COLORADO OFFICE OF THE STATE AUDITOR

We Set the Standard for Good Government

DEPARTMENT OF STATE

NOVEMBER 2015 PERFORMANCE AUDIT

THE MISSION OF THE OFFICE OF THE STATE AUDITOR
IS TO IMPROVE GOVERNMENT
FOR THE PEOPLE OF COLORADO

LEGISLATIVE AUDIT COMMITTEE

Senator Lucia Guzman – Chair	Representative Dan Nordberg – Vice-Chair
Senator Chris Holbert	Representative Dianne Primavera
Senator Cheri Jahn	Representative Su Ryden
Senator Tim Neville	Representative Lori Saine

OFFICE OF THE STATE AUDITOR

Dianne E. Ray	State Auditor
Matt Devlin	Deputy State Auditors
Kerri Hunter	
Cindi Radke	Audit Managers
Pooja Tulsian	
Jarrett Ellis	Team Leader
Larry Ciacio	Staff Auditors
Henry Hung	
Kiran Keshav	
Terry Paulson	
Manijeh Taherynia	

AN ELECTRONIC VERSION OF THIS REPORT IS AVAILABLE AT
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 REPORT NUMBER 1503P WHEN REQUESTING THIS REPORT

OFFICE
OF THE STATE AUDITOR

We Set the Standard for Good Government

DIANNE E. RAY, CPA
STATE AUDITOR

November 20, 2015

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of the Department of State. This audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Department of State.

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

303.869.2800

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

CONTENTS

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

REPORT HIGHLIGHTS

DEPARTMENT OF STATE

PERFORMANCE AUDIT, NOVEMBER 2015

CONCERN

We found that the Department of State (Department) lacks formal documented processes for cash fund management and budgeting and there is no statutory definition of the structure and oversight of the Business Intelligence Center (Center) to ensure effective management, accountability, and transparency of Center operations. Our audit also found that the Department did not always ensure compliance with statutes, best practices, and its own internal policies for its information technology (IT) processes.

KEY FACTS AND FINDINGS

- The Department did not identify and establish appropriate fee levels for business registration and filing fees charged in Fiscal Years 2012 through 2014, to ensure that fee revenue correlated to its incurred costs. In addition, we found that the Department lacked adequate written procedures to establish, review, and approve budgets.
- Donations and related expenditures transactions for the Center are accounted for outside of the State's accounting system, excluding both the revenue and expenditures information from publicly-available State financial information.
- The Center program lacks formal oversight, structure, and documented policies, procedures and processes. As a result, we were unable to determine if the Center was meeting Department goals and program objectives.
- The Department did not comply with Sections 24-37.5-404(3) and 24-37.5-404(4), C.R.S. to ensure its Agency Cyber Security Plan was approved by the Governor's Office of Information Technology's Chief Information Security Officer, within the required deadlines.
- The Department has not formalized a service level agreement with the Governor's Office of Information Technology (OIT) to ensure that IT services provided by OIT are meeting the Department's needs.

BACKGROUND

- The Department is primarily funded via business filing fees, which comprised between 74 and 86 percent of the Department's total annual revenue in Fiscal Years 2010 through 2014.
- The Department established the Business Intelligence Center in Fiscal Year 2014 to consolidate public data relevant to businesses on a single platform and provide the tools to make this data useful for the business community.
- The Department maintains the Statewide Colorado Voter Registration and Election System (SCORE), as required by Section 1-2-302(1) and 1-2-301(4)(a)(II), C.R.S., which is used by both the Department and county clerks to carry out their responsibilities related to state and federal elections.

KEY RECOMMENDATIONS

The Department needs to:

- Ensure its budgetary practices provide coverage for the cost of services while maintaining a reasonable cash fund balance by establishing and documenting a strategic cash fund management plan and formalizing the procedures for fee revisions.
- Improve the structure, accountability and transparency of the Business Intelligence Center Program.
- Complete and submit its current Agency Cyber Security Plan to the State's Chief Information Security Officer for approval and ensure future submissions meet the required annual deadlines.
- Work with OIT to develop a service level agreement, develop and document performance metrics to measure OIT's services, and perform periodic reviews of OIT.

The Department of State agreed with the audit recommendations in this public report.

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

CHAPTER 1

OVERVIEW

The Secretary of State (Secretary) is one of five independently elected constitutional officers of the State. As the chief executive officer of the Department of State (Department), the Secretary administers Colorado's elections laws [Section 1-1-107, C.R.S.], manages the statewide voter registration database [Section 1-2-301, C.R.S.], and administers funds received through the federal Help America Vote Act [Section 1-1.5-104, C.R.S.].

The Secretary also regulates charitable solicitations, charitable gaming, and notaries public in accordance with Statute [Sections 6-16-104, 12-9-103, and 12-55-103, C.R.S., respectively]. As the State's primary record keeper, the Secretary of State collects, stores, and provides public access to annual reports, articles of incorporation, liens, and other documents filed according to Titles 4 and 7, C.R.S., and the Uniform Commercial Code [Title 4, C.R.S.].

The Department is comprised of four divisions:

- Elections Division
- Business and Licensing Division
- Information Technology Services Division
- Administration Division

THE ELECTIONS DIVISION supervises primary, general, and congressional vacancy elections [Section 1-1-107, C.R.S.]; maintains the statewide voter registration system [Section 1-2-301, C.R.S.]; authorizes official recounts for federal, state, and district elections [Section 1-10.5-102, C.R.S.]; and administers the Fair Campaign Practices Act [Section 1-45-111.5, C.R.S.]. This Division also helps the Secretary of State supervise the State's 64 county clerks in the execution of their statutory responsibilities relating to voter registration and elections [Section 1-1-107, C.R.S.].

THE BUSINESS AND LICENSING DIVISION, created in the Fiscal Year 2013-14 Long Bill, is responsible for the programmatic functions previously carried out in the Administrative Division related to business filings and licensing services. This Division is responsible for (1) collecting, storing, and providing public access to articles of incorporation, annual reports, and a variety of other documents filed by for-profit and not-for-profit entities under Colorado's corporation and association laws [Section 7-90-301, C.R.S.]; (2) collecting, storing, and providing public access to a variety of Uniform Commercial Code documents, including security interests, liens, and other items that are utilized by lending institutions [Section 4-9.5-108, C.R.S.]; (3) registering business names and organizations, trade names, and

trademarks [Section 7-90-301, C.R.S.]; (4) administering the State Administrative Rules Code, a body of statutes governing the rule-making authority of many state agencies [Section 24-4-103, C.R.S.]; (5) overseeing the bingo and raffles program pursuant to Section 3 of Article XVIII of the Colorado Constitution; (6) administering the Charitable Solicitations Act [Title 6, Article 16, C.R.S.], which forbids fraudulent charitable solicitation; and (7) licensing and regulating notaries public [Section 12-55-103, C.R.S.]. This Division also operates the Business Intelligence Center (Center), a program that the Department created to provide the Colorado business community with easier access to public data stored on State information systems.

THE INFORMATION TECHNOLOGY (IT) SERVICES DIVISION provides technical services, systems development, and support to the Department. Specifically, its functions include (1) ensuring that the Department is compliant with rules and policies as set forth by the Colorado Information Security Act, and (2) managing both the Business and Licensing Division's web based systems used for electronic filing and online services offered to the public, and the State of Colorado Registration and Elections system (SCORE), which is the statewide computerized voter registration system, in accordance with Sections 1-2-302(1) and 1-2-301(4)(a)(II) C.R.S.

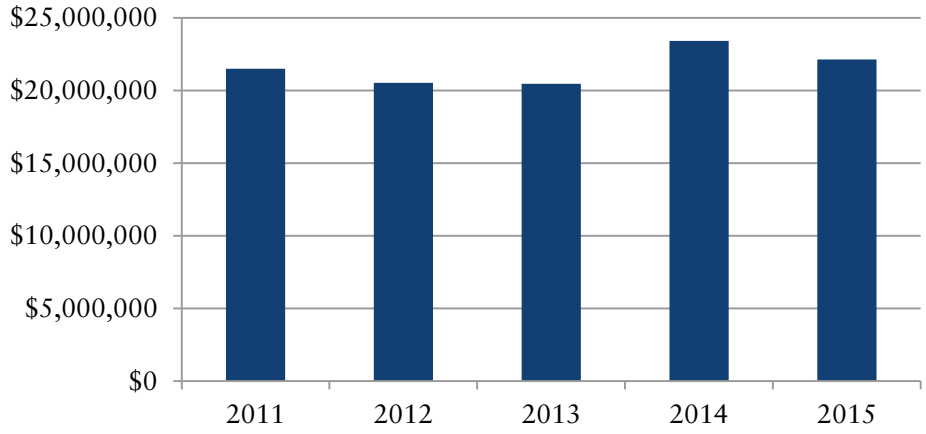
THE ADMINISTRATION DIVISION provides general management supervision for the entire Department, including budgeting, accounting, and human resource services.

FUNDING AND FINANCES

The majority of funding for the Department consists of cash funds, primarily from business filing fees deposited into the Department of State Cash Fund. The other funding source for the Department is the Federal Elections Assistance Fund, which supports the federal Help America Vote Act (HAVA) program. Monies in the Federal Elections Assistance Fund are continuously appropriated. As shown in EXHIBIT 1.1, the Department was appropriated cash funds ranging between

approximately $20.5 million and $23.4 million each year during the Fiscal Years Ending June 30, 2011 through June 30, 2015.

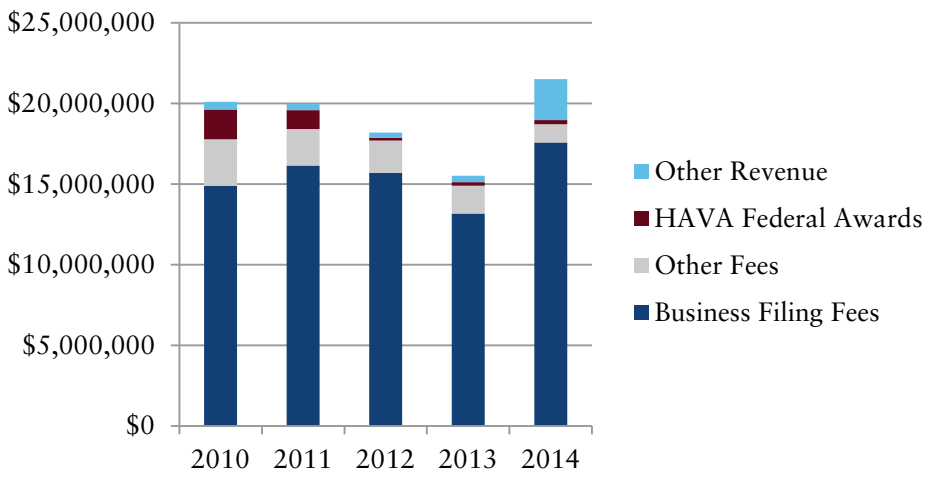
EXHIBIT 1.1. DEPARTMENT OF STATE APPROPRIATIONS
DEPARTMENT OF STATE CASH FUND
FISCAL YEARS ENDING JUNE 30, 2011 - JUNE 30, 2015



SOURCE: Office of the State Auditor analysis of Fiscal Year 2013-14 and Fiscal Year 2014-15 Joint Budget Committee Appropriations Reports.

As shown in EXHIBIT 1.2, the Department's primary source of revenue is fee revenue. Total fee revenues during Fiscal Years Ending June 30, 2010 through June 30, 2014, ranged between 87 and 97 percent of the Department's total revenue. Business filing fees comprised between 74 and 86 percent of the Department's overall revenue during the same period, while other fee revenue, including fees for registering charitable organizations, notaries public, bingo halls, and political lobbyists comprised an additional 5 to 14 percent of the Department's total revenue. Federal HAVA funds, which are continuously appropriated, declined from 9 percent to approximately 1 percent of overall revenue over this period. Other notable revenue sources included a transfer from the State's General Fund of $2.175 million in Fiscal Year 2014. Pursuant to HB14-1341, the State Legislature repaid $2.175 million in general funds that it had previously swept from the Department's cash fund.

EXHIBIT 1.2. DEPARTMENT OF STATE REVENUE
FISCAL YEARS 2010 THROUGH 2014



SOURCE: Office of the State Auditor's analysis of data from the Colorado Financial Reporting System (COFRS).

AUDIT PURPOSE, SCOPE, AND METHODOLOGY

We conducted this performance audit pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of the state government. We performed audit work from March 2015 through November 2015. 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 the audit evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We acknowledge and appreciate the cooperation and assistance provided by the Department of State during this audit.

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 controls are described in the audit findings and recommendations. The key objectives of the audit were to determine whether:

- The Department has adequate budgeting processes in place to establish, assess, and revise fees.

- The Department maintains adequate oversight, authority, accountability, and transparency of Business Intelligence Center (Center) operations.

- The Department has adequately ensured the confidentiality, availability, and reliability of the Statewide Colorado Voter Registration and Election system (SCORE).

To accomplish our audit objectives we performed the following audit work:

- Reviewed the Department's budget requests submitted to the Joint Budget Committee and the Department's policies and procedures, interviewed Department staff to determine how budgets are created, and compared the Department's budgeting process with best practices published by the Government Finance Officers Association and the National Association of State Budget Officers to identify any gaps in their processes.

- Reviewed applicable statutes, staff responsibilities, and Department policies and procedures to determine the Center structure, oversight, and program roles and responsibilities; interviewed Department staff to understand Center program operations and how the success of the program is measured; and compared the Center program structure, oversight, accountability and transparency with best practices published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

- Reviewed applicable statutes and Department and State IT policies to determine the data availability, reliability, and confidentiality requirements for the SCORE system; interviewed Department IT staff to understand the roles and responsibilities in achieving the desired IT controls; and inspected the IT controls and associated documentation over the SCORE system to determine whether the Department's controls were designed according to policy and operating effectively.

We relied on sampling techniques, to support our audit work. Specifically:

- We selected a non-statistical, judgmental sample of 25 total expenditure transactions made from donated funds and Center appropriations to review compliance with State Fiscal and Procurement Rules.

- We selected a non-statistical, judgmental sample of six changes made to the SCORE system to evaluate whether the Department's change control procedures were designed adequately and operating effectively, to ensure that only authorized changes were made to the SCORE system.

- We selected a non-statistical, judgmental sample of seven SCORE backup tapes to determine whether backup tapes were sent to an offsite location on a periodic basis to ensure quick retrieval in the event of a disaster.

When samples were chosen, the results of our testing were not intended to be projected to the entire population. Rather, the samples were selected to provide sufficient coverage of those areas that were significant to the objectives of this audit.

We also planned our audit work to address one additional objective to determine whether the Department accounts for all of its license and fee revenues in the State's accounting system. Based on the results of our testwork, we had no recommendations in this area.

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 controls, as well as specific details about the audit work supporting our findings, conclusions, and recommendations, are described in CHAPTERS 2 and 3 of this report.

During our audit work, we identified certain matters that are not included in this audit report that were reported to the Department's management in a separate confidential report dated November 2015. These matters were considered sensitive to protecting state information technology assets.

In addition, we communicated certain deficiencies in internal control that were not significant to the objectives of the audit to the Department's management in a separate letter dated November 12, 2015.

CHAPTER 2

DEPARTMENT OF STATE OPERATIONS

The Department of State is responsible for the sound financial management of its Department of State Cash Fund and the day to day operations and oversight of its Business Intelligence Center (Center). We identified several problems with the

Department's cash fund management and budgeting processes and oversight of the Business Intelligence Center. Specifically, we found that the Department lacks formal documented processes to ensure that its cash fund revenues approximate its expenditures, and lacks formal procedures to establish, review, and prepare its budget. We also found that the Department has not formally defined the structure and oversight of its Business Intelligence Center. We discuss these issues and our recommendations in the remainder of CHAPTER 2.

CASH FUND MANAGEMENT AND BUDGET PROCESS

As previously discussed, the principal source of revenue for the Department of State is fee revenue collected for various business registrations and filings. The Department records these revenues in the Department of State Cash Fund. As part of its annual budget request, the Department submits a report of the Department of State Cash Fund including its forecasted revenue, estimated expenditures, and anticipated Department of State Cash Fund balance for the next fiscal year. The Department's budget requests are subject to the State's annual budget process for approval and adoption in the annual appropriations bill, or Long Bill.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

Throughout the audit, we interviewed Department personnel. We also reviewed Department budget requests submitted to the Joint Budget Committee (JBC) for Fiscal Years 2014, 2015, and 2016 along with the supporting documentation used to compile these requests. We analyzed data from the State's accounting system—the Colorado Financial Reporting System (COFRS) prior to July 1, 2014, and the

Colorado Operations Resource Engine (CORE) as of July 1, 2014. We also reviewed statutes relevant to the Department of State Cash Fund and researched best practices relative to setting fees and managing government cash funds.

The purpose of our audit work was to determine whether the Department has adequate cash management and budgeting processes in place to assist it in establishing, assessing, and revising its fees, and to help ensure that it complies with the related statutory requirements.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

STATUTORY REQUIREMENTS. Statute [Section 24-21-104(3)(b), C.R.S.] requires the Department to "adjust its fees so that the revenue generated from the fees approximates its direct and indirect costs, including the cost of maintenance and improvements necessary for the distribution of electronic records; except that the department may reduce its fees to generate revenue in an amount less than costs if necessary pursuant to Section 24-75-402(3)." Section 24-75-402(3)(c), C.R.S. mandates that "the uncommitted reserves of any cash fund at the conclusion of any given fiscal year shall not exceed the target reserve," and Section 24-75-402(2)(e.5), C.R.S. defines the target reserve as 16.5 percent of the fiscal year's expenditures. The Governmental Accounting Standards Board defines fund balance, or uncommitted reserves as used in relation to cash funds, as the difference between assets and liabilities in a fund. Therefore, the excess or deficit of revenue over expenditures equals additions to, or subtractions from, fund balance. Because of this interdependent relationship, if one of these primary components of a fund changes, at least one of the remaining two items is affected to keep the relationship in balance. For example, if revenues decrease below the level of expenditures, fund balance decreases.

GOVERNMENT FINANCE OFFICERS ASSOCIATION (GFOA) BEST PRACTICES. The GFOA's *Recommended Budget Practices, A*

Framework for Improved State and Local Government Budgeting recommends that government entities evaluate revenue and expenditure options together and adopt formal written policies that identify the manner in which fees and charges are set to the extent to which they cover the cost of services.

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS (AICPA) BEST PRACTICES. The AICPA's *Audit and Accounting Guide for State and Local Governments*, *March 1, 2014*, recommends adoption and communication of procedures to establish authority and responsibility for budget development, approval, and amendments.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

Overall, we found that the Department did not identify and establish appropriate fee levels for business registration and filing fees charged in Fiscal Years 2012 through 2014 to ensure that fee revenue correlated to its incurred costs. In addition, we found that the Department lacked adequate procedures to establish, review, and approve budgets. The specific issues we identified are described in more detail below.

CASH FUND TRENDS. Our analysis of the Department's actual expenditures, revenue, and fund balance for the period July 1, 2012 through December 31, 2014, indicates widely varying trends in the Department's fund balance which resulted from variances in revenues and expenditures. Specifically, we found the following:

- **VARYING FUND BALANCE.** While the Department maintained uncommitted cash fund reserves in excess of the statutory 16.5 percent limit until October 2012, its fund balance fell to levels as low as $1.3 million, approximately $2 million below the Department's statutory limit, for the first three quarters of Fiscal Year 2014, after it enacted a fee holiday for the period of October 1, 2012 through February 28, 2013. Additionally, the Department

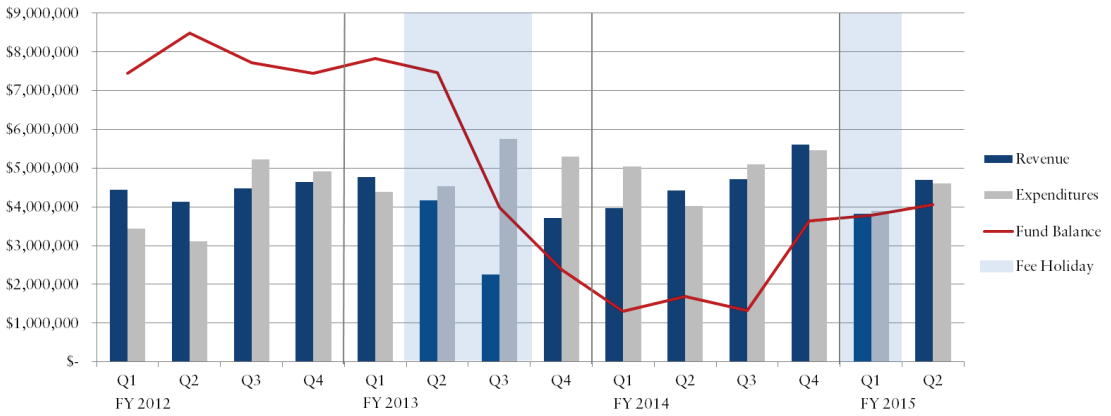
incurred substantial unanticipated costs, reducing the fund balance, to implement HB 13-1303, which required extensive revisions to the State's voter registration system and increased reimbursements to counties for election expenses. Further, pursuant to HB14-1341, at the close of Fiscal Year 2014, the General Assembly repaid $2.175 million in general funds that it had previously swept from the Department's cash fund, unexpectedly increasing the fund balance.

- **VARYING FEES.** As previously mentioned, the Department enacted fee holidays from October 1, 2012, through February 28, 2013, and again from July 1, 2014, through October 31, 2014. As a result, businesses were charged different fee amounts depending on when they registered or filed with the Department. For example, prior to October 1, 2012, the fees to register a trademark or register as a bingo hall owner were $30 or $1,000, respectively; however, from October 1, 2012, through February 28, 2013, the fees were reduced to $1.

- **REVENUE SHORTFALLS.** Due to the cyclical nature of the Department's operations, Department staff indicated that expenditures typically outpace revenues in Quarter 3 of each fiscal year. However, we noted that expenditures also significantly outpaced revenues in Quarter 4 of Fiscal Year 2013 and Quarter 1 of Fiscal Year 2014; these two quarters were outside of Department-enacted fee holidays. The results of operations in these quarters directly contributed to the low fund balance in Quarters 1 through 3 of Fiscal Year 2014.

EXHIBIT 2.1 shows revenue, expenditure, and fund balance trends for the Department of State Cash Fund by quarter from July 1, 2011, through December 31, 2014.

EXHIBIT 2.1. DEPARTMENT OF STATE CASH FUND
TRENDS IN ACTUAL REVENUE, EXPENDITURE, AND FUND BALANCE
JULY 1, 2011 THROUGH DECEMBER 31, 2014



SOURCE: Office of the State Auditor's analysis of data from the Colorado Financial Reporting System, July 2011 through June 2014, and Colorado Operations Resource Engine, July through December 2014.

INTERNAL REVIEW AND APPROVAL OF BUDGETS. We found that the Department's budget requests submitted to the Joint Budget Committee for Fiscal Years 2014 and 2015 contained unsupported numbers and that the Department did not have formal procedures in place to establish authority and responsibility for budget development, approval, and amendments. The concerns we identified are:

- **LACK OF SUPPORTING DOCUMENTATION.** The Department did not provide us with supporting documentation for any of the amounts, both revenues and expenditures, contained in the Fiscal Year 2014 budget request. In addition, for the Fiscal Year 2015 budget request, the Department could not provide us with supporting documentation, such as calculations or estimates used to derive planned changes from prior year expenditures, to explain the source of more than one-third of the figures reflected in the budget request. These unsupported revenues and expenditures net to approximately $1.66 million. The Department did provide us with supporting documentation for the numbers contained in its Fiscal Year 2016 budget request.

- **LACK OF DOCUMENTED REVIEW AND APPROVAL.** During our review of the Department's Fiscal Years 2014, 2015, and 2016 budget documents, we found that the budget documents did not contain evidence of internal reviews or approvals. Department staff indicated that Department management reviewed and approved the budget documents through verbal conversations with staff.

WHY DID THE PROBLEMS OCCUR?

Overall, we noted that the Department does not have a formal plan in place to facilitate management of the Department of State Cash Fund to meet strategic goals. Specifically, the Department has not (1) defined objectives for managing the cash fund or (2) developed and implemented procedures, including those to establish, review, and revise fees, as necessary, to achieve the objectives.

We also noted that the Department lacks formal written policies and procedures for its annual budget request process, including, but not limited to, specifying which budget items are to be reviewed, who is to perform the reviews, and how the reviews are to be documented.

WHY DO THESE PROBLEMS MATTER?

The lack of a formal strategic cash fund management plan could lead to unpredictable trends in the Department's finances. In addition, the Department-enacted fee holidays ultimately resulted in businesses being charged fees inequitably, based on when they paid the fees. For example, the full-rate fees paid by registrants outside of fee holiday periods effectively subsidize the discounted rates paid by other businesses during fee holidays.

In addition, when the Department does not document a formal review of its budget request, there is a potential risk that inaccurate figures will be included in the budget request. As a result, the Joint Budget Committee and other parties charged with governance may not receive accurate insight into the Department's financial status and may, therefore, make decisions based on inaccurate data.

RECOMMENDATION 1

The Department of State should ensure that its budgetary practices provide coverage for the Department's cost of services while maintaining a reasonable cash fund balance by establishing and documenting a strategic cash fund management plan, including:

A Establishing objectives to support managing the cash fund to its strategic goals.

B Creating and implementing formal policies and procedures for establishing, reviewing, and revising fees, as deemed appropriate, to meet statutory requirements and its objectives as established in PART A.

C Formalizing written policies and procedures for the preparation of the Department's annual budget request, including the establishment of a documented review process.

RESPONSE

A AGREE. IMPLEMENTATION DATE: JULY 2016

Over the past year and a half, the Department has significantly upgraded the capacity of its Finance Unit. This turnover of staff resulted in more rigorous monitoring of the Department's financial performance and to significant improvements to cash fund management in FY 2014-15. While the Department is in compliance with the maximum cash fund reserve limits established in CRS §24-75-402 (2015), it recognizes that it would benefit from a more formal cash fund management policy. To accomplish this objective, the Department's Finance Unit will work with the Secretary of State, Chief of Staff, and other members of senior staff to create a cash fund management policy that both complies with the statutory maximum cash fund reserve and the Department's strategic goals.

B AGREE. IMPLEMENTATION DATE: JULY 2017

As previously noted, over the past year and a half, the Department has improved the capabilities of its Finance Unit. The current team has greatly improved internal monitoring and reporting of the Department's financial performance. Under CRS §24-21-104(3)(b) (2015), the Department is charged with setting its fees at levels that are appropriate to cover the Department's costs and to ensure compliance with CRS §24-75-402 (2015). The Department complied with this statute in FY 2014-15 and believes that it has followed sound practice in the analyses utilized for the establishment of new fees and the monitoring of fee holidays. That said, the Department recognizes that it would benefit from a more formal process for the regular review and potential revision of its fees.

In order to implement this recommendation, the Department's Finance Unit will work with the Secretary of State, Chief of Staff, and other members of senior staff to establish a regular schedule and formal process for reviewing the Department's fees.

C AGREE. IMPLEMENTATION DATE: JULY 2016

As previously noted, over the past year and a half, the Department has improved the capabilities of its Finance Unit. Furthermore, as noted in the audit report, the Department provided the auditors with complete supporting documentation for the FY 2015-16 budget request (the first prepared by current Finance Unit staff). While the Department is pleased with the improvement in the quality of its budget requests, it recognizes that it would benefit from a more formal budget document review process and written policies and procedures for the preparation of the Department's annual budget request.

The Department has already taken action towards implementing this recommendation. In addition to the existing informal budget conversations and approvals, the Department's Chief of Staff

formally signed off to indicate his review of all budget schedules submitted as part of the FY 2016-17 budget request.

In addition, the Department has solicited sample policies from other state agencies for examples of budget policy and procedure documents. The Department intends to adapt these policies to its needs. Upon receipt of the examples, the Department's Finance Unit will work with the Chief of Staff and other members of senior staff to formalize the policies and procedures for the development of future Department budget requests.

BUSINESS INTELLIGENCE CENTER

State departments and agencies hold vast amounts of data in various systems and formats. In July 2013, the Secretary of State collaborated with the Governor's Office of Information Technology and the Office of Economic Development and International Trade, and the Statewide Internet Portal Authority to consolidate public data relevant to businesses on a single platform and provide the tools to make this data useful for the business community, forming the Business Intelligence Center (Center). The Center currently operates within the Department of State with one dedicated full-time equivalent staff who serves as the Center program manager. Center operations are supported by the Executive Committee and the Advisory Board. The Executive Committee is currently comprised of the following:

- Secretary of State
- Center Program Manager
- Governor's Chief Strategy Officer
- Representatives from the Governor's Office of Information Technology and the Office of Economic Development and International Trade

The Advisory Board is currently comprised of 13 members, including representatives from:

- Department of State
- Governor's Office of Information Technology
- Governor's Office of Economic Development and International Trade
- Governor's Office of Policy, Research and Legislative Affairs
- Statewide Internet Portal Authority
- Interested parties from the private sector

To execute the daily operations of the Center, the program manager oversees two contracts. The Department contracts with Xentity

Corporation, a data consulting and support services company to facilitate the gathering and publishing of public data, which is then hosted on the Colorado Information Marketplace, a data repository maintained by the Governor's Office of Information Technology. The Department also contracts with a marketing and events management firm to facilitate, market, and conduct the Go Code Colorado Challenge (Challenge), a contest where the technology community develops various applications to use the published public data to provide solutions to current business problems. The annual Challenge events highlight the publicly available data the Department aggregates through the Center.

The Department was appropriated $750,000 and $1.5 million in the Department of State Cash Fund in Fiscal Years 2014 and 2015, respectively, to fund the program. In addition to the use of appropriated funds, Department staff and the marketing contractor solicit program sponsors to donate money to help fund Challenge activities. Department staff entered into a service agreement with Denver Civic Ventures (DCV), a 501(c)(3) not for profit corporation, to act as a fiscal agent—someone who manages fiscal matters on behalf of another party—for any donated revenues. The Center received approximately $76,000 and $71,000 in donated revenues in Fiscal Years 2014 and 2015, respectively.

OVERSIGHT AND ACCOUNTABILITY OF THE BUSINESS INTELLIGENCE CENTER OPERATIONS

The Center's mission is to "promote economic growth and good governance by making business-relevant data accessible and useable for informed decision-making and to create and nurture a vibrant environment where Colorado business challenges are addressed." To accomplish this mission, the Department has established a number of objectives related to the strategic direction of the Center. These objectives include the following:

- Partner with local, state, and federal government and private industry to identify and make data resources accessible.
- Provide resources to help users effectively leverage data and data resources.
- Work with the Colorado business community to identify business challenges it faces.
- Annually create and run Go Code Colorado to challenge teams to create software applications to solve business challenges using public data.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

We interviewed Department personnel to gain an understanding of the Center's purpose, structure, policies, procedures, and processes. We reviewed statutes related to the Department's roles, responsibilities, authorities, structure, and operations. We also reviewed statutes related to the SMART Act and nonprofit entities supported by State agencies. Additionally, we reviewed the Center's program budget and appropriations requests, service agreement and contracts, and expenditures for Fiscal Years 2014 and 2015. In addition, we compared the Center's program charter, mission, and Advisory Board and Executive Committee responsibilities to best practices established by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

We performed these procedures to determine whether the Department's oversight of the Center was effective to ensure the Center maintained accountability and transparency and established formal program policies.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

SMART ACT. The State Measurement for Accountable, Responsive, and Transparent (SMART) Government Act [Section 2-7-201, C.R.S.]

established a performance-based budgeting system for Colorado. Section 2-7-202(5), C.R.S., identifies the departments and offices that are subject to the new performance-based budgeting requirements under the SMART Government Act. The departments identified in statute include the Department of State. As expressed in the legislative declaration of the SMART Act [Section 2-7-201, C.R.S.], one goal of the Act is to ensure that state government is accountable and transparent in such a way that the general public can understand the value received for the tax dollars spent by the State.

DONATION BEST PRACTICES. Various State agencies that receive donations from private individuals and organizations share many common traits in the treatment of donated revenue and associated expenditures. These traits can be considered an established system of best practices. Typically, statutes provide express authorization to receive donations with language such as "the department is authorized to accept and receive gifts and donations for the purpose of…" To maintain a tax deductible status for donations, these agencies establish relationships with organizations, which are designated as 501(c)(3) not for profit corporations. Donors gift to these organizations rather than directly to the agencies. Agencies then seek nonappropriated spending authority for the donated funds from the Office of the State Controller (OSC). When the agencies expend money for purposes supported by donations, they then request reimbursement from the not for profit organization or similar entity. Upon receipt of the reimbursement, agencies record revenue in one of the 13 revenue accounts established in CORE to account for various sorts of donation revenues. This process allows donors to benefit from a tax deductible status by gifting to not-for-profit organizations or similar entities, while still allowing for transparency. These best practices facilitate transparency and accountability because lawmakers and other interested parties are able to easily discern donation activity and expenditures as recorded on CORE.

FINANCIAL DATA. State Fiscal Rule 1-2 requires departments to use the state financial system to record their financial transactions and financial information.

PROGRAM AND GOVERNANCE STRUCTURE BEST PRACTICES.

COSO is a joint initiative of the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, The Association of Accountants and Financial Professionals in Business, and The Institute of Internal Auditors. The organization was created in 1985 to study the elements leading to fraudulent financial reporting. In 1992, COSO published a framework for internal control, which is a set of best practices that organizations can employ to improve accountability and transparency in financial reporting and operations. This framework was most recently revised in 2013. *COSO Internal Control–Integrated Framework, May 2013*, establishes key principles necessary to maintain an effective environment of internal control. These principles include:

- **EXERCISING OVERSIGHT RESPONSIBILITY.** The board of directors should demonstrate independence from management and exercise oversight of the development and performance on internal control.

- **ESTABLISHING STRUCTURE, AUTHORITY, AND RESPONSIBILITY.** With board oversight, management should establish structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

- **ENFORCING ACCOUNTABILITY.** The organization should hold individuals accountable for their internal control responsibilities in the pursuit of objectives. The organization should deploy control activities through policies that establish what is expected and procedures that put policies into action.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

Overall we identified problems with the structure and oversight of the Business Intelligence Center and the adequacy of its internal controls and accountability to the State, as discussed below.

LACK OF TRANSPARENCY AND ACCOUNTABILITY FOR DONATIONS. We found that Department of State personnel do not follow best practices in the treatment of donations made to support Center operations. Sponsors and supporters of Go Code Colorado provide monetary donations to help finance the activities of the Go Code Colorado challenge events. These donations are made directly to DCV, who holds the funds for the benefit of the Department. The Department is not statutorily authorized to receive donations for the purposes of the Center; however, DCV retains physical custody of donated funds, thereby precluding a statutory violation. The service agreement (agreement) between the Department of State and DCV defines responsibilities for both parties. Specifically, the agreement states that DCV may only disburse funds upon explicit authorization from the Center Program Manager. In practice, the Center Program Manager incurs expenses related to the Go Code Colorado challenge and submits the invoices to DCV for payment. Because the payments are issued by DCV, a third party, the revenue and expenditure transactions are accounted for outside of the State's accounting system; excluding both the revenue and expenditures information from publicly-available state financial information.

Department management reported, and we verified through our audit testwork, that the Department sought and received guidance from the Office of the State Controller regarding the use of an external entity to receive donations prior to establishing the process.

BUSINESS INTELLIGENCE CENTER STRUCTURE. We were unable to determine if the Center was meeting Department goals and program objectives. Specifically we noted that the program lacked formal oversight, structure, and documented policies, procedures, and processes.

- **LACK OF OVERSIGHT AND STRUCTURE.** We found that the Center Executive Committee and the Advisory Board were not consistently recognized as the oversight mechanism for the program. In a white paper published on the Department's website in April of 2013 that detailed the Department's plan to create the

Center, the Department explained that the Executive Committee was to provide senior level approval and support for the overall project mission and charter while the Advisory Board was to advise the Program Manager on the operation of the Business Intelligence Center and help identify Go Code Colorado challenge problems, judges, and partners. However, we determined through interviews with Department personnel that neither of these two bodies is charged with oversight of the program; rather, the Executive Committee is purely informational in nature while the Advisory Board is more of an operational-level working group. While Department staff indicated that Department management, including the Secretary of State, is charged with oversight of the Center program, we found that the Department had not formally documented oversight authority and responsibilities beyond that of the Center Program Manager, as specified in the Manager's Position Description.

- **Lack of documented policies, procedures, and processes.** We found that the Center does not have documented policies and procedures to operate the program. For example, Center program staff indicated they informally consider State Fiscal and Procurement Rules when managing the Center program, but they do not have written policies in place to ensure that they do so, particularly when expending Go Code Colorado donations made to DCV.

WHY DID THE PROBLEMS OCCUR?

Based on our review of statutes defining the Department's roles, responsibilities, authorities, structure, and operations, we found no statutory definition of the Business Intelligence Center. Although the responsibilities and objectives of the Department of State are listed in statute, its responsibilities and objectives related to the Center program are not. While the General Assembly has endorsed the Center program by funding it through the Long Bill, a lack of statutory definition and authority precludes us from assessing whether or not the program meets its legislative intent.

In addition, there is a lack of defined governance over the Center, as demonstrated by the lack of defined roles for the Executive Committee, Advisory Board, and Department management, or other guidance, including policies and procedures related to accounting for donations and the related expenditures of the Center. Without clearly defined and delineated governance responsibilities among key parties involved in the Center, it is difficult for the Department to ensure all critical components of internal controls are implemented to achieve adequate oversight in management and financial operations of the Center program.

WHY DO THESE PROBLEMS MATTER?

When the Department does not have defined oversight, structure, and responsibilities of its program, there is a risk of noncompliance with related laws and regulations, as well as a lack of accountability in its operations and finances. Based on our review of 10 Center expenditures made by the DCV under the Department's direction during Fiscal Year 2014, we found issues related to noncompliance with State Fiscal Rules in nine out of the 10 expenditures (90 percent). The issues included:

- Two payments totaling $1,000 made to a Center staff member that were authorized by the staff member himself/herself, who is no longer a State employee.

- A payment of $5,000 issued outside of the State payroll system to a Department temporary employee, which department records indicated was intended as contractor compensation in lieu of overtime, circumventing the controls of the State payroll system.

- Seven reimbursements of expenses totaling over $15,370 that did not contain supporting documentation.

The Department took action to strengthen controls over the Center program at the beginning of Fiscal Year 2015, which included hiring a new Center Program Manager who worked with the Department Controller to implement standard Department financial practices. We

noted no issues in the Center expenditures we tested that were made by the DCV under the Department's direction during Fiscal Year 2015. However, a lack of documented policies and procedures increases the risk of repeating the matters noted in the Fiscal Year 2014 transactions, which can undermine public confidence in the program, potentially resulting in a negative impact on the growth of the program and its ability to fulfill its mission.

Further, as the Department continues to receive accolades for the program, existing and new sponsors have donated an additional $35,000 in Fiscal Year 2016, as of September 30, 2015. Due to the potential for continued program growth and public interest, it is important to ensure that the proper mechanisms are formally defined and best practices are codified and documented to facilitate effective oversight, accountability, and transparency.

RECOMMENDATION 2

The Department of State should improve the structure, accountability, and transparency of the Business Intelligence Center (Center) by:

A Working with the General Assembly to define the objectives, responsibilities, and structure of the Center.

B Creating formal roles for Department management, the Executive Committee, and the Advisory Board.

C Developing formal policies and procedures for Center operations, including those related to accounting for donations and related expenditures, once the formal roles in PART B are established.

RESPONSE

A AGREE. IMPLEMENTATION DATE: JULY 2016

The Department will work with the legislature during the 2016 legislative session to formally establish the Business Intelligence Center in statute. The Department has worked with the legislature during the 2013 legislative session to obtain spending authority to create the program and during the 2015 legislative session to obtain spending authority on an ongoing basis to continue program operations. The Department will seek legislation to formalize these operations, which the legislature has already approved through the budget process.

B AGREE. IMPLEMENTATION DATE: JULY 2016

The Department intends to implement this recommendation through formally-documented internal policies. Though the audit report indicates a lack of defined governance, the Business Intelligence Center (Center) falls within the same structure as other departmental programs, with the program manager reporting to

Department management and the responsibilities and expectations of the program manager laid out in the program manager's position description (PD). The Department will develop formal documentation that clearly defines the roles and responsibilities with respect to the Center for Department management, the Executive Committee, and the Advisory Board.

C AGREE. IMPLEMENTATION DATE: SEPTEMBER 2016

The Department will seek statutory authority to accept gifts, grants, and donations during the 2016 legislative session.

Over the past year, the Department has significantly improved its documentation and approval practices related to donated funds. Shortly after taking the position, the current Business Intelligence Center (Center) Program Manager approached the Department's Controller to discuss best practices for approvals and backup documentation related to the expenditure of donated funds. The Program Manager's improvement efforts are evidenced by the lack of exceptions noted in the auditor's samples since controls were strengthened beginning in Fiscal Year 2015.

If and when the legislature grants the Department statutory authority to accept donations, the Department's Finance Unit will work together with the Center Program Manager, the Office of the State Controller (OSC), and Denver Civic Ventures, the Department's fiscal agent, to implement the best practices described in the finding.

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

CHAPTER 3

THE SCORE SYSTEM AND IT CONTROLS

The Colorado Department of State (Department) maintains the SCORE voter registration system, which performs integral election functions and stores registration and election data. Specifically, the system stores personally identifiable information including social security numbers, driver's license numbers, political party affiliation, and addresses. The system maintains a

list of all registered voters for the State of Colorado. State statutes are in place, which stipulate the purpose and functionality of the system. According to Section 1-2-302(1), C.R.S., "The Secretary of State shall maintain the master list of registered electors of the entire state on as current basis as possible." Section 1-2-301(4)(a)(II), C.R.S., notes that the centralized statewide registration system shall enable county clerk and recorders and the Secretary of State to maintain voter registration information, as well as carrying out their responsibilities related to the conduct of elections.

The SCORE system is composed of a desktop application, and a backend database used to store and process data. The system can also be accessed via a web application accessible from the Internet. The system is physically hosted within two different data center facilities, one located in Centennial, CO and the other in Lakewood, CO. Both of these data center facilities host the production environment of the SCORE system. A production environment is a live instance of the system where software and other products are put into operation for their intended use by end users. Both of these data centers are maintained by the OIT.

AUTHORITY OVER INFORMATION TECHNOLOGY

The "IT Consolidation Bill," codified through Sections 24-37.5-102 C.R.S. to 24-37.5-112 C.R.S., was enacted during the 2008 Legislative Session, consolidating the IT operations for most of the Executive Branch. However, the Department, along with Department of Law, Department of the Treasury, State-supported institutions of higher education, and the Judicial and Legislative branches remained outside of OIT's oversight. In addition to the information presented in CHAPTER 1, the Department's Division of Information Technology is responsible for the IT infrastructure consisting of multiple servers, personal computers, networking equipment, firewall, telephone system, and other IT equipment to support its information systems, data, imaging needs, and Web presence.

A second IT governance structure relates to information security in Colorado state government and is slightly different and more expansive than the structure in place for other types of IT operations previously mentioned. Specifically, the General Assembly enacted the Colorado Cyber Security Program during the 2006 Legislative Session. That legislation was codified in Sections 24-37.5-401 through 406, C.R.S. Most of the law's requirements apply to public agencies that are defined in the law as "every state office, whether executive or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions." Therefore, despite the Department being a non-consolidated entity from an IT perspective, it must comply with the Colorado Cyber Security Program, which is responsible for developing and promulgating the State's primary information security policies.

During our audit work, we identified certain matters that are not included in this audit report that were reported in a separate confidential report dated November 2015.

AGENCY CYBER SECURITY PLAN

The Governor's Office of Information Security oversees the State's information security program and is responsible for developing and promulgating information security policies intended to control the risks associated with access, use, storage, and sharing of sensitive citizen and state information. Additionally, Statute [Sections 24-37.5-401 through 406, C.R.S.] which was signed into law by the Governor on June 6, 2006, requires each public agency or department to develop, document, and implement a plan to provide information security for the data and systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source. Further, non-consolidated agencies, such as the Department, are required to maintain an Agency

Cyber Security Plan (Agency Plan), which at a minimum, must align with the Colorado Information Security Policies (Security Policies), which were last updated in February 2015.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

Our audit work was designed to determine whether the Department was aware of the updates made to the Security Policies in February 2015. We also inquired with Department staff and reviewed the Department's Agency Plan to determine whether the new IT security requirements in the Security Policies have been incorporated into the Department's Agency Plan.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We used the following Colorado Revised Statutes and Colorado Information Security policies to determine whether the Department's Agency Plan was in place, up-to-date, and approved by both the Department and OIT management:

According to Section 24-37.5-404(3), C.R.S., each public agency is required to submit its information security plan to OIT's Chief Information Security Officer (CISO) for approval on or before July 15 of each year. Further, Section 24-37.5-404(4), C.R.S., states that in the event that an Agency Plan is not submitted to the CISO by September 15 of that year, the CISO shall be authorized to temporarily discontinue or suspend the operation of a public agency's communication and information resources until such plan has been submitted to or is approved by the CISO. This requirement is also stated in permanent rule 8 of C.C.R. 1501-5—Rules in Support of the Information Security Act for the Office of Information Technology.

As noted above, the Security Policies state that non-consolidated agencies, such as the Department, are required to maintain an Agency

Plan, which at a minimum, must align with the IT security requirements outlined in the Security Policies.

WHAT PROBLEM DID THE AUDIT WORK IDENTIFY?

We found that as of the end of September 2015, the Department has not updated the Agency Plan to meet the IT security requirements specified in the Security Policies that were released in February 2015 and, therefore, is not compliant with State statutes requiring the Agency Plan to be submitted to and approved by the CISO by no later than September 15, 2015. Department staff stated, and we confirmed, that discussions were held with the CISO in July 2015 to change the Agency Plan preparation and submission process, which would cause the Department to miss the July 15 statutory deadline. However, since then, the Department has not provided additional documentation of any further communications between the Department and the CISO regarding this matter to ensure the Department would meet the September 15 statutory deadline.

WHY DID THE PROBLEM OCCUR?

According to Department staff, management intends to create a more robust Agency Plan that goes above and beyond the IT security framework outlined in the Security Policies. However, the Department has not been able to complete this task yet based on other competing priorities.

WHY DOES THIS PROBLEM MATTER?

The security and availability of the SCORE system is essential to comply with Section 1-2-302(1), C.R.S., that requires SCORE to maintain a master list of registered electors of the entire state. During elections, the availability of the SCORE system is essential to perform integral election functions and store registration and election data. Without an approved information security plan that incorporates information security policies, standards, and guidelines, the

Department may not be adequately securing the SCORE system or achieving management objectives and expectations in mitigating security risks within the system. This, ultimately, could leave the system vulnerable and lead to unauthorized exposure, modification, or availability of the data within the system. In addition, the State's CISO could discontinue or suspend the operation of the Department's communication and information resources, due to non-compliance with the State's information security policy on submitting and obtaining Agency Plan approval. This would likely have a significant negative impact on the availability of the SCORE system and the daily operations of Department staff and county users.

RECOMMENDATION 3

The Department of State should ensure that IT security requirements in the Colorado Information Security Policies have been incorporated into the Department's Agency Cyber Security Plan (Agency Plan) by:

A Updating and submitting its Agency Plan to the State's Chief Information Security Officer for approval as soon as possible for the current annual cycle.

B Ensuring that the Agency Plan update and submission process continues to meet future, required annual deadlines.

RESPONSE

DEPARTMENT OF STATE

A AGREE. IMPLEMENTATION DATE: NOVEMBER 2015.

With the CISO's approval and encouragement, the Department is reworking its Agency Cyber Security Plan, including its Risk-Based Gap Analysis and Plan of Actions and Milestones, to create an improved set of measures of its information security program. The revised approach provides detailed information about the Department's security posture and activities under the security policies adopted by the CISO, the SANS Critical Controls, and the NIST Special Publication 800-53 Revision 4 framework. The Department will submit its 2015 Agency Cyber Security Plan for approval to the CISO by November 30, 2015.

The Department has regular contact with the CISO and staff of the state's Office of Information Security on issues regarding its security plan and actions. The Department believes that the agency continues to meet or exceed the operational and policy standards from its 2014 Agency Plan (e.g., weekly vulnerability scans, change management procedures, Payment Card Industry assessments and

third-party scans, third-party white hat penetration attempts). The Department's revised Agency Plan will bring even more maturity and visibility to the effectiveness and impact of the agency's security program.

B AGREE. IMPLEMENTATION DATE: MONTH JULY 2016.

The Department will prepare and submit future Agency Plans, as it has prior to 2015, in accordance with the statutory deadlines.

SERVICE LEVEL AGREEMENTS

A service-level agreement (SLA) is a documented list of roles and responsibilities assigned to the stakeholders involved in performing a particular function. For example, an SLA between an IT service provider and the customer will list the IT service provider's responsibilities, such as maintaining the IT system, performing backups according to a customer-established timeline, and responding to customer problems with the system. The SLA will also describe the customer's decision-making authority to create the system and all business requirements for the system, as well as the customer's responsibilities. These responsibilities could include collecting, classifying, and processing information in the system; approving user access or restrictions; establishing timelines for backups and disaster recovery; and disseminating or disposing of the information housed in the system.

A well-defined and well-executed SLA allows for better risk management, improved quality and performance of business services, demonstration of IT value, improved IT and business accountability, and IT priorities that align with improved business outcomes. The key to achieving these benefits is establishing realistic and measurable service-level agreements that support business and customer needs at acceptable costs.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

Our audit work was designed to determine whether IT controls related to the security of the two data centers were in place, properly designed, and operating effectively. Since both data centers are under OIT's management, we asked Department management and staff to determine whether SLAs were in place between the Department (the

customer) and OIT (the vendor) and to determine if IT controls around physical security, network security, environmental security, and backup and recovery have been addressed.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We used the following best practices, as well as Department and Colorado Information Security policies to determine whether an SLA was in place with OIT and covered the various aspects of data center security noted above.

We reviewed industry best practices, as specified by the Information Systems Audit and Control Association (ISACA), to determine specific criteria in this area. The Control Objectives for Information and Related Technologies (COBIT), version five of ISACA's globally accepted IT governance framework states that a formal contract agreement, such as an SLA, enables customer and vendor accountabilities and expectations to be clearly understood and helps define minimum performance targets for a deliverable and how they will be measured and reported.

The Department's Agency Cyber Security Plan (Agency Plan) outlines various vendor management activities, including IT service agreements and management and oversight of vendors. Agency Plan-Section 5 states that the Department "must establish and maintain a Cyber Security Vendor Management Program that is to provide guidance…for documenting terms of service delivery to include: confidentiality and non-disclosure agreements, security controls, and measuring and reporting." Additionally, the Agency Plan also requires the Department's Chief Information Officer to "complete periodic IT vendor performance reviews." These vendor management requirements also align with Colorado Information Security Policy, CISP-005 Section 7.3.

WHAT PROBLEM DID THE AUDIT WORK IDENTIFY?

We found that the Department does not have an SLA in place with OIT over the management of the two data centers where the Department's various IT systems, servers, and other computing infrastructure are housed, including the SCORE system. In addition, we could not determine how the Department was ensuring that the data center services managed by OIT were meeting service support requirements and its own vendor management policy. Further, we found that the Department is not performing periodic vendor reviews of OITs services.

WHY DID THE PROBLEM OCCUR?

Although Department staff stated that they have had informal communications with OIT, the Department has not worked with OIT to define customer (the Department) and vendor (OIT) accountabilities and expectations or to clarify the critical IT services that should be in place at the two data centers through a SLA. In addition, due to the lack of an SLA, the Department has not established quantitative and qualitative metrics for measuring the service provided by OIT. Finally, the Department has not established a process to perform periodic vendor reviews of OIT to ensure compliance with formalized agreements and its own vendor management policy.

WHY DOES THIS PROBLEM MATTER?

Without a formal agreement, or SLA, specifying data center services that OIT provides to its customers, the Department may not be able to gain appropriate levels of assurance over critical business requirements, such as the security and performance of its key business applications and IT systems, including SCORE. Specifically, the availability of the SCORE system, especially during elections, is a critical business requirement for the Department, and the system

should perform at optimum levels under periods of more frequent system usage. Further, the Department is non-compliant with its own policy of documenting formal agreements, such as an SLA, with service providers, as well as performing periodic vendor reviews.

RECOMMENDATION 4

The Department of the State (Department) should improve IT controls related to the operations and security of the two data centers it uses by:

A Working with the Governor's Office of Information Technology (OIT) to formalize an agreement regarding the service responsibilities and expectations over the management of the data centers that host the Department's critical IT systems, including SCORE.

B Developing and documenting performance metrics by which to measure the services provided by OIT to ensure compliance with the formalized agreement.

C Performing and documenting periodic reviews of OIT to ensure compliance with formalized agreements and to comply with the Department's vendor management policy.

RESPONSE

DEPARTMENT OF STATE

AGREE. IMPLEMENTATION DATE: APRIL 2016 *(ASSUMING APPROPRIATE OIT PRIORITIZATION OF DEVELOPING AN AGREEMENT)*.

A The Department currently has an ongoing working relationship with the Governor's Office of Information Technology (OIT), which includes regular monitoring of data centers and working to resolve any anomalies identified. The Department, though, agrees that service responsibilities and commitments of the OIT should be documented in a formal agreement with its agency customers. The Department will work with OIT to develop an agreement, and

intends to have it in place before the 2016 Election cycle peak election activities commence in April 2016.

B AGREE. IMPLEMENTATION DATE: APRIL 2016 *(ASSUMING APPROPRIATE OIT PRIORITIZATION OF DEVELOPING AN AGREEMENT)*.

The Department will ensure that the agreement includes performance metrics to measure OIT's services and performance under the terms of the agreement.

C AGREE. IMPLEMENTATION DATE: APRIL 2016 *(ASSUMING APPROPRIATE OIT PRIORITIZATION OF DEVELOPING AN AGREEMENT)*.

The Department will conduct periodic performance reviews to ensure both parties to the agreement are performing according to the terms of the agreement and in compliance with its vendor management policy.

APPENDIX A

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

SUMMARY OF FINDINGS RELATED TO
THE SMART GOVERNMENT ACT
DEPARTMENT OF STATE
NOVEMBER, 2015

The SMART Government Act [Section 2-7-204(5), C.R.S.] requires the State Auditor to annually conduct performance audits of one or more specific programs or services in at least two departments. These audits may include, but are not limited to, the review of:

- The integrity of the department's performance measures audited.
- The accuracy and validity of the department's reported results.
- The overall cost and effectiveness of the audited programs or services in achieving legislative intent and the department's goals.

During our performance audit of the Department of State (Department), we performed testwork related to the integrity and reliability of performance measurement for the Department of State's Business Intelligence Center (Center). Specifically, we performed procedures to determine whether the Department's oversight of the Center was effective to ensure the Center maintained accountability and transparency, and established formal program policies.

This document outlines our findings related to that testwork. We have presented our findings as responses to three key questions that can assist legislators and the general public in assessing the value received for the public funds spent by the Business Intelligence Center.

What is the purpose of the program, and how much does it cost?

According to the Department, the mission of the Business Intelligence Center is to "promote economic growth and good governance by making business-relevant data accessible and useable for informed decision-making and to create and nurture a vibrant environment where Colorado business challenges are addressed." The Department has not established written performance measures related to this function, but management reported that its goals are to increase the amount of useful data published, increase participation in the Go Code Colorado challenge events, and increase corporate partnership. In Fiscal Year 2015, the Department was appropriated $1.5 million to operate the program.

What key improvements did the audit recommend related to the Department's measurement and reporting of the Business Intelligence Center's performance?

The Department can improve structure, transparency, and accountability of the Business Intelligence Center's financial information.

What other key improvements did the audit recommend related to the effectiveness of the Business Intelligence Center in achieving its purpose?

We found that in RECOMMENDATION 2 the Department should define the objectives of the Center to help ensure that its legislative intent is achieved; create formal roles for the Department management, the Executive Committee, and the Advisory Board; and develop formal policies and procedures for operations.

GLOSSARY

STATE · OF · COLORADO
UNION AND CONSTITUTION
NIL SINE NUMINE
1876

ABBREVIATIONS

Agency Plan
: Department of State's Agency Cyber Security Plan.

AICPA
: American Institute of Certified Public Accountants.

Center
: Business Intelligence Center.

Challenge
: Go Code Colorado Challenge.

CISO
: Chief Information Security Officer.

COBIT
: Control Objectives for Information and Related Technologies.

COFRS
: Colorado Financial Reporting System.

CORE
: Colorado Operations Resource Engine.

COSO
: Committee of Sponsoring Organizations.

C.R.S.
: Colorado Revised Statute.

DCV
: Denver Civic Ventures.

Department
: Department of State.

GFOA
: Government Finance Officers Association.

HAVA
: Help America Vote Act.

ISACA
: Information Systems Audit Control Association.

JBC
: Joint Budget Committee.

OIT
: Governor's Office of Information Technology.

SCORE
: State of Colorado Registration and Election system.

Secretary
: Secretary of State.

SLA
: Service-level Agreement.

SMART
: State Measurement for Accountable, Responsive, and Transparent Government Act.

UCC
: Uniform Commercial Code.