July 29, 2013

Dianne E. Ray, CPA
State Auditor
Colorado Office of the State Auditor
200 East 14th Avenue, 2nd Floor
Denver, CO 80203

Re: Status report - implementation of audit recommendations

Dear Ms. Ray:

In response to your request, we have prepared a status report regarding the implementation of audit recommendations contained in the Statewide Internet Portal Authority Performance Audit released in December 2012. The attached report provides a brief explanation of the actions taken by the Statewide Internet Portal Authority (SIPA) to implement each recommendation.

SIPA is a rapidly growing enterprise that now provides information technology services to over 230 state and local governmental agencies. SIPA has historically operated with only two or three employees in order to minimize its operating costs and maximize savings for its customers. As the Performance Audit pointed out, this situation has resulted in some deficiencies relating to internal controls and comprehensive, well-documented operational policies and procedures. The recommendations made by your office have provided SIPA with opportunities to better align its policies and procedures with its practices and improve its overall performance. In aligning its policies and procedures to its practices SIPA will continue to offer exemplary customer service and ensure its customers have the ability to acquire great technological solutions for their operations.

SIPA and its Board of Directors have made it a priority to achieve full implementation of the audit recommendations, and SIPA has taken steps to implement all of the audit recommendations. Some of the major initiatives undertaken by SIPA include the following:

- In January of this year, SIPA hired a part-time Director of Special Projects whose primary focus has been implementation of the audit recommendations.
- Within two months of the release of the audit SIPA implemented or partially implemented 58% of the applicable recommendations.
- SIPA has improved its internal financial controls by engaging an outside accounting firm and by adopting a set of financial procedures and policies with improved segregation of duties.

- Last week SIPA hired a full-time Director of Operations whose duties will include further development of procedures and policies that will improve SIPA's performance regarding internal controls and contract monitoring.
- SIPA worked with an outside insurance broker to acquire Professional and Technology Based Services, Technology Products, Information Security & Privacy, Privacy Notification, Regulatory Defense and Penalties, Multimedia and Advertising and Directors and Officers insurance from third parties.
- With the upcoming expiration of the contract of SIPA's current portal integrator, SIPA developed and published a Request for Proposals on June 19 that includes specific requirements for the portal integrator to achieve full compliance with applicable audit recommendations, including security and disaster recovery planning. (The RFP is posted on SIPA's website at http://www.colorado.gov/sipa.) After the award, SIPA will negotiate a new contract that incorporates those requirements to ensure compliance with the audit recommendations.
- SIPA's current portal integrator has made many changes to its existing policies to address the recommendations of the State Auditor. Such changes include revising its Disaster Recovery Plan to comply with State Cyber Security Policy P-CISP-004. SIPA continues to work with its portal integrator to continue such improvements.

As the attached status report demonstrates, 24 of the 29 audit recommendations have been implemented or are no longer applicable. Of the remaining recommendations, SIPA is working hard to achieve full implementation. We welcome your comments and suggestions related to SIPA's progress so far and its continued implementation of all recommendations.

If you have any questions, please do not hesitate to contact me at 720-409-5437 or by email at john@cosipa.gov.

Sincerely,

John Conley, PMP
Executive Director

cc: Jack Arrowsmith, Chairman, SIPA Board of Directors

AUDIT RECOMMENDATION STATUS REPORT

AUDIT NAME: Statewide Internet Portal Authority Performance Audit
AUDIT NUMBER: 2178
DEPARTMENT/AGENCY/ENTITY: Statewide Internet Portal Authority (SIPA)
DATE: November 2012

SUMMARY INFORMATION

Recommendation Number *(e.g., 1a, 1b, 2, etc.)*	**Agency's Response** *(i.e., agree, partially agree, disagree)*	**Original Implementation Date** *(as listed in the audit report)*	**Implementation Status** *(Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable)* Please refer to the attached sheet for definitions of each implementation status option.	**Revised Implementation Date** *(Complete only if agency is revising the original implementation date.)*
1a.	Agree	February 2013	Implemented	
1b.	Agree	June 2013	Implemented and Ongoing	
1c.	Agree	June 2013	Implemented	
2a.	Agree	September 2013	Partially Implemented	December 2013
2b.	Agree	June 2013	Implemented and Ongoing	
2c.	Agree	September 2013	Implemented and Ongoing	
2d.	Disagree	N/A	Partially Implemented	
2e.	Agree	March 2013	Implemented	
3a.	Agree	June 2013	Partially Implemented	September 2013
3b.	Agree	June 2013	Partially Implemented	September 2013
3c.	Agree	September 2013	Partially Implemented	
3d.	Agree	July 2013	Implemented	
4a.	Agree	March 2013	Implemented and Ongoing	
4b.	Agree	January 2013	Implemented and Ongoing	

Recommendation Number *(e.g., 1a, 1b, 2, etc.)*	**Agency's Response** *(i.e., agree, partially agree, disagree)*	**Original Implementation Date** *(as listed in the audit report)*	**Implementation Status** *(Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable)* Please refer to the attached sheet for definitions of each implementation status option.	**Revised Implementation Date** *(Complete only if agency is revising the original implementation date.)*
4c.	Agree	January 2013	Implemented and Ongoing	
4d.	Agree	January 2013	Implemented and Ongoing	
4e.	Agree	July 2013	Implemented and Ongoing	
4f.	Agree	June 2013	Implemented and Ongoing	
5a.	Agree	August 2013	Implemented	
5b.	Agree	August 2013	Implemented	
5c.	Agree	Implemented	Implemented	
6	Partially Agree	August 2013	Implemented	
7a.	Agree	Implemented	Implemented and Ongoing	
7b.	Agree	Implemented	Implemented	
7c.	Agree	Implemented	Implemented and Ongoing	
7d.	Agree	Implemented	Implemented and Ongoing	
8a.	Agree	February 2013	Implemented	
8b.	Not Applicable	Not Applicable	No Longer Applicable	
8c.	Not Applicable	Not Applicable	No Longer Applicable	

DETAIL OF IMPLEMENTATION STATUS

Recommendation #: 1a.

Agency Addressed: Statewide Internet Portal Authority

Recommendation Text in Audit Report:

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.

Agency's Response: a. Agree. Implementation date: February 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation:

Implemented and Ongoing.

Agency's Current Comments on Implementation Status of Recommendation:

SIPA and Colorado Interactive (CI) have addressed this recommendation in several ways, and, where appropriate, Colorado Interactive has updated its internal policies and procedures.

1. Security breaches – notifications pursuant to the Consumer Protection Act. SIPA reviewed the Colorado Consumer Protection Act and Colorado Interactive's policies regarding security breaches. Colorado Interactive's Incident Response Policy currently provides a procedure for responding to security incidents. It requires that Colorado Interactive will handle incidents "in a manner that is consistent with Federal, State and local laws and all applicable regulations pertaining to our business operations". In the event of a security breach, the policy requires specified staff members to "review State legislation to determine if specific notification is required to consumers who were affected by the security incident". Thus, if a security breach compromises the personal information of Colorado residents, then Colorado Interactive will comply with section 6-1-216 of the Colorado Consumer Protection Act, which

requires notification to any affected Colorado resident as soon as possible after becoming aware of a breach in the security of computerized data that includes personal information about the resident of Colorado. However, SIPA believes that more specificity is desirable and believes that the next portal integrator contract should expressly require compliance with the Colorado Consumer Protection Act. Therefore SIPA's RFP for the next portal integrator contractor specifically requires the contractor to "adhere to the Colorado Consumer Protection Act regarding breaches in security of citizen's personal identifiable information". (RFP, p. 45)

2. System outages - notification to users. Colorado Interactive has revised and improved its communication plan to notify users when there is a system outage. Under CI's Notification Policy, notification lists are maintained for various systems, including the content management system, the payment transaction engine system, the licensing system, and applications written and hosted by Colorado.gov. Users are provided opportunities to sign up for their desired and relevant notification lists. Notification information provided to users may be found online as follows:

   http://www.colorado.gov/registered-services/pdf/newUserInfoPack.pdf

   http://www.colorado.gov/registered-services/accountManagement.html (See link to "Notification Distribution Lists")

   http://mailman.coloradointeractive.org/mailman/listinfo

3. Disaster Recovery Plan - notifications in the event of a disaster. In the event of a disaster, Colorado Interactive's Disaster Recovery Plan requires CI's Director of Development to notify customers on any affected notification list. If the outage affects users of the Colorado.gov website not included in the notification lists, a notification will be placed in the banner section of the Colorado.gov homepage. Posting the notification on the Colorado.gov homepage will be possible even if the disaster brings down the Colorado.gov homepage because SIPA maintains a mirrored view to bring up temporarily during an outage.

Recommendation #: 1b.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: b. Agree. Implementation date: June 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

Colorado Interactive is now conducting regular risk assessments for its information systems, and Colorado Interactive has agreed to a process by which it will provide regular reports to SIPA on identified risks and Colorado Interactive's plans for mitigating the risks. SIPA will require ongoing implementation of this recommendation by reviewing and evaluating the reports that Colorado Interactive provides to SIPA and improving mitigation plans. In addition, specific requirements for regular risk assessments and reporting to SIPA will be incorporated into the next portal integrator contract. SIPA's RFP for the next contract specifically requires that, "The Contractor shall conduct semi-annual risk assessments of its information systems and report to SIPA on identified risks and plans for mitigating the risks." (RFP, p. 46)

Recommendation #: 1c.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: c. Agree. Implementation date: June 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented.

Agency's Comments on Implementation Status of Recommendation:

On a monthly basis, Colorado Interactive identifies users of the transaction payment engine system who have not logged in for at least 90 days and disables those users' access to the system. To confirm this, Colorado Interactive provides a monthly report to SIPA that lists all users, their last login date, and their status as enabled or disabled. SIPA then reviews the report to confirm that all users who have not logged in for 90 days or more are in a disabled status.

The next portal integrator contract will incorporate specific requirements for identifying and disabling unused IDs on the transaction payment engine system. SIPA's RFP for the next contract specifically requires the portal integrator to "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." (RFP, p. 46)

Recommendation #: 2a.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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.

Agency's Response: a. Agree. Implementation date: September 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Partially Implemented.

Agency's Comments on Implementation Status of Recommendation:

SIPA and Colorado Interactive have had extensive discussions about the impact of a disaster on the different systems and applications hosted by Colorado Interactive, as well as how to prioritize disaster recovery efforts among those systems and applications. As a result, SIPA and Colorado Interactive share a common understanding of how disaster recovery efforts should be prioritized. However, a thorough business impact analysis has not been completed, and it might not be completed during the current contract term that is about to expire. SIPA will continue to work with Colorado Interactive and the next portal integrator to implement Recommendation 2a.

Additional comments relating to Recommendation 2a are included in our comments under Recommendation 2c below.

Recommendation #: 2b.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: b. Agree. Implementation date: June 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation:

Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

Alternative processing plans are detailed in the current versions of Colorado Interactive's Continuity of Computer Operations Policy (dated 6/20/13) and its Disaster Recovery Policy (dated 7/19/13). However, SIPA believes that additional detail is needed and will continue to work with Colorado Interactive and the portal integrator selected from the current RFP process in order to improve alternative processing plans and incorporate specific requirements into SIPA's agreements with the portal integrator.

Additional comments relating to Recommendation 2b are included in our comments under Recommendation 2c below.

Recommendation #: 2c.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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

Agency's Response: c. Agree. Implementation date: September 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

Detailed recovery steps are included in the current versions of Colorado Interactive's Continuity of Computer Operations Policy (dated 6/20/13) and its Disaster Recovery Policy (dated 7/19/13). However, SIPA believes that additional detail is needed and will continue to work with Colorado Interactive and the portal integrator selected from the current RFP process in order to improve alternative processing plans and incorporate specific requirements into SIPA's agreements with the portal integrator.

In addition, SIPA offers the following general comments that relate to Recommendations 2a, 2b, and 2c, because they are interrelated recommendations.

These three recommendations share a common objective stated in the Audit Report, namely, the need for SIPA's portal integrator to "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". (Audit Report, p. 24, emphasis added.) The Audit Report pointed out a number of areas where improvements were necessary in Colorado Interactive's Disaster Recovery Plan. SIPA and Colorado Interactive have been working to address those improvements, and significant progress has been made to the Disaster Recovery Plan. However, additional work is needed, and SIPA will continue to work with its portal integrator (even after upcoming execution of a new contract) to achieve a comprehensive DRP that fully satisfies the cyber security policies of the State's Office of Information Technology.

Perhaps the major shortcoming noted about Colorado Interactive's Disaster Recovery Plan (DRP) was that it did not comply with State Cyber Security Policy P-CISP-004, which requires that a DRP include specific sections addressing such matters as development of the DRP, maintenance of the plan, regular testing and training, distribution to appropriate parties, step-by-step instructions for recovery and resumption of services, offsite backup storage, and post-resumption review. In the last several months, Colorado Interactive has made numerous additions to its Disaster Recovery Plan. As a result, its DRP now includes, at least minimally, all of the sections required by State Cyber Security Policy P-CISP-004. For example, new sections have been added that address regular testing, maintenance, distribution, training, offsite backup storage, and post-resumption review.

However, SIPA believes, and Colorado Interactive agrees, that CI's Disaster Recovery Plan is still not sufficiently detailed and that Colorado Interactive must continue to work on improving it to comply fully with Recommendations 2a, 2b, and 2c. In particular, Colorado Interactive needs to develop a much more thorough business impact analysis and alternative processing plans that are tied to a well-documented prioritization of systems and applications. While SIPA and Colorado Interactive are working toward full compliance, it is important to stress they have both agreed to work in good faith to overcome any disaster that occurs.

The new portal integrator contract will incorporate specific requirements for complying with State Cyber Security Policies and the audit recommendations. Toward that end, SIPA's RFP for the next contract includes specific requirements, including the following:

- The Contractor must "Develop an annual Disaster Recovery Plan to include: A business impact analysis that identifies the potential impacts to key business processes and allows the Contractor to formulate and prioritize its disaster recovery efforts; Alternative processing plans detailing how the Contractor will ensure that Portal transactions can continue to be processed and that hosted

websites will remain available; Detailed recovery steps, including identifying time frames for each step and for each disaster scenario; A schedule for regularly reviewing and updating the Disaster Recovery Plan. (RFP, p. 42-43)

- "Contractor's Business Continuity and Disaster Recovery Plan shall satisfy the requirements of the State's Information Security Policies as prescribed by the Governor's Office of Information Technology." (RFP, p. 97)
- "The Contractor shall adhere to the EGE's requirements, security policies, Service Level Agreement, and other applicable policies for projects with EGEs." (RFP, p. 36)
- Regarding Security Infrastructure: "The Contractor shall adhere to Colorado Statewide IT Security Policies and Standards as required, for developed systems." (RFP, p. 45)
- Regarding Security Infrastructure: "The Contractor shall present a written Security Management Plan that meets State security requirements." (RFP, p. 45)
- Regarding Disaster Recovery Plan: "Contractor's Business Continuity and Disaster Recovery Plan shall satisfy the requirements of the State's Information Security Policies as prescribed by the Governor's Office of Information Technology." (RFP, p. 97)

Recommendation #: 2d.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: Disagree. Implementation date: N/A

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Partially Implemented.

Agency's Comments on Implementation Status of Recommendation:

Although this recommendation is categorized as "Disagree", SIPA has always agreed with the underlying objective, that is, the need for an effective communication plan to notify customers about planned and unplanned system outages. It appears to SIPA that the only issues are (1) the best means to achieve effective communication and (2) the difficulty for auditors to assess the existing system of notification in time for the audit (as stated in the "Auditor's Addendum").

The Audit Report recommends that notifications be based on developing and maintaining a complete list of customers and then contacting affected customers on the list when there is a disaster. SIPA's approach is based on customers subscribing to the notifications they need and want to receive, based on the services they receive. (In addition, in the event of an actual disaster, SIPA would create a dedicated web page to reach not only customers whose identities are known, but also portal users that would not be on any notification lists.) Despite this difference in approach, SIPA agrees with the recommendation on the need for "a detailed communication plan for how to contact customers and end users in the event of an emergency".

Thus, SIPA has been working with Colorado Interactive on improving the subscription notification system, and Colorado Interactive has incorporated improvements into its communication plan. For more detail, please see SIPA's comments under Recommendation 1a above.

Recommendation #: 2e.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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

Agency's Response: e. Agree. Implementation date: March 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation:

Implemented.

Agency's Comments on Implementation Status of Recommendation:

Beginning in January 2013, SIPA scheduled and has conducted monthly reviews with Colorado Interactive. To date, those reviews have focused on improvements Colorado Interactive needs to make to its Disaster Recovery Plan in order to fully implement the audit recommendations. In addition, Colorado Interactive revised its Disaster Recovery Plan to ensure that the Plan is updated when there are changes to the environment, such as new systems and personnel changes.

The next portal integrator contract will incorporate a specific requirement to ensure compliance with Recommendation 2e. Toward that end, SIPA's RFP for the next contract includes a specific requirement that the Contractor must "Develop an annual Disaster Recovery Plan to include: . . . A schedule for regularly reviewing and updating the Disaster Recovery Plan. (RFP, p. 42-43)

Recommendation #: 3a.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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.

Agency's Response: a. Agree. Implementation date: June 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Partially Implemented.

Agency's Comments on Implementation Status of Recommendation:

SIPA has not yet drafted a comprehensive set of contract monitoring policies. However, SIPA will be hiring a contract employee with procurement and contract management expertise at the state government level who will focus on developing such policies to fully implement this recommendation. In addition, SIPA has hired a Director of Operations who will be responsible for carrying out contract monitoring activities in accordance with the recommendations contained in the Audit Report.

In preparation for a formal set of contract monitoring policies, SIPA has been improving its contract management practices. For example, SIPA is improving its utilization of its customer relationship management (CRM) system to better document meetings with contractors, project status updates, and communications with customers and contractors. When a customer informs SIPA that there is a problem with a project, contract, or statement of work, SIPA opens a case in its CRM system and tracks the problem until successful resolution is achieved. SIPA staff members have been instructed on making better use of the system for such purposes, and temporary staff has been assigned to audit and correct record-keeping errors in the system.

SIPA also adopted a set of Internal Financial Policies and Administrative Procedures that includes detailed procedures for managing accounts payable. Section 4.4 of those policies and procedures addresses a portion of Recommendation 3a by requiring SIPA's administrative assistant to review contractor invoices against the appropriate statement of work to verify that the amount invoiced is correct and that payment is due under the statement of work.

Recommendation #: 3b.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: b. Agree. Implementation date: June 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation:

Partially Implemented.

Agency's Comments on Implementation Status of Recommendation:

As noted in SIPA's comments regarding Recommendation 3a, SIPA has not yet adopted a formal set of contract monitoring policies, but it will be hiring a contract employee with procurement and contract management expertise at the state government level who will focus on developing such policies to fully implement this recommendation, and SIPA has hired a Director of Operations who will be responsible for contract management in accordance with the policies and the audit recommendations.

In the meantime, SIPA has incorporated most of Recommendation 3b into its contract management practices. SIPA utilizes it customer relationship management system to maintain contract monitoring documentation, including the executed contract, task orders, invoices, status updates, and notes from meetings with contractors and government entities that discuss the contractor's adherence to contract provisions, as well as resolution of any outstanding problems reported to SIPA.

Recommendation #: 3c.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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

Agency's Response: Agree. Implementation date: September 2013.

Agency's Written Response in Audit Report:

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

Current Implementation Status of Recommendation:

Partially Implemented.

Agency's Comments on Implementation Status of Recommendation:

All SIPA staff members have been trained on utilizing the customer relationship management system for carrying out contract management practices and procedures as described in our comments regarding Recommendations 3a and 3b. When formal contract monitoring policies are adopted, affected staff will be trained on the policies.

Recommendation #: 3d

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: d. Agree. Implementation date: July 2013.

Agency's Written Response in Audit Report:

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

Current Implementation Status of Recommendation: Implemented.

Agency's Comments on Implementation Status of Recommendation:

Since SIPA's executive director is the only individual currently responsible for contract oversight, contract management outcome measures have been incorporated into the executive director's annual performance evaluation by SIPA's Board of Directors. In addition, SIPA plans to incorporate contract management outcome measures into the performance evaluation plan of the newly hired Director of Operations.

Recommendation #: 4a.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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.

Agency's Response: a. Agree. Implementation date: March 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented and Ongoing

Agency's Comments on Implementation Status of Recommendation:

SIPA engaged an outside accounting firm to handle accounting duties. In addition, SIPA adopted a detailed set of financial policies and procedures that establishes a proper segregation of duties among individual SIPA staff members and SIPA's outside accounting firm. The financial policies and procedures specifically cover segregation of duties relating to accounts payable and accounts receivable. The adopted financial policies will be tested and reviewed as part of SIPA's 2013 independent financial audit.

Recommendation #: 4b.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: b. Agree. Implementation date: January 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

SIPA has worked with its bank to limit access as recommended. In addition, this recommendation is incorporated as a matter of policy into the Board of Director's Financial Policies and SIPA's Internal Financial Policies and Administrative Procedures.

Recommendation #: 4c.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: c. Agree. Implementation date: January 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation:

Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

SIPA now conducts monthly reconciliations as recommended, and SIPA documented the procedures in its Internal Financial Policies and Administrative Procedures. For example, under Section 4.7, SIPA's outside accounting firm completes monthly reconciliations and submits a report to the Executive Director or the Director of Operations, who works with SIPA staff to resolve any issues or concerns identified. Documentation is retained as recommended.

Recommendation #: 4d.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: d. Agree. Implementation date: January 2013.

Agency's Written Response in Audit Report:

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

Current Implementation Status of Recommendation: Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

SIPA deleted all access of the previous staff member whose access remained. SIPA adopted a formal password policy that requires all users to change their password once every six months. SIPA changed accounting systems and now has back-up procedures in place related to its data. SIPA adopted a set of Internal Financial Policies and Administrative Procedures that addresses terminating employees, ensuring that only employees with a business need can access the accounting system and ensuring proper segregation of duties within the accounting system (Section 4.10).

Recommendation #: 4e.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: e. Agree. Implementation date: July 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

SIPA now utilizes several centralized systems to perform its operations, including its accounting system (QuickBooks), its customer relationship management system, and its employee time tracking system. Records that are not in digital form are also centrally maintained by SIPA's administrative assistant. Written and electronic records must be retained for a minimum of three years pursuant to SIPA's Internal Financial Policies and Administrative Procedures, Section 4.11.

Recommendation #: 4f.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: f. Agree. Implementation date: June 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

SIPA engaged an outside accounting firm to provide financial accounting expertise and implement a comprehensive system with appropriate internal controls. In December of 2012, SIPA adopted an expense documentation policy, and SIPA's Board of Directors adopted an updated set of financial policies, including a banking account policy, a credit card usage policy, and an expense reimbursement policy. In June of this year, SIPA adopted a set of Internal Financial Policies and Administrative Procedures that details internal financial controls. Staff members have received appropriate training. SIPA's annual financial audit is just getting underway, and we expect to receive valuable feedback from the independent financial audit. If needed, SIPA contemplates engaging a third party to perform a desk audit of systems for purposes of monitoring the effectiveness of SIPA's system of controls.

Recommendation #: 5a.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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.

Agency's Response: a. Agree. Implementation date: August 2013.

Agency's Written Response in Audit Report:

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

Current Implementation Status of Recommendation: Implemented.

Agency's Comments on Implementation Status of Recommendation:

In December of 2012, SIPA adopted an expense documentation policy, and SIPA's Board of Directors adopted an updated set of financial policies to include a credit card usage policy and an expense reimbursement policy. In June of this year, SIPA adopted a set of Internal Financial Policies and Administrative Procedures that includes the previously adopted expense documentation policy, together with additional policies regarding allowable expenses. These policies require expenses to be directly related to the business of SIPA and prohibit expenditures for alcoholic beverages and personal entertainment.

Recommendation #: 5b.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: b. Agree. Implementation date: August 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented.

Agency's Comments on Implementation Status of Recommendation:

In December of 2012, SIPA adopted an expense documentation policy, and SIPA's Board of Directors adopted an updated set of financial policies to include an expense reimbursement policy that covers documentation requirements. In June of this year, SIPA adopted a set of "Internal Financial Policies and Administrative Procedures that includes the previously adopted expense documentation policy. Itemized receipts are required except for incidental expenses under $10. Expense documentation for meals and travel expenses must include a list of those in attendance.

Recommendation #: 5c.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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.

Agency's Response: c. Agree. Implementation date: Implemented

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented.

Agency's Comments on Implementation Status of Recommendation:

SIPA implemented procedures to ensure that credit card bills are paid timely and balances are within limits. SIPA set up automatic payment for its credit card so that late fees cannot be applied. Prior to the audit, SIPA had also increased its credit limit and set policies with its financial institutions to limit the amount staff can charge.

Recommendation #: 6

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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.

Agency's Response: Partially Agree. Implementation date: August 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation:

Implemented.

Agency's Comments on Implementation Status of Recommendation:

As noted in SIPA's comments to Recommendations 5a and 5b, SIPA and its Board of Directors have now adopted clear policies requiring that expenses must have a direct business purpose and must be documented to demonstrate the business purpose. Charges incurred by all employees, including the executive director, are reviewed monthly to ensure that they are for a proper business purpose and are adequately documented. SIPA has reviewed State fiscal rules and IRS regulations and believes that its new expense policies are consistent with those rules and regulations.

Recommendation #: 7a.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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.

Agency's Response: a. Agree. Implementation date: Implemented.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

As noted in its written response in the Audit Report, SIPA updated its financial policies with the Board of Director's adoption of a Retained Earnings Policy last December, and SIPA will continue to evaluate its fee structure and fund balance against planned expenses and future obligations.

Recommendation #: 7b.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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

b. Making the fund balance policy publically available.

Agency's Response: b. Agree. Implementation date: Implemented.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation:

Implemented.

Agency's Comments on Implementation Status of Recommendation:

As noted in its written response in the Audit Report, SIPA updated its financial policies with the Board of Director's adoption of a Retained Earnings Policy last December, and all of SIPA's policies are publically available upon request.

Recommendation #: 7c.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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

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.

Agency's Response: c. Agree. Implementation date: Implemented.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation:

Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

As noted in its written response in the Audit Report, SIPA will continue to evaluate its fee structure and fund balance against planned expenses and future obligations. In addition, SIPA will be evaluating its fee structure as part of the RFP process for a new portal integrator.

Recommendation #: 7d.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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

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.

Agency's Response: d. Agree. Implementation date: Implemented.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation: Implemented and Ongoing.

Agency's Comments on Implementation Status of Recommendation:

As noted in its written response in the Audit Report, SIPA staff monitors and makes decisions related to bank account balances on a weekly basis and this practice will continue. SIPA manages its financial accounts in a manner that allows it the most flexibility for cash flow and maximum interest income.

Recommendation #: 8a.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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.

Agency's Response: a. Agree. Implementation date: February 2013.

Agency's Written Response in Audit Report:

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.

Current Implementation Status of Recommendation:

Implemented.

Agency's Comments on Implementation Status of Recommendation:

Following the release of the Audit Report, SIPA's executive director and legal counsel continued working with an insurance broker to develop a comprehensive risk management program for SIPA. Based on the advice of the insurance broker, and following discussions with SIPA's Board of Directors, SIPA procured policies covering Professional and Technology Based Services, Technology Products, Information Security and Privacy, Multimedia and Advertising Liability, Designees and Officers, and Employment Practices.

Other potential insurance was discussed with SIPA's insurance broker, including automobile insurance, theft/fraud insurance, international travel insurance and property insurance. The insurance broker recommended that SIPA did not need any additional insurance at this time. It was noted that SIPA staff should routinely accept rental car insurance offered by rental car companies, and SIPA therefore adopted a policy that staff must accept rental car insurance when traveling on SIPA business.

Accordingly, SIPA believes that, combined with its existing policies, including policies regarding its fund balance and the fund balance itself, and based upon the professional advice of its insurance broker, SIPA now has appropriate insurance in place for an effective and comprehensive risk management program.

Recommendation #: 8b.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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

Agency's Response: b. Not Applicable. Implementation date: Not Applicable.

Agency's Written Response in Audit Report:

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

Current Implementation Status of Recommendation: No Longer Applicable.

Agency's Comments on Implementation Status of Recommendation:

Based on its implementation of Recommendation 8a, self-insurance is unnecessary, and therefore this recommendation is no longer applicable.

Recommendation #: 8c.

Agency Addressed: Statewide Internet Portal Authority

Original Recommendation in Audit Report:

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:

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

Agency's Response: c. Not Applicable. Implementation date: Not Applicable.

Agency's Written Response in Audit Report:

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

Current Implementation Status of Recommendation:

No Longer Applicable.

Agency's Comments on Implementation Status of Recommendation:

Based on its implementation of Recommendation 8a, self-insurance is unnecessary, and therefore this recommendation is no longer applicable.