Why did the problem occur?

SIPA has not worked with a risk management professional, such as an insurance broker, to develop a comprehensive risk management plan for the organization. According to SIPA, when it began operations in 2005, SIPA staff did preliminary research to obtain insurance coverage and found the premiums to be prohibitively expensive; SIPA has not formally revisited the issue of self-insurance since then and could not provide documentation of any of its informal efforts to revisit the decision to self-insure.

Why does this problem matter?

Risk management, and a decision to self-insure, can be complicated; it involves identifying the risks that threaten the organization, assessing the potential financial impact of those risks, and developing a plan to cover the organization if one of the risks materializes into a financial claim against the organization. Most risk management plans consider the amount of risk that an organization can afford to finance itself (e.g., through self-insurance) as well as the amount of risk that the organization needs to cover by purchasing a commercial insurance policy. Because SIPA has not completed a comprehensive risk management plan, it has not gone through the formal steps of identifying the risks that it can afford to cover; therefore, its decision to self-insure 100 percent of the risks may not be in the best interests of the organization. Further, while SIPA's 2010 business plan says that one of the purposes of the fund balance is to fund self-insurance, the 2010 plan also states that the fund balance can be used for "other sundry items" such as software license renewals. SIPA has not determined whether its fund balance reserves are sufficient to cover the types of risk and potential claims to which SIPA is susceptible.

Typical risks that businesses need to protect themselves against include theft; lawsuits from employees for issues such as discrimination, harassment, and wrongful termination; lawsuits from customers for failure to provide quality or timely services or for damage to the customers' property or business; and natural disasters such as floods or fires that damage office equipment and furniture and that can shut down information systems and result in lost revenues. Audit work discussed in previous sections of this report identified business practices at SIPA such as an overall lack of internal controls and insufficient contract monitoring practices that leave SIPA particularly vulnerable to some of these risks, such as theft or breach of contract lawsuits from customers. If a loss event occurred that rendered SIPA unable to operate for a period of time, it is possible that about 260

government entities could experience disruption of services, including, but not limited to the loss of their websites and the ability to accept electronic payments; longer lines at government service offices; and decreased goodwill with taxpayers who lose the ability to transact services online. Such disruptions could lead to the loss of revenue, and government entities could lose the availability of software applications.

Recommendation No. 8:

The Statewide Internet Portal Authority (SIPA) should work with the SIPA Board to develop a comprehensive risk management program for SIPA. This effort should include:

a. Working with an insurance broker to identify the risks to the organization, evaluating how much risk SIPA can afford to finance itself through self-insurance, and, if applicable, how much risk SIPA should finance through the purchase of commercial insurance policies. SIPA should work with the Board to ensure that SIPA's insurance elections align with the Board's fund balance policy discussed in Recommendation No. 7. If SIPA decides to self-insure, it should document that decision.

b. Establishing written policies discussing the appropriate terms of its self-insurance policy and the amount that should be reserved for self-insurance.

c. Creating a separate self-insurance fund to pay for any claims.

Statewide Internet Portal Authority and Board of Directors Response:

a. Agree. Implementation date: February 2013.

SIPA agrees with part "a" of this recommendation and has been working with an insurance broker since June of 2012 to assess its insurance needs. SIPA is currently reviewing insurance policies covering a broad array of potential risks (including technology liability, privacy breaches and issues related to content) and related proposals from a variety of carriers. SIPA intends to purchase one or more insurance policies in the coming months.

b. Not Applicable. Implementation date: Not Applicable.

SIPA intends to purchase a commercial policy and therefore will not continue to self-insure.

c. Not Applicable. Implementation date: Not Applicable.

SIPA intends to purchase a commercial policy and therefore will not continue to self-insure.

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 2178

Report Control Number 2178