



# OFFICE OF THE STATE AUDITOR



KERRI L. HUNTER, CPA  
—  
STATE AUDITOR

September 14, 2021

## EVALUATION OF WEB APPLICATION SECURITY AT THE COLORADO STATEWIDE INTERNET PORTAL AUTHORITY (PUBLIC REPORT) – STATUS REPORT

Members of the Legislative Audit Committee:

Attached is the status report from the Statewide Internet Portal Authority (SIPA) on the implementation of recommendations contained in the Office of the State Auditor's (OSA) *Evaluation of Web Application Security at the Colorado Statewide Internet Portal Authority – Public Report IT Performance Evaluation*.

### OSA REVIEW OF DOCUMENTATION

As part of the status report process, we requested and received supporting documentation for each recommendation that SIPA reported as having been implemented or partially implemented. Specifically, we reviewed the following documentation:

- Draft SIPA Information Security Policies and Procedures and documentation of SIPA's Board Members appointment reviewing the draft policies and procedures. (Recommendation Nos: 1-1, 1-2, and 1-3; Partially Implemented)
- Evaluation of SIPA staff security skills and competencies and the plan to address the identified gaps. (Recommendation No.: 1-4; Implemented)

Based on our review, the supporting documentation substantiates SIPA's reported implementation status.

OFFICE OF THE STATE AUDITOR  
1525 SHERMAN STREET  
7TH FLOOR  
DENVER, COLORADO  
80203

303.869.2800



Your public sector partner for technology  
*Colorado SIPA makes tech simple*

September 1, 2021

Kerri L. Hunter, CPA  
State Auditor  
Colorado Office of the State Auditor  
1525 Sherman St., 7<sup>th</sup> Floor  
Denver, CO 80203

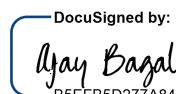
Dear Auditor Hunter:

In response to your request, we have prepared the attached status reports on the implementation status of evaluation recommendations contained in the Evaluation of Web Application Security at the Colorado Statewide Internet Portal Authority. The reports provide a brief explanation of the actions taken by the Colorado Statewide Internet Portal Authority to implement each recommendation.

We appreciate the opportunity to have undergone an audit of our web application security, as well as our processes related to security and vendor management. At SIPA, we believe that audits such as these provide us with the opportunity to improve our organization and better serve our state and local government partners.

If you have any questions about this status report and the Colorado Statewide Internet Portal Authority's efforts to implement the evaluation recommendations, please contact Jerrod Roth at (720) 409-5632 or [jerrod@cosipa.gov](mailto:jerrod@cosipa.gov).

Sincerely,

DocuSigned by:  
  
B5EFB5D277A84E2...  
Ajay Bagal  
Executive Director

## EVALUATION RECOMMENDATION STATUS REPORT

EVALUATION NAME	<i>Evaluation of Web Application Security at the Colorado Statewide Internet Portal Authority – Public Report</i>
EVALUATION NUMBER	<i>2050P-IT</i>
AGENCY	<i>Statewide Internet Portal Authority</i>
DATE OF STATUS REPORT	September 1, 2021

### SECTION I: SUMMARY

REC. NUMBER	AGENCY'S RESPONSE	ORIGINAL IMPLEMENTATION DATE	CURRENT IMPLEMENTATION STATUS	CURRENT IMPLEMENTATION DATE
1-1	Agree	December 2021	Partially Implemented	December 2021
1-2	Partially Agree	December 2021	Partially Implemented	December 2021
1-3	Agree	December 2021	Partially Implemented	December 2021
1-4	Agree	December 2021	Implemented	August 2021

## SECTION II: NARRATIVE DETAIL

### RECOMMENDATION 1-1

The Colorado Statewide Internet Portal Authority should improve security governance and management processes and controls by:

1. Establishing, with input from the Board, policies and procedures for managing risks related to information security. SIPA should seek input from the Board and establish requirements for conducting periodic security risk assessments, based upon an industry-recognized security framework, and utilizing the results of these assessments to determine areas of risk tolerance, risk mitigation, and risk avoidance. In addition, these policies and procedures should also establish requirements for periodic reporting of the status of security risk to the Board.

CURRENT IMPLEMENTATION STATUS	Partially Implemented	CURRENT IMPLEMENTATION DATE	December 2021
-------------------------------------	-----------------------	-----------------------------------	---------------

### AGENCY UPDATE

SIPA staff developed a draft policy that includes the elements outlined in this recommendation. It has been reviewed by the Governor's Office of Information Technology, IT Governance and Security staff. The policy was updated based on their feedback. Currently the policy is under review by members of the SIPA Board of Directors.

### RECOMMENDATION 1-2

The Colorado Statewide Internet Portal Authority should improve security governance and management processes and controls by:

2. Developing formal policies and procedures for the management of information security. These policies and procedures should cover, but not be limited to, the relevant aspects of security necessary to ensure the confidentiality, integrity, and availability of systems and services provided by SIPA to the State, address the security roles and responsibilities of SIPA personnel, partners, and data owners (e.g., State agencies or offices), define a frequency by which these policies and procedures will be reviewed and approved by SIPA management, conducting a review and approval in line with the determined frequency.

CURRENT IMPLEMENTATION STATUS	Partially Implemented	CURRENT IMPLEMENTATION DATE	December 2021
-------------------------------------	-----------------------	-----------------------------------	---------------

### AGENCY UPDATE

SIPA staff developed a draft policy that includes the elements outlined in this recommendation. It has been reviewed by the Governor's Office of Information Technology, IT Governance and Security staff. The policy was updated based on their feedback. Currently the policy is under review by members of the SIPA Board of Directors.

### RECOMMENDATION 1-3

The Colorado Statewide Internet Portal Authority should improve security governance and management processes and controls by:

3. Developing and clarifying in policies and procedures expected roles and responsibilities as they relate to state Security Policies. These policies and procedures should include expectations for account management and for providing timely and periodic training to these individuals on their security roles and responsibilities.

CURRENT IMPLEMENTATION STATUS	Partially Implemented	CURRENT IMPLEMENTATION DATE	December 2021
-------------------------------------	-----------------------	-----------------------------------	---------------

### AGENCY UPDATE

SIPA staff developed a draft policy that includes the elements outlined in this recommendation. It has been reviewed by the Governor's Office of Information Technology, IT Governance and Security staff. The policy was updated based on their feedback. Currently the policy is under review by members of the SIPA Board of Directors.

### RECOMMENDATION 1-4

The Colorado Statewide Internet Portal Authority should improve security governance and management processes and controls by:

4. Conducting an evaluation of the skills and competencies of the SIPA staff to identify gaps in the organization's security knowledge and experience with developing and executing a plan for addressing those gaps.

CURRENT IMPLEMENTATION STATUS	Implemented	CURRENT IMPLEMENTATION DATE	August 2021
-------------------------------------	-------------	-----------------------------------	-------------

### AGENCY UPDATE

The SIPA Chief Technology Officer has conducted an initial evaluation of staff skills and competencies related to security knowledge. This was completed by utilizing a commercially available software tool. A plan was developed to address shortfalls in security knowledge of staff.