Application for the
National Legislative Program Evaluation Society
2013 Excellence in Evaluation Award

We Set the Standard for Good Government

Office of the State Auditor

Dianne E. Ray, CPA
State Auditor

May 10, 2013

Ms. Lisa Kieffer
Georgia Department of Audits and Accounts
270 Washing Street, SW
Room 1-156
Atlanta, GA 30334-8400

Mr. Joel Alter
Office of the Legislative Auditor
658 Cedar Street, 1st Floor South
St. Paul, MN 55155

Mr. Angus Maciver
Office of the Legislative Auditor
Performance Audits
P.O. Box 201705
Helena, MT 59620-1705

Dear Members of the 2013 NLPES Awards Committee:

On behalf of the Colorado Office of the State Auditor, I am pleased to submit this application for the 2013 NLPES Excellence in Evaluation Award. We appreciate this opportunity to highlight the superb work and accomplishments of our performance audit staff over the past four years. We look forward to receiving the results of your review. Thank you for your time and consideration.

Sincerely,

Dianne E. Ray, CPA
State Auditor

Colorado Office of the State Auditor
Excellence in Evaluation Award Summary Narrative
Calendar Years 2009-2012

The Office of the State Auditor (OSA) is the accountability arm of the Colorado General Assembly. Our mission is simple—Improve government for the people of Colorado. To ensure that we accomplish our mission, our performance audits identify efficiencies and cost-savings and improve effectiveness and transparency in government. Our performance audits also provide objective information, quality services, and solution-based recommendations.

Every day, our performance audit staff and the work they perform reflect the OSA's tagline: "We set the standard for good government."

Body of Work

Overall, the OSA's body of work consistently demonstrates the value of a thorough, credible, and impartial assessment of the operation of state programs for legislators, agencies, and the public. A recent editorial by *The Denver Post Editorial Board* (see Attachment D) stated:

> "The Office of the State Auditor is not always appreciated as the bulwark to good government that it clearly is. Yet its performance audits routinely uncover questionable practices that might otherwise have gone on for years."

Our group of performance auditors collectively has produced a substantial body of work. Between January 2009 and December 2012, the OSA released a total of 59 performance audits, or an average of approximately 15 audits per year. These performance audits have covered divisions, programs, and operations in all 19 of Colorado's principal executive branch departments, as well as the Governor's Office, the Judicial Branch, and certain political subdivisions and other entities as provided for by law. See Attachment B for a listing of audits broken down by year and by topic.

Our performance audits have ranged from complex, multi-agency audits to audits of single programs. Our performance audits have highlighted the importance of governance and accountability, helped to protect the public, ensured the delivery of quality services, and covered matters of importance to state government administration. Some performance audits involved the use of contractors, due to the specialized expertise required to perform the audit work. These audits allowed us to examine technically complex programs that are important for the State, its employees, and its citizens. Even when contractors are involved, the OSA's audit managers and audit supervisors hold significant responsibility for planning the audit work, developing audit findings and recommendations, and writing the audit report.

One notable change in the OSA's staffing over the last 4 years is the growth in experience and tenure of our performance audit staff. We have reaped the benefits as our performance audit staff have moved away from entry-level auditors toward highly functioning senior auditors and audit supervisors. Not including senior management positions, the OSA has maintained an average of about 25 professional staff assigned to conduct performance audits (see Attachment A).

Our performance audits originate from a number of different sources. Of the 59 performance audits released during Calendar Years 2009 through 2012, 28 audits (47 percent) were discretionary, 19 audits (32 percent) were conducted in response to a legislative request for audit, and the remaining 12 audits (20 percent) were statutorily required. The fact that over half of the OSA's audits were driven by legislative mandates or by legislative requests demonstrates the value legislative members place on our work as well as our commitment to remaining responsive to the needs of the General Assembly. Moreover, the General Assembly has passed bills that expand our

audit responsibilities. For example, during the 2011 Legislative Session, the General Assembly expanded the State Auditor's authority to conduct information security audits as well as performance audits of public highway authorities and special purpose authorities. The General Assembly also turned to our office to provide audit coverage and ensure agency implementation of the State Measurement for Accountable, Responsive, and Transparent (SMART) Government Act, which established a performance-based budgeting system for all of Colorado's 19 principal executive branch departments, the Judicial Department, and four independent offices.

As part of this application, we have included three performance audits completed during the 4-year period under review that demonstrate the variety of performance audits we conduct, the quality of our audit work, and the scope of impact our audits have on government operations. Please see Attachment C for a copy of each selected audit report.

- *Conservation Easement Tax Credit Performance Audit* (September 2012). This performance audit is an example of how our work can be a catalyst that brings together various state agencies and stakeholders to bring about significant positive change for the effective and efficient administration of government programs. A key message we emphasized throughout the audit report is that having strong processes for administering the tax credit is important for accomplishing land conservation goals while ensuring that the State is not foregoing more revenue than it should. As of 2009, nearly $640 million in tax credits had been claimed by Colorado taxpayers. Our audit recommendations provided the state agencies responsible for administering the tax credit program with a detailed roadmap for how to strengthen their processes and ensure that tax credits being claimed and used by taxpayers are valid.

  Additionally, in December 2012, shortly after the initial audit hearing, the Legislative Audit Committee requested that draft legislation be prepared to address a key finding in the audit report: The State should fundamentally shift the manner in which the conservation easement tax credit is administered by requiring that certain aspects of a conservation easement donation be reviewed and approved *before* a tax credit claim can be filed. The OSA convened a working group representing state agencies responsible for administering the tax credit and stakeholders. As a result of the working group's efforts, the Legislative Audit Committee voted unanimously to sponsor legislation. Senate Bill 13-221 was introduced on March 15, 2013, and, at the time of this application, had passed both the House and Senate and was awaiting the Governor's signature. Through this collaborative effort, the state agencies and stakeholders were able to accomplish the goals as outlined in the OSA's performance audit and, therefore, successfully balance land preservation and conservation goals and landowner interests while protecting the broader interests of Colorado taxpayers.

- *Unemployment Insurance Program Performance Audit* (October 2011). This performance audit is an example of how we used LEAN principles to augment the comprehensiveness and thoroughness of our work auditing core government programs. First developed in the private sector and now being adapted to the public sphere, LEAN principles promote continuous and rapid operational improvement by eliminating non-value-added processes and ensuring that value-added processes occur in the right sequence without creating bottlenecks. An overarching theme of this audit was that an efficient and effective UI Program is critical for providing much-needed benefits to qualified recipients in a timely manner while minimizing the financial burden on those businesses whose premiums fund

the UI Program. We successfully used LEAN principles and methodologies to demonstrate that the UI Program had missed significant opportunities to improve the efficiency and effectiveness of its operations. Since 2006, the UI Program's workload had almost tripled without a corresponding increase in staff. As a result, claimants often waited more than an hour, if not longer, when they contacted the UI Program's call center. By mapping each step in the unemployment insurance claims process, we identified non-value-added processes and forms that the UI Program could eliminate, as well as computer enhancements it could implement, to collect claims information more cost-effectively and serve claimants more efficiently. We estimated that 16 percent of the UI Program's non-management staff could be reallocated to more cost-effective functions if the UI Program reduced the use of paper forms, required most claimants to apply online, further automated claims processing, and pursued statutory changes to simplify eligibility determination.

In addition to focusing on increased efficiencies, we were also concerned with significant overpayments of UI benefits in Calendar Year 2010. We used a statistically valid sample to estimate that the UI Program paid $60 million in benefits to claimants who did not prove they were legally present in the United States, a requirement in state law. By strengthening a couple of key steps in the eligibility determination process, we concluded that the State could avoid making such improper payments in the future and, therefore, save costs to the Unemployment Insurance Trust Fund.

- *Office of Cyber Security Performance Audit* (November 2010). This award-winning performance audit is an example of the OSA's successful efforts over the past several years to build in-house expertise for conducting performance audits of electronic information systems and related critical infrastructure. This audit attempted to answer one basic overarching question: Are citizen data maintained by the State secure? To answer this question, we reviewed the Office of Cyber Security's progress in fulfilling the statutory requirements of the Colorado Cyber Security Program, which applies to every state department, division, office, commission, bureau, board, and institution in the Executive, Judicial, and Legislative Branches.

  In addition to assessing cyber security plans and response protocols, we tested physical security of key state buildings and conducted covert penetration tests of state networks, applications, and information systems. By simulating real cyber attacks against state networks and information systems, the audit team identified a significant number of serious vulnerabilities in the State's IT networks and applications and gained unauthorized access to thousands of individuals' records, including state employees' records, containing confidential data. The public audit report is included with this application; however, the OSA also issued a confidential report to the Office of Cyber Security and the agencies whose systems had been breached so they could immediately begin remedying the vulnerabilities identified during the audit. Since the audit's public release in December 2010, we have received a number of requests from local, state, and national organizations to discuss the audit and train other audit organizations on the methodologies used to execute the penetration test.

Making An Impact

The OSA's performance audits have a significant impact and benefit for all Coloradans by promoting transparency and accountability in state government; improving the efficiency,

effectiveness, and quality of operations and service delivery; identifying cost savings and other financial benefits; and producing legislative change.

The impact of each individual performance audit is unique. Some audits receive substantial media attention and public focus that precipitates quick and often sweeping legislative changes. Other audits receive less public attention, yet the audited agency takes the audit seriously and works diligently to implement the recommendations and improve operations. Overall, the OSA focuses on several key strategies to ensure that our performance audits have an impact:

- **Identify Financial Benefits for the State.** We recognize that legislators and taxpayers look to the OSA to identify cost savings and other financial benefits in state programs and operations, especially during times of ongoing economic challenges. It is also symbolically important for us that these financial benefits exceed the OSA's net operating costs. During Fiscal Years 2009 through 2012, our performance audits identified financial benefits (e.g., cost savings, improved collection of fees or debts owed, general fund cost recoveries, or increases in the value of assets in the State's accounting system) totaling $140.2 million. This represents about a 5:1 ratio when compared with the OSA's total net operating costs over the same 4-year period.

- **Identify the Need for Statutory Change**. As a legislative agency, it is important that our audits identify when statutory change is necessary to improve program effectiveness and efficiency and provide quality information to the General Assembly about available policy options. During the 2009 through 2012 Legislative Sessions, a total of 22 separate bills were enacted that related to audit recommendations made by the OSA. See Attachment E for a complete listing of audit-related legislation.

- **Identify Value-Added, Actionable Recommendations.** We strive to promote positive change in government by developing recommendations and solutions that will address the problems we identify and that agencies can realistically implement. Agency agreement with our audit recommendations is the necessary first step toward achieving meaningful change. The OSA made a total of 1,031 performance audit recommendations during Calendar Years 2009 through 2012, and agencies agreed or partially agreed with 99 percent of these recommendations. See Attachment F for a count of responses by agency.

- **Hold Agencies Accountable for Implementation.** We strive to promote positive change in government by holding agencies accountable for implementing the recommendations they agree to implement. In early 2010, we determined that one approach to achieving this goal was to provide more information to legislators and the general public via a centralized tracking and reporting effort. We now annually report to the Legislative Audit Committee, the Joint Budget Committee, and all 13 committees of reference that provide oversight of state agencies on the implementation status of all performance audit recommendations—providing specific focus on those recommendations that are not yet fully implemented.

  As shown by the table in Attachment F, of the 1,031 performance audit recommendations the OSA made during Calendar Years 2009 through 2012, a total of 900 recommendations (78 percent) were reported to have been fully or partially implemented as of June 30, 2012. Moreover, we note that only 24 of the 197 (12 percent) audit recommendations reported as not implemented were from audits prior to 2012. The majority of unimplemented

recommendations were from recent audits released in Calendar Year 2012, and reflect recommendations that we would not expect to be fully implemented at this time.

The increased visibility created by the OSA's new reporting effort has provided a strong motivation for state agencies to implement their recommendations and thus improve Colorado state government. For example, the Joint Budget Committee required that all state agencies respond during their Fiscal Year 2014 budget briefings as to why they had not implemented some of the older performance audit recommendations and provide a schedule for when the recommendations would be implemented. The legislative committees of reference also questioned agencies asking for explanation about the outstanding audit recommendations. We believe that the positive response and action taken by legislative committees demonstrates the success of this ongoing project. We have also seen the positive impact that it has had on state agencies' efforts to better track and manage the implementation process.

Furthering the Profession

The OSA and its staff advance the profession of legislative program evaluation and performance auditing through active involvement and leadership in professional associations and the broader accountability community, including the National Legislative Program Evaluation Society (NLPES), National Conference of State Legislatures (NCSL), Institute of Internal Auditors, Mountain & Plains Intergovernmental Audit Forum, National State Auditors Association, Information Systems Audit and Control Association, and Association of Government Accountants.

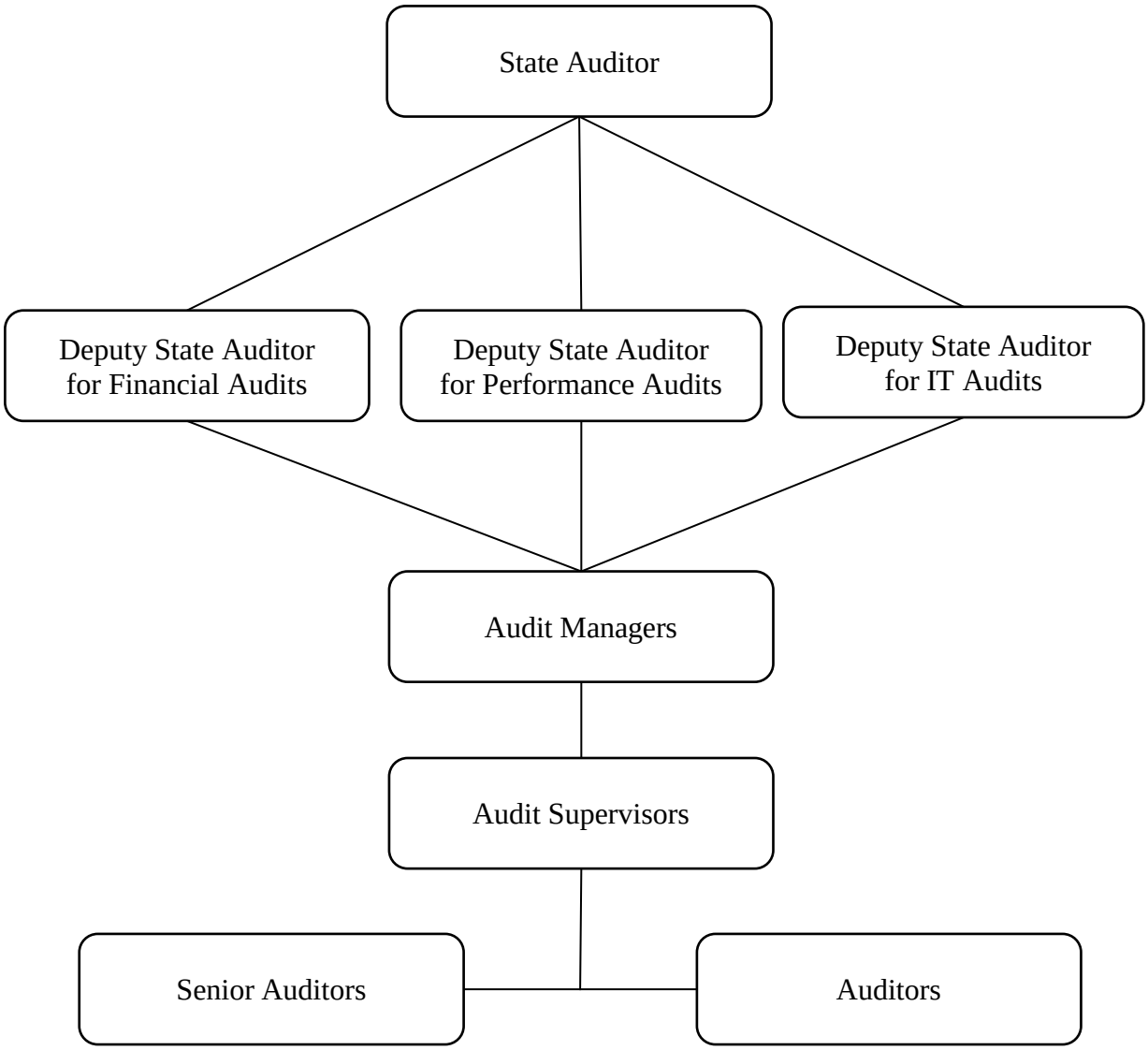
In particular, the OSA demonstrates a clear commitment to NLPES and its mission. We are pleased to have had a performance audit manager serving on the NLPES Executive Committee since 2009. His ongoing participation and leadership on the Executive Committee helps keep the OSA connected to our peer organizations and working to address the collective demands and issues we face as legislative audit and evaluation organizations.

The OSA's involvement in NLPES, NCSL, and other audit-related conferences provides important opportunities for exchanging ideas and developing skills. See Attachment G for a listing of the various external presentations provided by OSA staff. In September 2011, the OSA was pleased to host and help organize the NLPES 2011 Fall Professional Development Seminar in Denver. The seminar was well attended—drawing participation from about 100 performance auditors and program evaluators from 24 different states—and covered a wide range of topics. We were privileged to have our Communication Analyst provide a plenary session to all seminar participants on using messaging techniques to write more effective audit reports. The plenary session received high scores on participant evaluations.

In addition to conference participation, our staff have contributed articles to the NLPES Newsletter and routinely responded to inquiries posted on the NLPES email list and the Question of the Month forum. Finally, the OSA provided meeting space and support for the NLPES Executive Committee's meetings in September 2009, May 2010, and May 2011. This allowed NLPES to avoid the cost of meeting space and, because the meetings were in Denver, travel costs for the NLPES Staff Liaison. Keeping administrative costs low is important for ensuring that NLPES can allocate more of its financial resources for training and professional development activities for the membership.

ATTACHMENT A

Colorado Office of the State Auditor
Organizational Chart
Calendar Years 2009-2012



Note: Effective June 1, 2011, a third Deputy State Auditor position was added to oversee the OSA's IT audits and some performance audits.

Colorado Office of the State Auditor Total Performance Audit FTE by Position				
Position	**Calendar Year**			
	2009	**2010**	**2011**	**2012**
Audit Manager	5	7	5	5
Audit Supervisor/Independent Contributor	3	9	11	13
Senior Auditor	9	5	4	3
Auditor	8	3	5	3
Total Performance Audit FTE	**25**	**24**	**25**	**24**
Note: Counts are as of December 31 and do not include the Deputy State Auditors or the State Auditor.				

Colorado Office of the State Auditor Total Expenditures by Fiscal Year	
Fiscal Year	**Total Expenditures**[1]
2009	$8,042,056
2010	$7,230,618
2011	$7,721,769
2012	$7,809,210

Source: Colorado Financial Reporting System.
[1]Includes all aspects of operations, including in-house performance and financial audits, contract audits, and the Local Government Audit Division.

ATTACHMENT B

Colorado Office of the State Auditor
Performance Audits by Year
Calendar Years 2009-2012

Calendar Year 2012 Performance Audits

Amendment 35 Tobacco Tax Funded Grant Programs, Report #2166 (August 2012)
Automobile Inspection and Readjustment Program, Report #2169 (December 2012)
Board of Assessment Appeals, Report #2141 (January 2012)
Conservation Easement Tax Credit, Report #2171 (October 2012)
Consolidation of the Executive Branch Information Technology, Report #2151 (March 2012)
Evaluation of State Capital Asset Management and Lease Administration Practices, Report #2175 (December 2012)
Implementation of the College Opportunity Fund, Report #2162 (July 2012)
Implementation of the State Measurement for Accountable, Responsive and Transparent (SMART) Government Act, Report #2168 (August 2012)
Medicaid Eligibility Status for Adult Civil Patients, Report #2131B (June 2012)
Medicaid Hospital Provider Fee Program, Report #2177 (October 2012)
Office of Administrative Courts, Report #2176 (October 2012)
Public Utilities Commission, Report #2174 (June 2012)
Statewide Internet Portal Authority, Report #2178 (December 2012)
Tobacco Tax and Tobacco Settlement Revenue Collections and Distributions, Report #2183 (June 2012)
Wildlife Cash Fund, Report #2190 (June 2012)

Calendar Year 2011 Performance Audits

Administrative Leave Use in the State Personnel System, Report #2123 (March 2011)
Bus Cost Allocation Model, Regional Transportation District, Report #2057 (February 2011)
Colorado State Veterans Nursing Homes, Report #2158 (September 2011)
Division of Gaming, Report #2149 (November 2011)
Division of Youth Corrections, Report #2136 (December 2011)
Employment Verification and Public Contracts for Services Laws, Report #2129 (November 2011)
Implementation of the Medicaid Pediatric Hospice Waiver Program, Report #2134 (June 2011)
Motorcycle Operator Safety Training Program, Report #2142 (September 2011)
Oversight of Guardianships and Conservatorships, Report #2132 (September 2011)
****Recipient of the National Legislative Program Evaluation Society 2012 Impact Award***
Psychiatric Medication Practices for Adult Civil Patients, Report #2131A (June 2011)
Sustainability of the Colorado Financial Reporting System, Report #2152 (July 2011)
Tax Processing, Report #2157 (September 2011)
Treasury Investment Program, Report #2146 (July 2011)
Unemployment Insurance Program, Report #2140 (November 2011)

Calendar Year 2010 Performance Audits

Anhydrous Ammonia Tank Inspection Program, Report #2058 (August 2010)
CollegeInvest College Savings Plans, Report #2056 (November 2010)
Colorado Low-Income Telephone Assistance Program, Report #2055 (June 2010)
Concealed Handgun Permit Database, Report #2104 (December 2010)
Dental Loan Repayment Program, Report #2077 (July 2010)
Employee Benefits Program, Report #2073 (November 2010)
Executive Compensation Practices, Regional Transportation District, Report #2048 (March 2010)
Higher Education Student Fees, Report #2046 (August 2010)
Medicaid Outpatient Substance Abuse Treatment Benefit, Report #2079 (December 2010)
Office of Cyber Security, Report #2068A (December 2010)
****Recipient of the National State Auditors Association 2011 Excellence in Accountability Award***
****Recipient of the National Legislative Program Evaluation Society 2011 Impact Award***

Office of Risk Management, Report #2061 (September 2010)
Pinnacol Assurance, Workers' Compensation Insurance Fund, Report #2042 (June 2010)
Section 1512 Reporting, American Recovery and Reinvestment Act of 2009, Report #2053 (June 2010)
Unemployment Insurance Trust Fund, Report #1993 (July 2010)
Vehicle Emissions Program, Report #2062 (September 2010)
Weatherization Assistance Program, Report #2070 (November 2010)

Calendar Year 2009 Performance Audits

Access to Medicaid Home and Community-Based Long-Term Care Services, Report #1914 (February 2009)
Annual Compensation Survey, Report #1984 (June 2009)
Automobile Inspection and Readjustment (AIR) Program, Report #1989 (September 2009)
CollegeInvest Scholarship and Loan Forgiveness Programs, Report #2011 (September 2009)
Colorado Mental Health Institute at Pueblo, Report #1986 (December 2009)
Colorado Tourism Office, Report #1974 (June 2009)
Controls Over Medicaid Claims for Durable Medical Equipment, Report #1990 (November 2009)
Controls Over Payments, Medicaid Community-Based Services-Developmental Disabilities, Report #1832 (July 2009)
Department of Personnel & Administration and State Personnel Board, Report #1983 (July 2009)
Division of Aeronautics, Report #1907 (February 2009)
Division of Wildlife, Land Acquisition and Management, Report #1990 (August 2009)
Implementation of Senate Bill 06-090, Report #1985 (June 2009)
Problem Drivers and Traffic Fatalities, Report #1992 (November 2009)
Workforce Investment Act, American Recovery and Reinvestment Act of 2009, Report #2052 (December 2009)

Electronic copies of all audit reports conducted by the Colorado Office of the State Auditor can be found by clicking on the "OSA Audit Reports" link on our webpage:

http://www.leg.state.co.us/OSA/coauditor1.nsf/Home?openform.

Note: Dates listed in parentheses signify when the report was released by the Legislative Audit Committee and does not necessarily match the date listed on the report cover.

Colorado Office of the State Auditor
Performance Audits by Topic
Calendar Years 2009-2012

Public Safety/Regulatory Programs

Anhydrous Ammonia Tank Inspections
[+]Concealed Handgun Permit Database
Division of Aeronautics
Division of Gaming
Division of Youth Corrections
[*]Implementation of Senate Bill 06-090
[*]Motorcycle Operator Safety Training Program
Oversight of Guardians and Conservatorships
[*]Problem Drivers and Traffic Fatalities
[*]Public Utilities Commission

Public Assistance/Public Health Programs

[*]Access to Medicaid Home and Community-Based Long-Term Care Services
[*]Amendment 35 Tobacco Tax Funded Grant Programs
Colorado Low-Income Telephone Assistance Program
[*]Colorado Mental Health Institute at Pueblo
Colorado State Veterans Nursing Homes
Controls Over Medicaid Claims for Durable Medical Equipment
Controls Over Payments for Medicaid Community-Based Developmental Disability Services
[*]Implementation of the Medicaid Pediatric Hospice Waiver Program
[*]Medicaid Eligibility Status for Adult Civil Patients
[+]Medicaid Hospital Provider Fee Program
[+]Medicaid Outpatient Substance Abuse Treatment Benefit
[*]Psychiatric Medication Practices for Adult Civil Patients

Environment/State Lands

[+]Automobile Inspection and Readjustment Program
Division of Wildlife Land Acquisition and Management
[*]Wildlife Cash Fund
Vehicle Emissions Program

American Recovery and Reinvestment Act

Section 1512 Reporting
Weatherization Assistance Program
Workforce Investment Act

KEY
[*] Denotes a legislative request for audit.
[+] Denotes a statutorily required audit.

Higher Education

CollegeInvest College Savings Plans
CollegeInvest Scholarship and Loan Forgiveness Programs
[+]Dental Loan Repayment Program
[*]Higher Education Student Fees
Implementation of the College Opportunity Fund

Workforce/Economic Development/Taxation

Board of Assessment Appeals
[+]Colorado Tourism Office
[*]Conservation Easement Tax Credit
[*]Employment Verification and Public Contracts for Services Laws
Tax Processing
[*]Tobacco Tax and Tobacco Settlement Revenue Collections and Distributions
Unemployment Insurance Program
Unemployment Insurance Trust Fund

Information Technology & Systems

Consolidation of the Executive Branch Information Technology
Office of Cyber Security
Sustainability of the Colorado Financial Reporting System

State Government Administration & Employees

[*]Administrative Leave Use in the State Personnel System
[+]Annual Compensation Survey
[+]Department of Personnel & Administration and State Personnel Board
Employee Benefits Program
Evaluation of State Capitol Asset Management and Lease Administration Practices
[+]Implementation of the State Measurement for Accountable, Responsive and Transparent (SMART) Government Act
[+]Office of Administrative Courts
[+]Office of Risk Management
Treasury Investment Program

Political Subdivisions

[*]Regional Transportation District Bus Cost Allocation Model
[*]Regional Transportation District Executive Compensation Practices
[+]Pinnacol Assurance Workers' Compensation Insurance Fund
Statewide Internet Portal Authority

ATTACHMENT C

Conservation Easement Tax Credit
Department of Revenue
Division of Real Estate

Performance Audit
September 2012

OFFICE OF THE
STATE AUDITOR

LEGISLATIVE AUDIT COMMITTEE
2012 MEMBERS

Representative Cindy Acree
Chair

Representative Angela Williams
Vice-Chair

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

OFFICE OF THE STATE AUDITOR

Dianne E. Ray
State Auditor

Monica Bowers
Deputy State Auditor

Greg Fugate
Legislative Audit Manager

Christopher Harless
Anne Jordan
Andrew Knauer
Heidi Schaefer
Legislative Auditors

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

Office of the State Auditor

Dianne E. Ray, CPA
State Auditor

September 21, 2012

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of Colorado's conservation easement tax credit. The 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 Revenue, the Division of Real Estate, and the Conservation Easement Oversight Commission.

Legislative Services Building • 200 East 14th Avenue • Denver, Colorado 80203-2211
Ph. 303.869.2800 • Fax: 303.869.3060

This page intentionally left blank.

TABLE OF CONTENTS

Glossary of Abbreviations

BOREA – Board of Real Estate Appraisers

CEOC – Conservation Easement Oversight Commission

COMaP – Colorado Ownership, Management, and Protection project

DOR – Department of Revenue

DRE – Division of Real Estate

FMV – fair market value

GOCO – Great Outdoors Colorado

IRS – U.S. Internal Revenue Service

OIT – Governor's Office of Information Technology

TABOR – Taxpayer's Bill of Rights

TPS – Taxpayer Service Division

USPAP – Uniform Standards of Professional Appraisal Practice

CONSERVATION EASEMENT TAX CREDIT
Performance Audit, September 2012
Report Highlights

Dianne E. Ray, CPA
State Auditor

Department of Revenue
Division of Real Estate

PURPOSE
To determine whether there are effective internal controls in place at the Department of Revenue (DOR) and the Division of Real Estate (DRE) to ensure that conservation easement tax credits being claimed and used by taxpayers are valid.

BACKGROUND
- A conservation easement is an interest in real property with the purpose of promoting land conservation. The restrictions on development and other land uses imposed by a conservation easement are intended to maintain the property in a relatively undeveloped state.
- Taxpayers may claim a state income tax credit for all or part of a conservation easement that is donated to a certified governmental entity or nonprofit organization.
- As of 2009, nearly $640 million in tax credits had been claimed for about 3,200 conservation easements. In return, landowners restricted development rights and other land uses on about 925,000 acres of land.

OUR RECOMMENDATIONS
- DOR should strengthen its conservation easement tax credit claim review process and improve its information management practices.
- DRE should strengthen its processes for reviewing conservation easement appraisals and certifying conservation easement holders.
- DOR, DRE, and the Conservation Easement Oversight Commission (CEOC) should ensure that the CEOC consultation process furthers the State's ability to determine the validity of conservation easement tax credit claims.
- DOR and DRE should evaluate options to better protect the State's investment of public resources in tax-credit-generating conservation easements.
- DOR, DRE, and the CEOC should work together to design a pre-approval process for reviewing and approving conservation easement tax credits.

DOR, DRE, and the CEOC agreed with our recommendations.

AUDIT CONCERN
The State foregoes a significant amount of annual tax revenues to incentivize land conservation. House Bill 08-1353 was intended to try to curb historical abuses of the tax credit and help ensure the validity and proper valuation of tax-credit-generating conservation easements. However, our audit demonstrates that more changes need to be made to strengthen the administration of Colorado's conservation easement tax credit to ensure that tax credits being claimed and used by taxpayers are valid.

KEY FACTS AND FINDINGS
- DOR's process for reviewing conservation easement tax credit claims and uses does not ensure coverage of a key requirement—the easement's conservation purpose—and other relevant risk factors.
- DOR's tax examiners do not sufficiently document their reviews of conservation easement tax credit claims and uses. Review documentation held little information about judgments made and conclusions reached.
- The CEOC consultation process is limited in its ability to help inform and facilitate DOR's decision making to allow or disallow tax credit claims. The CEOC tends to take a substantive compliance approach when reviewing conservation easement transactions that DOR refers for consultation, and the CEOC's deliberations tend to take on a landowner-centered perspective.
- DRE's appraisal review process is not sufficient to ensure that all appraisals of tax-credit-generating conservation easements undergo a desk review or that potential problems with appraisals are identified and referred for further investigation.
- DRE's certification process does not ensure that governmental entities and nonprofit organizations holding tax-credit-generating conservation easements continue to meet the minimum certification requirements.
- The State lacks adequate protections when governmental entities and nonprofit organizations that hold tax-credit-generating conservation easements are no longer certified.
- The State's current approach to administering the conservation easement tax credit creates uncertainty for the taxpayer and does not align review and decision-making responsibilities with those with the most appropriate and relevant expertise.
- Measuring the public cost of the conservation easement tax credit is generally straightforward. However, measuring the benefits the public has received in return is more difficult and limited because of a lack of available data.

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

This page intentionally left blank.

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
1	32	Strengthen the review of conservation easement tax credit claims to ensure coverage of key requirements and consideration of relevant risk factors by (a) including a basic review of the reported conservation purpose as part of a Level 1 review, and developing risk factors or other selection criteria that would require referral of the claim to the CEOC for a more complete assessment of the easement's conservation purpose as part of a Level 2 review; (b) expanding the current list of risk factors to include phased donations and donors with prior disallowed credit claims; and (c) evaluating and updating the list of risk factors on at least an annual basis.	Department of Revenue	Agree	March 2013
2	38	Ensure that the review of conservation easement tax credits claims is consistently applied and that the resulting decisions to allow or disallow claims are appropriate and substantiated by (a) developing and utilizing a standard work program or review tool to guide and document tax examiners' review of conservation easement tax credit claims; (b) developing more complete and detailed written policies and procedures for reviewing conservation easement tax credit claims, including how reviews should be documented; (c) instituting a quality review process whereby a supervisor and/or quality control staff routinely reviews a sample of conservation easement tax credit claim reviews completed by tax examiners. Supervisors and quality control staff performing the reviews should receive training to maintain at least a basic level of competency with the conservation easement tax credit and related issues.	Department of Revenue	Agree	July 2013

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
3	43	Ensure that electronic data and information management systems effectively support the administration of the conservation easement tax credit by (a) utilizing a relational database to manage data at the donation and taxpayer levels in a manner that captures the complexity of the tax credit claims and uses over time; (b) capturing data from Form DR 1305 for all conservation easement tax credit claims in the year in which the claim is made, regardless of when the use of the credit occurs; and (c) instituting appropriate data entry controls to help prevent data inaccuracies, and routine clean-up procedures to help identify and correct any data inaccuracies that do occur.	Department of Revenue	Agree	December 2013
4	50	Improve communication efforts and continue to build a common understanding about the purpose and goals of the consultation process. This should include using the consultation process to hold routine discussions about the general issues and trends being observed with conservation easement transactions associated with tax credit claims.	Department of Revenue	Agree	June 2012 and Ongoing
			Division of Real Estate	Agree	June 2012 and Ongoing
			Conservation Easement Oversight Commission	Agree	June 2012 and Ongoing
5	51	Provide the CEOC with more information, such as areas of concern or specific questions that need to be addressed, when referring individual conservation easement tax credit claims to the CEOC for consultation. DOR should also communicate its final decisions to allow or disallow tax credit claims that are referred for consultation.	Department of Revenue	Agree	December 2012

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
6	52	Revise the CEOC's written orientation manual to better address the CEOC's broader responsibility to the general taxpayer when defining "the public interest." The manual should explicitly recognize that the consultation process should further the State's ability to determine whether the landowner has complied with the statutory and regulatory requirements for claiming the conservation easement tax credit.	Division of Real Estate Conservation Easement Oversight Commission	Agree Agree	March 2013 March 2013
7	61	Ensure that the conservation easement appraisal review process is effective at identifying and referring problematic appraisals for investigation before a tax credit is claimed by (a) performing a desk review of, at a minimum, all conservation easement appraisals for which a tax credit will be claimed; (b) developing standard operating procedures that outline the general parameters of the desk review, including the risk factors warranting a desk review and the required and/or significant attributes that should be examined on every desk review; (c) developing and utilizing a standard review template, or other similar tool, to ensure the consistency and completeness of the desk review and to document the significant judgments made, conclusions reached, and subsequent actions taken; and (d) working with the General Assembly to further clarify in statute the intended purpose and scope of the conservation easement appraisal review requirement.	Division of Real Estate	Agree	a. January 2013 b. January 2013 c. January 2013 d. July 2013
8	66	Strengthen the conservation easement holder certification process by formally establishing "conditional certification" in state rule. This should include specifying the appropriate purpose and use of conditional certification, what evaluation criteria would result in conditional certification versus full certification or denial of certification, and any other administrative requirements that are necessary to implement conditional certification.	Division of Real Estate	Agree	March 2013

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
9	69	Strengthen the certification process to ensure that conservation easement holders continue to meet the certification requirements on an ongoing basis. At a minimum, DRE should periodically conduct an in-depth review of documentation for conservation easements that holders have accepted since their initial certification or most recent certification renewal.	Division of Real Estate	Agree	January 2013 and Ongoing
10	72	Evaluate options for protecting the State's investment of public resources in tax-credit-generating conservation easements when the conservation easement holder is no longer certified. Report back to the Legislative Audit Committee and the House and Senate Finance Committees by July 1, 2013, on viable options and pursue statutory and/or regulatory change, as appropriate. At a minimum, options that should be considered include (a) strengthening DRE's ability to investigate complaints against conservation easement holders that hold tax-credit-generating conservation easements, regardless of whether or not the holder is certified and (b) utilizing assignment clauses in the deeds for tax-credit-generating conservation easements that reserve the State's right to require the transfer of the easement to another certified conservation easement holder when the original holder ceases to exist; is no longer certified; or is unwilling, unable, or unqualified to enforce the terms and provisions of the easement.	Division of Real Estate Department of Revenue	Agree Agree	July 2013 July 2013

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
11	80	Work together to design a pre-approval process for reviewing and approving conservation easement tax credit claims prior to their use. Report to the Legislative Audit Committee and the House and Senate Finance Committees by July 1, 2013, on a proposed pre-approval process, including any statutory and regulatory changes that are necessary for implementation. At a minimum, the proposed pre-approval process should ensure that (a) the State has reasonable assurances that conservation easement tax credits being claimed by taxpayers are valid and comply with all statutory and regulatory requirements, (b) conservation easement tax credit claims are approved or denied separately from and prior to any uses of the tax credit, (c) all essential elements related to conservation easement tax credit claims are reviewed and approved by those with the most appropriate and relevant expertise, and (d) the review and approval of tax credit claims is timely.	Department of Revenue Division of Real Estate Conservation Easement Oversight Commission	Agree Agree Agree	July 2013 July 2013 July 2013
12	92	Help to ensure the State's ability to measure the public benefits of the conservation easement tax credit by: (a) Improving taxpayer forms to capture data in a format that facilitates aggregate analysis and reporting on the specific conservation purposes and land attributes that are being protected by conservation easements, (b) Ensuring that taxpayers donating tax-credit-generating conservation easements submit Form DR 1304, and (c) Eliminating unnecessary or duplicative data collection forms and consolidating public reports when possible.	Department of Revenue	Agree	July 2013

This page intentionally left blank.

Overview of the Conservation Easement Tax Credit

Chapter 1

First established by state statute in 1976 (Section 38-30.5-102, C.R.S.), a conservation easement, also known as a conservation easement in gross, is a freely transferable interest in real property with the purpose of promoting land conservation. Specifically, a conservation easement is a right of the owner of the easement, also known as the conservation easement holder, to restrict the landowner from subdividing and building on the land or using the land in certain ways.

The restrictions imposed by a conservation easement are intended to maintain the property in a relatively undeveloped state, thereby preserving and protecting certain conservation purposes. Conservation easements typically afford the protection of fish, wildlife, and plant habitats, or the preservation of land areas for outdoor recreation, education, open space, or historical importance. As of September 2011, there were more than 4,300 conservation easements in Colorado covering approximately 1.6 million acres, or about 2.4 percent of the state's total land area. The map insert illustrates the location of conservation easements throughout the state.

The specific conservation purposes being protected and any restrictions on the landowner are contained in a legal document, called a deed of conservation easement, that is recorded in the local property records and becomes part of the chain of title for the property.

Conservation easements are generally seen as an attractive alternative to the acquisition of land as "fee title," which is the most complete ownership interest one can have in real property. Some potential advantages of conservation easements include:

- **Flexibility**. The terms of a conservation easement can often be tailored to meet the specific needs of both the landowner and the conservation easement holder while still ensuring the easement's conservation purpose.

- **Private Ownership**. Conservation easements are desirable because protecting and preserving natural habitat, open space, or other conservation purposes can be achieved without requiring the government

to acquire ownership of the land. With a conservation easement, the land is maintained under private ownership, which means that the landowner retains the ability to occupy the land, sell it, or pass it on to heirs. Depending on the terms of the conservation easement, traditional land uses such as livestock grazing or agricultural production may be allowed to continue on the property. The property also remains on the local tax rolls for property tax purposes.

- **Cost**. Conservation easements are less costly than a fee title acquisition because the holder is only paying the landowner for the development rights to the land and for other use restrictions, as opposed to the entire bundle of surface property rights. In general, the value of the development rights are the difference between the full market value of the land if left unencumbered and the full market value of the land with the conservation easement in place.

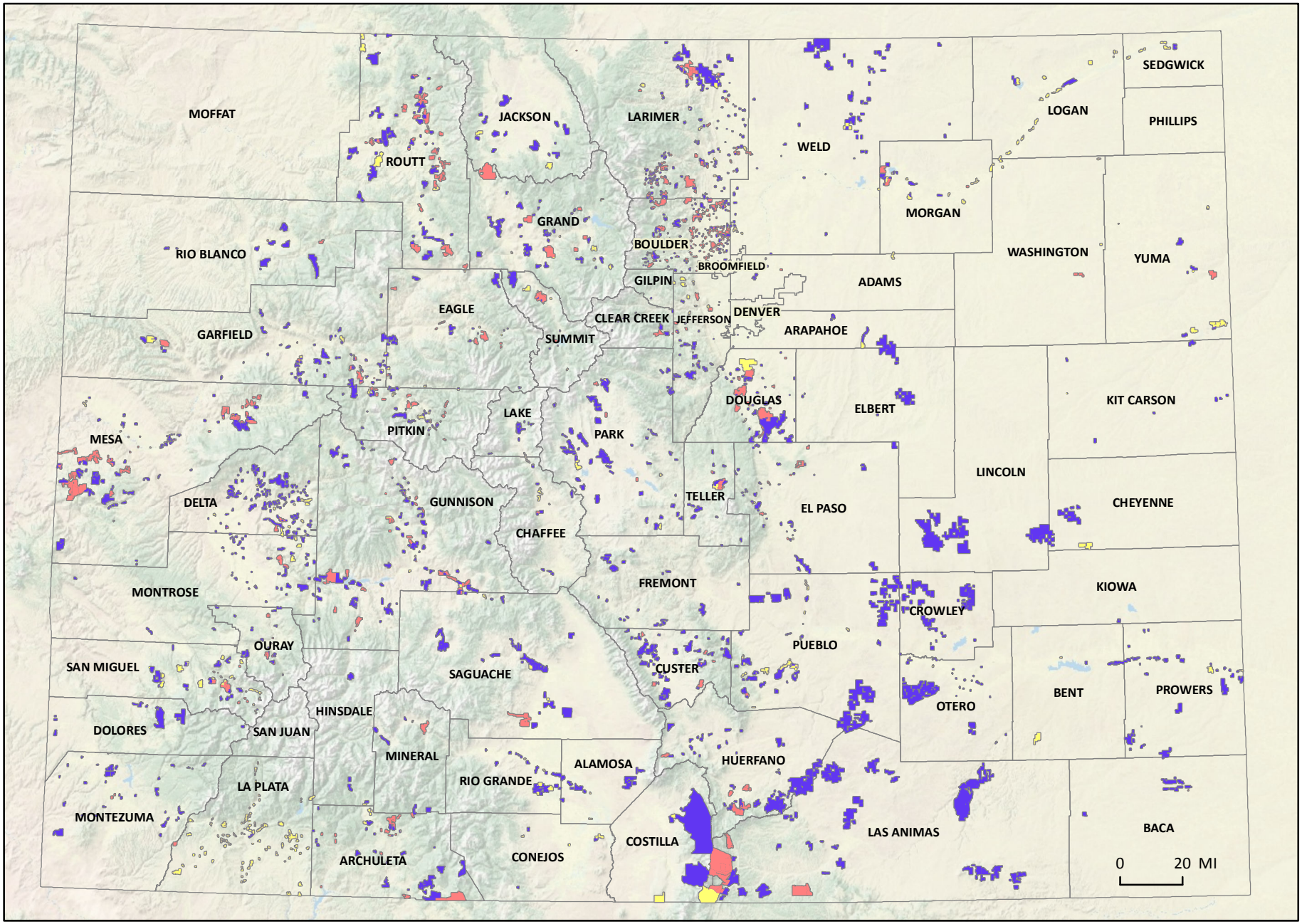
In addition to these considerations, tax policy at the federal and state levels gives landowners incentives to donate conservation easements instead of gifts of fee title.

Federal and State Tax Benefits

Landowners (i.e., taxpayers) who donate all or a portion of a conservation easement to a governmental entity or nonprofit organization may qualify for federal and state tax benefits. Federal law [26 USC 170(h)] allows taxpayers to claim a federal income tax deduction for all or part of a donated conservation easement, which the tax code refers to as a "qualified conservation contribution." Taxpayers must meet the general requirements for a charitable contribution, as well as the specific requirements for conservation easement donations.

In addition to the federal tax deduction, 15 states, including Colorado, provide a state income tax credit to incentivize land protection through conservation easements. A tax credit, as distinguished from a tax deduction, is applied after the tax liability is calculated, and it results in a dollar-for-dollar reduction of the tax liability. The 15 states that provide a conservation easement tax credit have not followed a uniform model or approach in creating their credits. There is significant variation among the states on basic parameters, such as the maximum dollar amount of the credit allowed, which taxpayers may claim the credit, and whether the credit can be transferred to other taxpayers. We provide a comparison of states' conservation easement income tax credits in Appendix A.

Conservation Easements in Colorado



Conservation easements created in 2000 or later Conservation easements created before 2000 Date established unknown

Source: Geospatial Centroid at Colorado State University with data provided from Colorado Ownership, Management, and Protection (COMaP) v9 Database. Colorado State University, Fort Collins, CO. (September 2011).

Colorado's Conservation Easement Tax Credit

For tax years beginning on or after January 1, 2000, state statute [Section 39-22-522(2), C.R.S.] allows taxpayers to claim a state income tax credit for all or part of a donated conservation easement. Throughout the report we refer to such conservation easements as tax-credit-generating easements. A taxpayer does not have to claim a federal tax deduction to claim the state tax credit. However, under state law, the state conservation easement tax credit is not allowed if the conservation easement donation does not qualify as a charitable conservation contribution in accordance with federal laws and regulations.

Specifically, to qualify for the state tax credit, the donated conservation easement must meet a number of minimum requirements, including the following:

- **Perpetuity.** The conservation easement must be perpetual in nature. For example, a deed of conservation easement that only imposes restrictions for a set period of time (e.g., 10 years) would not qualify for a tax credit because the easement is not held in perpetuity. The deed of conservation easement must ensure that the restrictions remain on the property forever, thereby creating an ongoing legal and financial obligation for current and future landowners to manage and maintain the property in accordance with the easement's terms and conditions. Because conservation easement holders do not occupy the land, they must have stewardship programs in place to ensure that landowners abide by the easement's terms and conditions, which can involve the easement holder's taking legal action against the landowner.

- **Conservation Purpose.** The conservation easement must be exclusively for one or more of the following conservation purposes:

    - The preservation of land areas for outdoor recreation by, or the education of, the general public.

    - The protection of a relatively natural habitat or ecosystem.

    - The preservation of open space (including farmland and forest land) where there is significant public benefit, and the preservation is (1) for the scenic enjoyment of the general public or (2) pursuant to a clearly delineated federal, state, or local governmental conservation policy.

    - The preservation of a historically important land area or a certified historical structure.

The deed of conservation easement must prohibit uses of the land that are inconsistent with the established conservation purpose. For example, a donated conservation easement would not qualify for a tax credit if the purpose of the easement is to protect habitat for a threatened bird species and the deed of conservation easement does not prevent the landowner from using pesticides that would eliminate the insects that are the natural food source for the bird species.

- **Qualified Organization.** The conservation easement must be donated to a qualified organization. State statute [Section 38-30.5-104(2), C.R.S.] requires the holder of a conservation easement to be a governmental entity or a nonprofit organization that is exempt under section 501(c)(3) of the federal Internal Revenue Code. Typically, nonprofit organizations that hold conservation easements are land trusts or other conservation organizations. Additionally, effective January 1, 2010, for nonprofit organizations and January 1, 2011, for governmental entities, if a tax credit will be claimed for a donated conservation easement, state statute [Section 12-61-720(8), C.R.S.] requires the governmental entity or nonprofit organization receiving the donation to be certified by the Division of Real Estate within the Colorado Department of Regulatory Agencies at the time of the donation. This certification process is intended, in part, to ensure that the conservation easement holder has a commitment to protect the conservation purposes of any conservation easement donations and has sufficient resources to enforce compliance with the easements' restrictions.

- **Qualified Appraisal and Appraiser.** The fair market value of the conservation easement donation must be established by a qualified appraisal completed by a qualified appraiser no more than 60 days prior to the donation and not later than the filing of the income tax return for the year of the donation. In Colorado, any individual who performs a conservation easement appraisal must be licensed as a certified general appraiser and comply with all state licensure and continuing education requirements established by the Board of Real Estate Appraisers. The appraisal must also be performed in accordance with Uniform Standards of Professional Appraisal Practice (USPAP). Appraisers must adhere to licensure, continuing education, and USPAP requirements for all conservation easement appraisals they perform, regardless of whether the easement is purchased or donated or a tax credit will be claimed. However, if a conservation easement appraisal will be used to claim a state tax credit, the appraiser must have completed a conservation easement appraiser update course once every 2 years.

Other Requirements

The state conservation easement tax credit is available to Colorado resident individuals, C corporations, trusts, estates, and members of pass-through entities, such as partnerships, S corporations, and limited liability companies, that donate all or part of a perpetual conservation easement to a governmental entity or charitable organization.

The landowner donating a conservation easement must file a claim for the full value of the available tax credit in the tax year in which the easement is donated. A "tax year" is a period of 12 consecutive months that is covered by a particular tax return and used as a basis for calculating liabilities. For individuals, the tax year runs on a calendar-year basis, beginning January 1 and ending December 31. For example, an individual donating a conservation easement in June 2012 would claim the tax credit on his or her 2012 state income tax return (i.e., Tax Year 2012) that will be due in April 2013. For businesses, the tax year may run on either a calendar-year basis or the entity's fiscal year.

When filing a tax return claiming a conservation easement tax credit, the landowner may use all or part of the credit in that same tax year depending on the amount of the landowner's state income tax liability. If the landowner has a state income tax liability that is less than the value of the tax credit in the tax year in which the conservation easement is donated, the remaining value of the credit can be carried forward and used against income tax liabilities for up to 20 succeeding tax years. The credit cannot be applied to tax years prior to the donation.

House Bill 00-1348 made the conservation easement tax credit transferable. This means that landowners may sell all or a portion of their tax credit to another taxpayer, known as a transferee. The sales price of the credit depends upon the terms of the sales contract (e.g., buyers often only pay a percentage of the total value of the credit). Landowners can use the transferability of the conservation easement tax credit to gain a lump-sum payment versus realizing their credit's full value over time. The transferability of the credit also makes the credit accessible to a broader range of taxpayers because, generally speaking, only those taxpayers who have a sufficient state income tax liability over a 20-year period are able to utilize the full value of their tax credits themselves. Financial gains from the sale of a conservation easement tax credit are taxed as ordinary income.

Only one conservation easement tax credit may be earned and claimed each year by the landowner donating a conservation easement. That is, multiple credits may not be earned in one year from multiple donations. Additionally, the full value of a credit must be used or abandoned by either the landowner or a transferee before the landowner can claim another credit for another donation.

Tax Credit Calculation

Currently, for Tax Years 2007 and beyond, the total dollar amount of any single tax credit that can be claimed is equal to 50 percent of the donation's fair market value, up to a maximum of $375,000. Thus, a taxpayer would reach the maximum credit allowed with a conservation easement donation that had a fair market value of $750,000 or greater. The following table shows how the calculation of the tax credit's total dollar amount has changed since the credit first became available on January 1, 2000.

State Conservation Easement Tax Credit
Calculated Credit Amounts and Maximums

Tax Years	Calculated Credit Amount as a Percentage of the Donation's Fair Market Value (FMV)	Maximum Credit Allowed	Enabling/Amending Legislation
January 1, 2000–December 31, 2002	100% of FMV	$100,000	House Bill 99-1155
January 1, 2003–December 31, 2006	100% of the first $100,000 in FMV plus 40% of the FMV exceeding $100,000	$260,000[1]	House Bill 01-1090
January 1, 2007–Present	50% of FMV	$375,000[2]	House Bill 06-1354

Source: Office of the State Auditor's analysis of the Colorado Revised Statutes and Session Laws.
[1] This maximum would be reached by a conservation easement donation with a FMV of $500,000 or greater.
[2] This maximum would be reached by a conservation easement donation with a FMV of $750,000 or greater.

Although state statute limits the total dollar amount of any *single* tax credit, there is no permanent aggregate limit on the total dollar amount of conservation easement tax credits available for tax years ending prior to January 1, 2011. However, House Bill 10-1197 limited the total dollar amount available for new conservation easement tax credits to $26 million for tax years beginning during calendar years 2011, 2012, and 2013. House Bill 11-1300 subsequently lowered this aggregate limit to $22 million each for 2011 and 2012 and increased this aggregate limit to $34 million for 2013. Taxpayers who wish to claim a conservation easement tax credit in any of these years must first obtain a credit certificate from the Division of Real Estate. The credit certificate reserves the taxpayer's right to claim a tax credit.

The Division of Real Estate distributes credit certificates on a first-come, first-served basis throughout the year. Once the total dollar value of issued certificates reaches the aggregate limit for a given calendar year, taxpayers requesting credit certificates are issued a certificate for a subsequent year. The following table shows the total dollar value of tax credit certificates issued by the Division of

Real Estate and the available balance under the aggregate limits as of August 17, 2012.

Tax Credit Certificates Issued by the Division of Real Estate *(As of August 17, 2012)*		
Calendar Year	**Dollar Value of Issued Certificates[1]**	**Available Balance**
2011	$22,000,000	$0
2012	$22,000,000	$0
2013	$2,362[2]	$33,997,638
Total	**$44,002,362**	**$33,997,638**

Source: Division of Real Estate.

[1] The dollar value of the tax credit certificate corresponds to the dollar value of the tax credit that the taxpayer will claim. However, the final dollar value of the tax credit may be lower once it is reviewed by the Department of Revenue because of disallowances and adjustments.

[2] The Division of Real Estate issued all of the certificates for credits available under the 2012 capped amount. Therefore, in accordance with state rules, it began issuing tax certificates for new tax credit claims that will count against the 2013 capped amount.

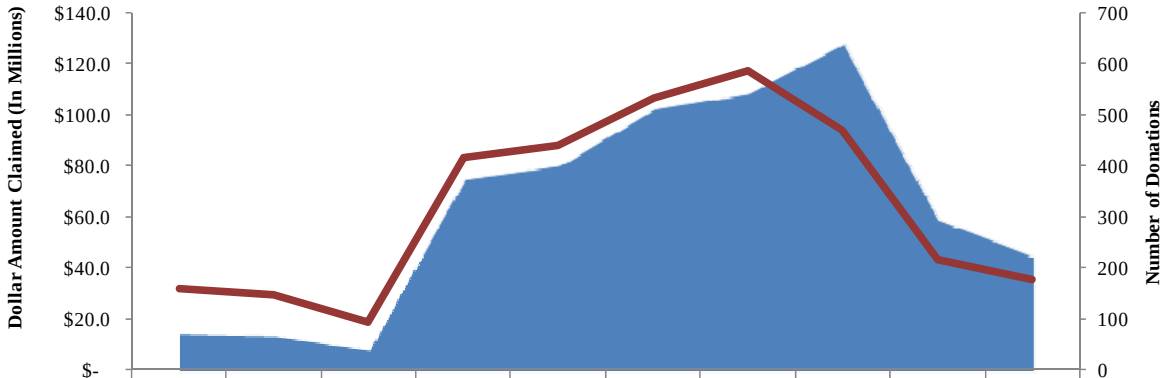
In years that the State has surplus revenue under Article X, Section 20 to the Colorado Constitution, more commonly known as the Taxpayer's Bill of Rights (TABOR), taxpayers who donate conservation easements and whose available tax credit is larger than their tax liability are eligible for a tax refund of up to $20,000 for tax years beginning January 1, 2000, through December 31, 2002, and up to $50,000 for tax years beginning on or after January 1, 2003. Only the original donor of the conservation easement qualifies for a tax refund; refunds are not available to transferees. The State had a TABOR surplus and allowed for payment of the conservation easement tax credit as a refund in Tax Years 2000, 2001, and 2005.

Tax Credit Utilization

Similar to other tax credits, the State "pays" for the conservation easement tax credit by foregoing revenues from individual and corporate income taxes that it otherwise would have collected. Overall, for the 10-year period since the credit's inception in Tax Year 2000 through Tax Year 2009, taxpayers have claimed approximately $639 million in tax credits resulting from approximately 3,200 conservation easement donations. As of the completion of our audit, the Department of Revenue had not completed its review and entry of the Tax Year 2010 and 2011 data. For purposes of illustrating overall trends, the following chart provides a compilation of data maintained by the Department of Revenue on conservation easement tax credits claimed for Tax Years 2000 through 2009.

Conservation Easement Tax Credits Claimed
Tax Years 2000 Through 2009

Total Dollar Amount Claimed: $638.9 Million
Total Number of Donations: 3,227



	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Dollar Amount Claimed	$14.9	$14.1	$8.8	$75.3	$80.5	$102.9	$109.2	$128.5	$59.5	$45.2
Number of Donations	159	146	92	414	439	531	585	468	216	177

Tax Year

Source: Office of the State Auditor's analysis of Department of Revenue data.

The data show a significant increase in the dollar amount of credits claimed between Tax Years 2000 and 2007. The dollar amount of credits claimed increased by 762 percent over this period, with a high in Tax Year 2007 of approximately $128.5 million in claims.

Subsequent to Tax Year 2007, the dollar amount of credits claimed fell by 65 percent to approximately $45.2 million in Tax Year 2009. The trend line will fall again because of the aggregate limits in place for the tax credit for 2011, 2012, and 2013. Apart from trends in overall economic conditions, legislative changes are likely a key factor driving utilization of the conservation easement tax credit. For example, increases in the maximum dollar amount of the credit, as well as changes that made the credit transferrable to taxpayers other than the landowner, may have provided further incentives for landowners to donate a conservation easement and pursue the tax credit, thereby contributing to the increase in claims through Tax Year 2007. Legislative changes in 2008, which we discuss in the next section, put more safeguards in place to ensure the validity of the conservation easement donations being used to claim a tax credit. This additional scrutiny may have dissuaded some landowners from pursuing the tax credit.

House Bill 08-1353

Discoveries of possible abuses of tax benefits associated with conservation easements resulted in the federal Internal Revenue Service (IRS) initiating audits of conservation easement transactions completed by Colorado taxpayers. DOR received information about these audits from the IRS in 2007, which triggered further audits and investigations by the Department of Revenue and the Division of Real Estate. Although the conservation purpose of some easements was questioned, the most common problems identified were violations of USPAP standards and misstatements of value by the appraisers conducting the appraisals. By overvaluing the land, the fair market value of the conservation easement donation was inflated, thereby inappropriately allowing the landowner to claim a larger tax credit.

In response to problems identified by the federal and state tax audits, the General Assembly enacted House Bill 08-1353 during the 2008 Legislative Session to help ensure the validity and proper valuation of conservation easements that are donated by landowners and used as the basis for claiming a tax credit. House Bill 08-1353 made the following significant changes:

- Established additional requirements for appraisers conducting conservation easement appraisals, including that a copy of the completed appraisal and an affidavit affirming several items (e.g., a statement specifying the value of the unencumbered property and the total value of the conservation easement along with details of the methods used to determine these values) be submitted to the Division of Real Estate within 30 days following the completion of the appraisal.

- Required the Division of Real Estate to review submitted conservation easement appraisals and corresponding affidavits for completeness and to track this information in an electronic database.

- Authorized the Division of Real Estate to investigate the activities of any appraiser who submits an appraisal of a conservation easement, including whether the appraiser complied with USPAP requirements or a substantial misstatement of value has occurred.

- Established a certification process at the Division of Real Estate whereby governmental entities and charitable organizations that hold tax-credit-generating conservation easements must meet certain minimum requirements.

- Established a nine-member Conservation Easement Oversight Commission to advise the Division of Real Estate and the Department of

Revenue regarding conservation easements for which a tax credit is claimed and to review applications for conservation easement holder certification.

- Required the Department of Revenue to consult with the Division of Real Estate and the Conservation Easement Oversight Commission to develop and implement a separate process for its review of conservation easement tax credit claims.

Administration

There are a number of different actors involved in the creation and acquisition of conservation easements that are used as a basis for claiming a tax credit:

- **Landowner (Donor).** An individual or corporate taxpayer who owns the land that is subject to a conservation easement and who donates all or a portion of the easement to a governmental entity or nonprofit organization. The landowner uses the conservation easement tax credit to offset its state income tax liability or sells the credit to another taxpayer. Throughout the report we use the terms landowner and donor interchangeably.

- **Conservation Easement Holder.** A governmental entity or nonprofit organization that acquires a conservation easement through a donation from a landowner. The conservation easement holder is responsible for monitoring the land to ensure that the landowner abides by the easement's terms and conditions.

- **Appraiser.** A state-licensed real estate professional, typically hired by the landowner, who appraises conservation easements in accordance with established professional appraisal standards with the purpose of determining the conservation easement's fair market value.

- **Transferee.** An individual or corporate taxpayer who, generally with the assistance of a third-party broker, purchases a conservation easement tax credit from a landowner. The transferee uses the purchased tax credit to offset its own state income tax liability.

There are a number of different agencies that share responsibility for administering Colorado's conservation easement income tax credit:

- **Department of Revenue (DOR).** As the State's tax authority, DOR is responsible for administration, collection, audit, enforcement, and other activities pertaining to Colorado's tax laws. DOR's Taxpayer Service

Division (TPS) is responsible for processing tax filings, including all conservation easement tax credit claims. If a conservation easement tax credit claim does not comply with applicable laws and regulations, TPS staff disallow the taxpayer's use of the credit.

If TPS disallows the use of a credit, the taxpayer may either submit any missing documentation to resolve the issue without requesting a formal hearing or has 30 calendar days to protest the decision and request a formal administrative hearing with DOR's Executive Director. The taxpayer has the opportunity to hold a pre-hearing conference with DOR's Tax Conferee Section that works with the taxpayer to try to come to a final resolution on protested matters. If a pre-hearing conference with the Tax Conferee fails to achieve a successful resolution, then the matter proceeds to a formal administrative hearing. The taxpayer may appeal the Executive Director's final determination to the district court for the county where the taxpayer resides or has his or her principal place of business. Pursuant to House Bill 11-1300, certain taxpayers were provided the option to bypass DOR's administrative hearing process and take their protest directly to the district court of the county where the land encumbered by the conservation easement is located. We did not review DOR's Tax Conferee or administrative hearing processes as part of this performance audit.

- **Division of Real Estate (DRE).** DRE is organizationally located within the Department of Regulatory Agencies and is responsible for the regulation of real estate professionals (e.g., real estate brokers, real estate appraisers, mortgage loan originators) doing business in Colorado. DRE works with the Real Estate Commission and the Board of Real Estate Appraisers to administer licensing and continuing education requirements, investigate complaints, and take disciplinary action against licensees for noncompliance with applicable requirements.

  With respect to conservation easement tax credits and the enactment of House Bill 08-1353, DRE receives copies of all conservation easement appraisals completed in Colorado. DRE also certifies those organizations that are qualified to hold conservation easements for which a tax credit will be claimed. Finally, starting January 1, 2011, DRE began issuing conservation easement tax credit certificates as a means of administering the aggregate caps on the total dollar amount of available conservation easement tax credits for calendar years 2011, 2012, and 2013.

- **Conservation Easement Oversight Commission (CEOC).** The nine-member CEOC is a Type 2 agency that, upon referral by DRE or DOR, reviews documents, such as a deed of conservation easement or an appraisal report, to provide advice regarding conservation easement

transactions for which a tax credit is claimed. The CEOC also reviews applications for certification from conservation easement holders and makes recommendations to the DRE Division Director to approve or deny certification.

The CEOC members represent a number of different stakeholder interests. By statute, the Great Outdoors Colorado Trust Fund, the Department of Agriculture, and the Department of Natural Resources each have a permanent member on the CEOC, and the Governor appoints the remaining six members for a 3-year term. (Three of the initial appointments were for a 2-year term.) The six gubernatorial appointments must represent a local land trust, a state or national land trust, a local government open space or state conservation agency, a historic preservation organization, a certified general appraiser with conservation easement appraisal experience, and a landowner who has donated a conservation easement in Colorado. No more than three of the Governor's appointees serving at the same time may be from the same political party.

- **Board of Real Estate Appraisers (BOREA).** This seven-member board is a Type 1 agency with jurisdiction over all real estate appraisers in Colorado, including those who appraise conservation easements. BOREA makes policy decisions and establishes rules regarding licensure, continuing education, and experience requirements; reviews complaints; and takes disciplinary action against appraisers. BOREA's membership comprises three licensed appraisers, one county assessor, one banker with experience in mortgage lending, and two members of the general public. All members are appointed by the Governor with confirmation by the State Senate for a 3-year term.

Audit Purpose, Scope, and Methodology

We conducted this performance audit in response to a legislative request. Audit work was performed from December 2011 through September 2012. We acknowledge the cooperation and assistance provided by management and staff at the Department of Revenue and the Division of Real Estate, the members of the Conservation Easement Oversight Commission, and staff affiliated with the COMaP (Colorado Ownership, Management, and Protection) project at Colorado State University.

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

evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The overall objective of this audit was to determine whether there are effective internal controls in place at both the Department of Revenue and the Division of Real Estate to ensure that conservation easement tax credits being claimed and used by taxpayers are valid. We planned our audit work to assess the effectiveness of those internal controls that were significant to our audit objectives. Our conclusions on the effectiveness of those internal controls are described in the audit findings and recommendations.

Because of the significant legislative changes that occurred in 2008, our audit focused on requirements and processes in place for the conservation easement tax credit since the enactment of House Bill 08-1353. Specifically, we evaluated:

- Whether processes for reviewing conservation easement appraisals are sufficient to ensure that the appraisal is performed by a qualified appraiser and that any material violations of professional standards, substantial misstatements of value, or other relevant matters are identified and communicated to DOR.

- Whether processes for certifying and renewing certification for conservation easement holders are sufficient to ensure that only qualified entities are being certified to hold conservation easements for which state tax credits will be claimed.

- Whether processes for reviewing conservation easement tax credit claims are sufficient to ensure that unqualified tax credit claims are denied and qualified tax credit claims are not denied.

- Whether all essential elements related to conservation easement tax credit claims are reviewed at the most effective and efficient point in the process.

- The conservation easement tax credit program's overall value and effectiveness.

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.

To accomplish our audit objectives, we:

- Researched federal and state laws, rules, and regulations pertaining to the federal conservation easement tax deduction and Colorado's state conservation easement tax credit.

- Reviewed DOR and DRE policies and procedures for administering Colorado's conservation easement tax credit.

- Interviewed DOR and DRE management and staff and other stakeholders, including all members of the CEOC.

- Reviewed and analyzed documentation and data on conservation easement tax credit claims, conservation easement appraisals, and conservation easement holder certification applications.

- Gathered and analyzed information on general trends in conservation easements in Colorado.

- Compared and contrasted Colorado's conservation easement tax credit with similar programs in other states.

We relied on sampling techniques to support our audit work in three specific areas:

- We selected a nonstatistical judgmental sample of 10 conservation easement tax credit donor claims and associated supporting documentation filed in Tax Years 2009 and 2010. We selected our sample items to provide representation of credit claims that were allowed and disallowed, credit claims of varying dollar amounts, credit claims from individual and corporate taxpayers and pass-through entities (e.g., nonprofits or limited liability companies), conservation easements held by different conservation easement holders, conservation easements in different areas of the state, and conservation easement donations made by the same donor over time. We designed our sample to help provide sufficient, appropriate evidence for the purpose of evaluating DOR's process for reviewing tax credit claims based on our audit objectives.

- We selected a nonstatistical judgmental sample of 25 of the 46 organizations that had applied for certification as a conservation easement holder as of March 2012. We selected our sample items to provide representation of approved and denied applications, governmental entities and nonprofit organizations, different sized organizations, and organizations located in different areas of the state. We did not select any organizations that were accredited by the Land Trust Alliance because certification applications from these organizations receive expedited

approval by DRE. We designed our sample to help provide sufficient, appropriate evidence for the purpose of evaluating DRE's certification process based on our audit objectives.

- We selected a nonstatistical judgmental sample of 10 of the 330 conservation easement appraisals that had been submitted to DRE as of February 2012 and were specifically related to a conservation easement tax credit claim filed in Tax Years 2009 or 2010. We selected our sample items to provide representation of conservation easement appraisals that DRE subjected to a desk review, as well as conservation easement appraisals that DRE did not subject to a desk review. We designed our sample to help provide sufficient, appropriate evidence for the purpose of evaluating DRE's conservation easement appraisal review process based on our audit objectives.

Specific details about the audit work supporting our findings, conclusions, and recommendations are described in the body of the report.

This page intentionally left blank.

Administration of the Conservation Easement Tax Credit

Chapter 2

The General Assembly created the conservation easement tax credit in 1999 partly in response to the rapid population growth that Colorado was undergoing. About one million new residents came to the state in the 1990s, increasing the population by about 31 percent. Residential and commercial land development boomed during this time, especially in rural areas where land was quickly being converted from agricultural uses. In this context, the conservation easement tax credit was proposed as a way to limit the spread of new development and to protect swaths of land that are considered valuable for conservation. Additionally, lawmakers recognized that the tax credit might provide a much-needed lifeline to some farmers and ranchers who were facing increasing economic pressure and were looking for additional ways to monetize their land holdings, short of selling to developers.

Overall, the various requirements and processes in place for administering the conservation easement tax credit are intended to accomplish land conservation goals while ensuring that the State is not foregoing more revenue than it should. Having strong administrative processes to determine whether a tax credit claim should be allowed or disallowed is important for protecting the broader taxpayer interests because foregone tax revenues cannot be used to fund state services and programs, such as education, transportation, or unemployment benefits.

As of 2009, nearly $640 million in tax credits had been claimed on about 3,200 easements since the credit was first made available in 2000, although this total may end up being lower because some claims have been disallowed and are in various stages of dispute resolution. In return, landowners preserved about 925,000 acres of land in a predominantly natural, scenic, or open condition. Despite these positive aspects, however, the conservation easement tax credit has also fallen subject to abuse by some developers, landowners, and appraisers who misrepresented properties' conservation or financial values to obtain undue financial benefits. New requirements were put in place in 2008 through the enactment of House Bill 08-1353 to try to curb these types of abuses.

The State took an important step forward in its administration of the conservation easement tax credit with the enactment of House Bill 08-1353. However, our audit demonstrates that more changes need to be made to strengthen the

administration of Colorado's conservation easement tax credit to ensure that tax credits being claimed and used by taxpayers are valid.

Colorado's conservation easement tax credit is administered through a series of interrelated processes performed by the Department of Revenue (DOR), the Division of Real Estate (DRE), and the Conservation Easement Oversight Commission (CEOC). As discussed in this chapter, our audit findings suggest two different, but not mutually exclusive, directions for strengthening the State's administration of the conservation easement tax credit. One direction is to improve each of the individual processes. Throughout this chapter we make a number of recommendations to DOR, DRE, and the CEOC for improving reviews of tax credit claims, reviews of conservation easement appraisals, and the certification of conservation easement holders. A second direction, which we discuss at the end of this chapter, is to fundamentally shift the manner in which the tax credit is administered by moving to a pre-approval process. We believe that such a move could hold a number of important benefits for the State and its taxpayers and is worthy of further study by DOR, DRE, and the CEOC and consideration by the General Assembly.

If the State moves forward with and adopts a pre-approval process, DOR, DRE, and the CEOC will likely need to adjust their implementation of the other recommendations contained in this report. Conversely, if a pre-approval process is not ultimately adopted, it will be important that DOR, DRE, and the CEOC fully implement the remaining audit recommendations to strengthen the individual processes for administering the conservation easement tax credit.

Review of Tax Credit Claims

DOR is responsible for the administration, collection, audit, enforcement, and other activities pertaining to Colorado's tax laws. Thus, DOR is the decision maker and accountable party when it comes to determining whether taxpayers meet the legal and regulatory requirements to qualify for a conservation easement tax credit, and it has the authority to disallow claims when these requirements are not met. We detail the various requirements to qualify for a conservation easement tax credit in Chapter 1.

One of the objectives of our audit was to determine whether DOR's review process is sufficient to ensure consistent and appropriate treatment of conservation easement tax credit claims. To address this objective, we reviewed applicable statutes, rules and regulations, and DOR policies and procedures. We also conducted numerous interviews with DOR management and staff who perform and oversee the tax credit claim review process. Finally, we reviewed hard-copy and electronic file documentation for a nonstatistical judgmental sample of 10 conservation easement tax credits claimed in Tax Years 2009 and 2010. We selected our sample to include coverage of areas important for

evaluating the overall tax credit review process, such as credit claims that were allowed and disallowed, were made by the same donor, were forwarded to DRE and the CEOC for consultation, were of varying dollar amounts, and were from individual and corporate taxpayers and pass-through entities (e.g., partnerships, S corporations, and limited liability companies).

As described in Recommendation Nos. 1 through 3, we found that DOR's review of conservation easement tax credit claims needs attention in three areas. Specifically, the scope of DOR's review does not ensure coverage of key requirements and relevant risk areas, tax examiners do not sufficiently document their reviews of conservation easement tax credit claims and uses, and there are concerns about the completeness and accuracy of tax credit data maintained in DOR's database.

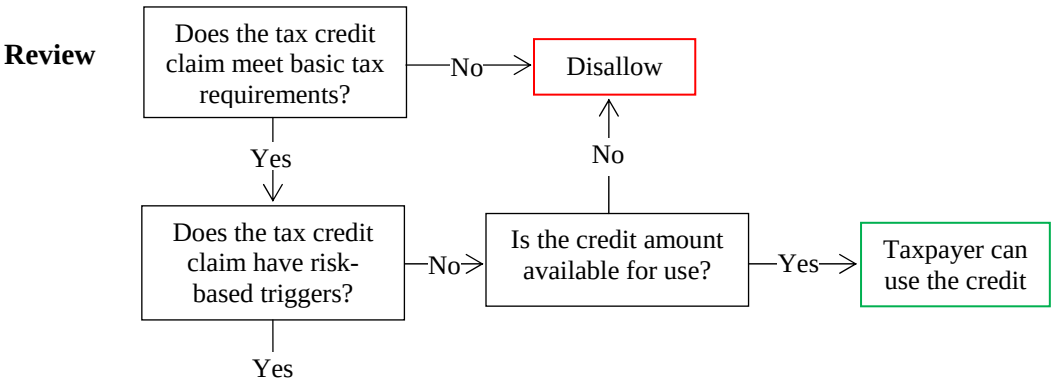
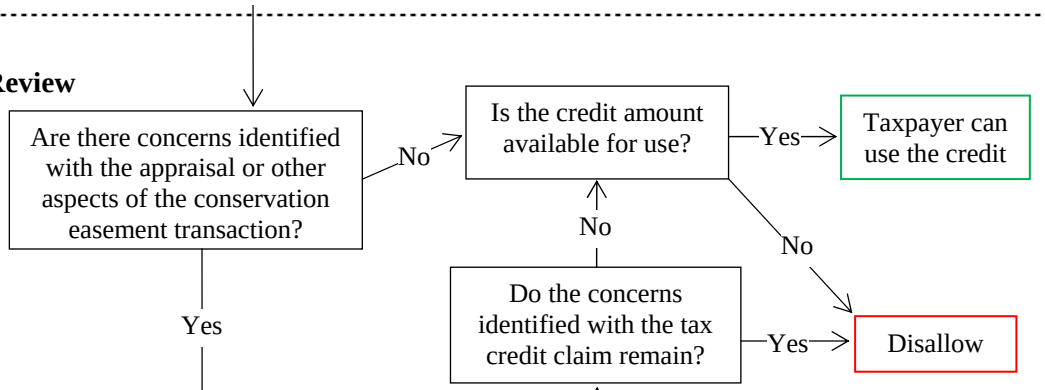
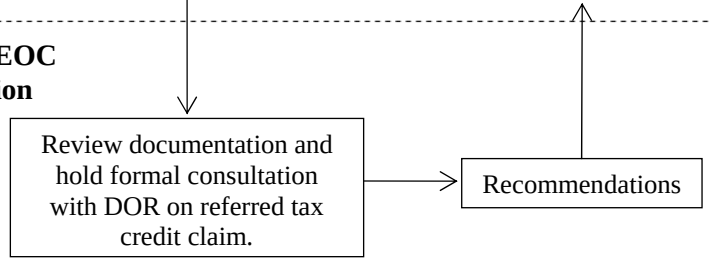
Scope of Review

DOR's Taxpayer Service Division (TPS) is responsible for reviewing tax filings, including all conservation easement tax credit claims. Two TPS tax examiners are assigned to review conservation easement tax credit claims and supporting documentation to determine whether the tax credits being claimed and used by taxpayers are valid. TPS's review of conservation easement tax credit claims is *the* primary control for ensuring that the State does not (1) lose tax revenues by allowing unqualified tax credit claims or (2) over-collect tax revenues by disallowing qualified tax credit claims.

Generally speaking, TPS utilizes a risk-based approach when reviewing conservation easement tax credit claims, which means that not every statutory and regulatory requirement is examined on every claim. Additionally, similar to other tax administration processes, when tax examiners review a tax credit claim, they do not technically "approve" the claim. Rather, they do not disallow the claim. A tax credit claim can be disallowed at several different points during the review process, and credit claims that are not disallowed are available for use by the taxpayer. As described in Chapter 1, the landowner (i.e., donor) must file a claim for the tax credit in the tax year in which the easement is donated, regardless of whether the credit is used to offset a tax liability in that year. However, in terms of the timing of TPS's review, tax examiners only review tax credit claims once a taxpayer (either the donor or a transferee) files a tax return *using* the credit. That is, if a credit claim is filed in 2010 but is not used to offset a tax liability until 2012, then TPS's review would not occur until 2012. (We discuss some problems caused by this timing issue later in Recommendation Nos. 3 and 11.)

The following table provides a summary of TPS's process for reviewing conservation easement tax credit claims, as well as the different factors that are examined at each level of the review process.

Colorado Department of Revenue
Conservation Easement Tax Credit Review Process

Process Flow	Which Claims Are Reviewed?	Factors Reviewed
DOR Level 1 Review 	All conservation easement tax credit claims.	• The taxpayer was a Colorado resident at the time of the donation or transfer. • All required forms and documents were submitted. • The donation occurred during the donor's tax year, or the transfer occurred before the transferee's filing deadline. • The tax liability was calculated correctly. • The appraisal was performed by a qualified appraiser. • Whether risk-based triggers are present (e.g., certain land uses listed in the appraisal). • The credit amount is available for use.
DOR Level 2 Review 	Conservation easement tax credit claims with risk-based triggers identified through a Level 1 review.	• The fair market value of the easement was established by a qualified appraisal. • The deed of conservation easement is perpetual and restricts imminent development. • The highest and best use is appropriate. • Comparables are appropriate. • Building envelopes and water, mineral, and drilling rights are not excluded. • Zoning changes are not assumed. • Ownership is not divided. • The credit amount is available for use.
DRE & CEOC Consultation 	Conservation easement tax credit claims referred by DOR for consultation.	• DRE issues an opinion to DOR on whether it appears there may be material violations of Uniform Standards of Professional Appraisal Practice that could adversely impact analyses and conclusions stated in the appraisal. • CEOC issues an opinion to DOR on whether to accept or reject the tax credit associated with the conservation easement transaction.

Source: Colorado Office of the State Auditor's interviews with Department of Revenue staff and review of available procedural documentation.

All conservation easement tax credits undergo a Level 1 review, during which a tax examiner determines compliance with basic tax requirements. The tax examiner also determines whether certain risk factors or "triggers" are present, thereby warranting a more in-depth Level 2 review by another tax examiner. Examples of risk factors include appraisers or conservation easement holders with past problems or issues and appraisals that list gravel mining as the highest and best use (i.e., the category of possible use that would give the land the most value without an easement). During a Level 2 review, a more experienced tax examiner reviews the deed of conservation easement, the appraisal, and other documentation substantiating the tax credit claim. Concerns identified through a Level 2 review that relate to the appraisal or other aspects of the conservation easement transaction (e.g., conservation purpose) are referred for a formal consultation with DRE and the CEOC. Generally, after receiving input from DRE and the CEOC, DOR makes the final decision to allow or disallow the tax credit claim. The tax examiner working the claim also determines whether the credit amount being used is available (e.g., the donor has not claimed or used more than one conservation easement tax credit for the same tax year or the total amount of the credit used by donors and transferees does not exceed the total credit amount allowed).

Conservation Purpose

To qualify for a tax credit, state statute [Section 39-22-522(2), C.R.S.] requires donated easements to meet one or more federally recognized conservation purposes—preservation of land areas for outdoor recreation; protection of fish, wildlife, or plant habitat; preservation of open space; or preservation of a historically important land area. Ensuring the appropriateness of an easement's conservation purpose is one of the cornerstones to the tax credit.

As shown in the previous table, there are a number of factors that TPS staff examine during their review process. These review factors are generally aligned with the various statutory and regulatory requirements that must be met in order to claim the conservation easement tax credit. However, we found that conservation purpose receives little to no coverage by TPS's tax examiners during their reviews of tax credit claims. This is a concern, given the legal and substantive significance of an easement's conservation purpose for qualifying for a tax credit.

Specifically, we found that conservation purpose is not one of the factors that TPS's tax examiners review during either a Level 1 or a Level 2 review of the tax credit claim. During a Level 1 review, TPS staff do not perform a basic verification that the conservation purpose reported by the landowner is consistent with one or more of the four allowable conservation purposes. (We discuss problems related to landowner reporting on conservation purposes in Chapter 3.)

During a Level 2 review, TPS staff review the appraisal and the deed of conservation easement; however, the Level 2 review focuses primarily on the appraisal methodology and does not include a review of conservation purpose.W we found no evidence that DOR had reviewed the conservation purpose for the 10 tax credit claims we sampled.

We recognize that fully validating an easement's conservation purpose may require careful review of the deed of conservation easement, the appraisal, and other documentation, such as a baseline report that documents the property's present condition. Additionally, as discussed later in Recommendation No. 11, tax examiners may lack the expertise necessary to fully evaluate an easement's conservation purpose. Nonetheless, the lack of consideration of the conservation purpose underlying conservation easement tax credit claims represents a significant gap in DOR's current Level 1 and Level 2 review processes that needs to be addressed. DOR should include at least a basic review of the conservation purpose reported by the taxpayer as part of a Level 1 review. State statute [Section 12-61-721(3)(a), C.R.S.] states that at the request of DOR, the CEOC shall advise DOR regarding conservation values. Thus, DOR should refer questionable claims to the CEOC for a more complete assessment of the easement's conservation purpose as part of a Level 2 review. Ultimately, if the conservation easement restricting the land being put under easement does not meet one of the legally recognized purposes, there is no reason for the State to be foregoing revenues to help protect it.

Risk Factors

As discussed previously, TPS utilizes a risk-based approach when reviewing conservation easement tax credit claims. Specifically, during a Level 1 review, tax credit claims are reviewed to determine whether certain risk-based triggers are present, thereby warranting a Level 2 review. Utilizing a risk-based approach can be a cost-effective way for DOR to target its staff resources when reviewing tax credit claims. However, risk-based approaches are only effective to the extent that relevant risk factors are properly identified and considered during the initial review. Although TPS has developed a list of risk factors to help target tax examiners' review activities, the list is incomplete in two key areas:

- **Phased Donations. "**Phasing" is a legal way for landowners to increase their tax benefits by donating conservation easements on different portions of a larger parcel of property or giving up additional development rights for the same parcel of land over time. In both cases, the new easement counts as a separate donation and may be eligible to receive a separate tax credit. During our file review, we identified five claims in our sample that appeared to be phased donations. Although phased donations are not necessarily problematic, according to DRE's staff appraiser and the

member of the CEOC who is an appraiser, special attention should be paid to appraisals of phased donations. The appraisal methodology can be complicated and, if not performed well, increases the risk of an incorrect valuation. Establishing the conservation purpose also becomes more complicated with phased donations because the conservation purposes cited for each donation need to be supported by the specific characteristics of that portion of the property. Currently, TPS does not include phased donations on its list of risk factors that escalate tax credit claims to a Level 2 review.

- **Donors with Prior Disallowed Claims.** During our file review, we identified one tax credit claim in our sample for Tax Year 2010 that was filed by a group of donors whose prior year claims had been disallowed. We inquired with TPS staff why these prior claims had been disallowed and whether those problems could be of concern for the 2010 claim. TPS staff reported that although the prior year disallowances were due to problems with the appraisals, the Level 1 review of the 2010 claim did not identify any triggers warranting a more in-depth review of the appraisal. We understand that each donation is a separate transaction, but it is reasonable to consider taxpayers who have had prior disallowances to be a higher risk group. The fact that the donors in the sampled case we reviewed had prior disallowances due to problems with the appraisals should have triggered the appraisal associated with the 2010 claim for additional review. Historical problems with taxpayers' tax credit claims are a reasonable risk indicator of problems with current claims that should be considered. TPS already takes this approach with respect to appraisers and conservation easement holders; tax credit claims that are associated with appraisers and conservation easement holders with known historical problems receive a more in-depth Level 2 review as a result.

By not specifically including phased donations or donors with prior disallowed claims on its "trigger list" for a Level 2 review, DOR is missing coverage of important risk areas. DOR does not follow a set schedule for evaluating and updating its list of risk factors. Some of the historical abuses of the tax credit were related to conservation easements on land for which the highest and best use was reported as gravel mining. Gravel mining continues to be a risk factor on TPS's list of risk factors; however, other risk factors have emerged and will continue to emerge as the tax credit evolves over time. Evaluating and updating the list of risk factors at least annually would ensure that the list is kept current and remains relevant to the tax credit claims being reviewed. In addition, DOR should use DRE and the CEOC to help identify new risks related to conservation easement transactions.

Recommendation No. 1:

The Department of Revenue (DOR) should strengthen its review of conservation easement tax credit claims to ensure coverage of key requirements and consideration of relevant risk factors by:

a. Including a basic review of the reported conservation purpose as part of a Level 1 review, and developing risk factors or other criteria that would require referral of the claim to the Conservation Easement Oversight Commission (CEOC) for a more complete assessment of the easement's conservation purpose as part of a Level 2 review.

b. Expanding the current list of risk factors to include phased donations and donors with prior disallowed credit claims.

c. Evaluating and updating the list of risk factors on at least an annual basis. DOR should consult with the Division of Real Estate (DRE) and the CEOC during this process.

Department of Revenue Response:

a. Agree. Implementation date: March 2013.

   DOR will include a basic review of the reported conservation purpose in its Level 1 review of conservation easement tax credit claims. In addition, as part of its on-going discussions with the Division of Real Estate (DRE) and the CEOC about improving the consultation process, DOR will develop risk factors to be considered as part of the Level 2 review of conservation easement tax credits which will include provisions for when the conservation purpose of an easement should be reviewed by the CEOC.

b. Agree. Implementation date: March 2013.

   DOR will expand its current list of risk factors to explicitly include all phased donations and prior disallowed credit claims. In addition, as part of its ongoing discussions with DRE and the CEOC about improving the consultation process, DOR will ask for input about its current list of risk factors which are used during the Level 1 and Level 2 reviews in order to determine more specific risk factors related to phased donations which may need to be addressed.

c. Agree. Implementation date: March 2013.

DOR currently updates its list of risk factors as it learns of new risks and will continue to do so. In addition, DOR will review its list of risk factors with DRE and the CEOC at the beginning of each fiscal year.

Review Documentation

Conservation easement transactions can be complex, and there are a number of requirements that the taxpayer must adhere to when claiming the tax credit. DOR's tax examiners must also rely on their professional experience and judgment when applying the tax laws and regulations and determining whether to allow or disallow a tax credit claim. Because of these characteristics, complete documentation of the review is important for ensuring that all required attributes are examined and that the resulting decisions to allow or disallow claims are appropriate and substantiated.

We found that TPS's tax examiners do not sufficiently document their reviews of conservation easement tax credit claims and uses. Tax examiners' notes were typically spread across various hard-copy documentation (e.g., letters, memos, tax returns, sticky notes) and electronic systems. More importantly, we found that the review documentation held little information about judgments made and conclusions reached by the tax examiners performing the review, including whether and which risk-based factors were present in the claim warranting a Level 2 review. As a result of these underlying documentation issues, we were limited in our ability to independently verify whether tax examiners reviewed key requirements that must be met for a conservation easement donation to qualify for a tax credit. The following bullet points highlight the specific documentation problems we encountered for the 10 sampled tax credit claims we examined.

- **Qualified Appraisal.** The appraisal establishes the fair market value of a conservation easement donation, which directly affects the amount of the tax credit that can be claimed. As discussed previously, conservation easement appraisals undergo a more in-depth Level 2 review only when certain risk-based factors are identified during a Level 1 review. We identified concerns related to reviews of appraisals for five of our 10 sampled claims. Specifically, for four of the claims, there was no documentation to indicate that the tax examiner had considered risk factors during the Level 1 review and that no risk factors were identified, thereby supporting the decision not to elevate the appraisals for these four tax credit claims to a Level 2 review. For the fifth claim, TPS reported that it eventually performed a Level 2 review and examined the appraisal when the taxpayer submitted required documentation after the claim was

disallowed. However, the only evidence of a Level 2 review we found was a number of blank sticky notes attached to the appraisal report, possibly as placeholders for the different sections that were examined. The tax examiner made no written notes on what was examined or the conclusions that were reached. This differed from two other claims in our sample for which the tax examiner documented that he or she had examined the appraisal during a Level 2 review as well as the issues or concerns identified during the review.

- **Qualified Appraiser.** Conservation easement appraisals supporting a tax credit claim must be conducted by an appraiser who is licensed by DRE as a certified general appraiser. For seven of our 10 sampled claims, there was no documentation indicating that the tax examiner had verified the appraiser was licensed by DRE. We noted that the appraiser associated with one of these claims was listed on TPS's list of risk factors, but it was unclear from the file documentation whether this was one of the reasons why the claim had a Level 2 review. We verified that the six appraisers who conducted the conservation easement appraisals associated with these seven sampled tax credit claims were licensed by DRE. For the three remaining claims in our sample (two were disallowed and one was allowed), neither we nor DOR could verify the appraiser's licensure status because the taxpayers did not submit some or all of the required documentation (e.g., appraisal report, appraiser affidavit) necessary to identify the appraiser completing the conservation easement appraisal.

- **Qualified Organization.** Entities holding tax-credit-generating conservation easements must be a governmental entity or a nonprofit organization and be certified by DRE. For two claims in our sample for which the certification requirement was applicable, there was no documentation indicating that the tax examiner had verified the conservation easement holders were certified by DRE. We verified that both holders associated with these two tax credit claims were certified by DRE. For six claims in our sample, the certification requirement was not applicable because the donations were made in 2009, before the certification requirement took effect. For the remaining two claims in our sample, neither we nor DOR could verify the conservation easement holder's certification status because the taxpayers did not submit some or all of the required documentation (e.g., tax forms, appraisal report) necessary to identify the governmental entity or nonprofit organization holding the donated conservation easement.

As discussed previously, we were generally limited in our ability to trace tax examiners' decisions to allow or disallow claims back to the underlying review documentation. Despite these limitations, however, for four of our sampled claims

our own review of the taxpayer's documentation revealed problems with the claim. Specifically, we found claims that should have been disallowed as well as problems on both allowed and disallowed claims that were not identified through the tax examiner's review. When combined with the lack of sufficient review documentation, these additional issues elevate the risk that DOR's decisions to allow or disallow conservation easement tax credit claims may not be appropriate and substantiated.

- **Missing Taxpayer Documentation.** We identified three claims for which taxpayers did not submit all documentation required by statute or rule, yet tax examiners allowed these taxpayers to use the tax credit. For two claims, the taxpayers did not submit the required tax forms and other supporting documentation, such as the appraisal, the appraiser affidavit, and the deed of conservation easement. These documents are key to substantiating that the donation meets requirements for claiming the tax credit. TPS staff confirmed that these two credits should have been disallowed because of the missing documentation. Finally, for the third claim, the taxpayer did not submit a copy of the appraiser affidavit. TPS staff stated that although the tax examiner should have obtained this document before allowing the credit, there was sufficient information from the other documentation on file to check the validity of the credit without subjecting the taxpayer to further requests. This course of action may have minimized some burden on the taxpayer, but statute requires that the appraiser affidavit accompany conservation easement appraisals. It is part of the supporting documentation for tax credit claims that is required to be submitted to DOR. Making an exception in this case is unfair to other taxpayers claiming the credit who submitted the required appraiser affidavit.

- **Credit Use and Carry-Forward Amounts.** We identified one claim for which the tax examiner did not properly verify the credit amounts being used and carried forward. The taxpayer mistakenly entered a $6,000 use of the credit on their e-filed return, despite having a tax liability of only $3,891. The taxpayer did not get more of a financial benefit than they were entitled to. However, the tax examiner should have caught this mistake and corrected the return appropriately. Additionally, the tax examiner's notes in DOR's electronic databases indicated that the taxpayer had used the full $6,000 credit even though the taxpayer had a carry-forward of $2,109 (the $6,000 incorrectly noted on the tax return minus the $3,891 use of the credit to offset the taxpayer's tax liability). This inaccurate accounting for the carry-forward amount in DOR's databases could cause confusion when the taxpayer tries to use the remainder of the tax credit in future tax years.

- **Claiming New Credits.** We identified one claim for which the donor tried to claim a new credit in 2009, despite not having fully used the carry-forward from their 2008 credit. State statute [Section 39-22-522(6), C.R.S.] restricts donors from claiming or using more than one conservation easement tax credit in the same tax year. Any previous credits claimed must be entirely used up or the remaining amounts abandoned by both donors and transferees before the donor can claim or use a new credit. DOR ultimately denied the tax credit claim for other reasons; however, we could not determine based on the available review documentation whether the tax examiner had also identified this problem.

Lack of Controls

Overall, DOR lacks sufficient controls over the review of conservation easement tax credit claims in three key areas. All of these controls are important for ensuring that decisions to allow or disallow credit claims are appropriate and substantiated. First, TPS's tax examiners do not use a standard work program or review tool to guide and document their review of conservation easement tax credit claims. As discussed previously, a key problem we identified through our audit was insufficient documentation of the tax examiners' reviews, which made it difficult to verify which items were reviewed on each tax credit claim and the resulting judgments made, conclusions reached, and subsequent actions taken. Use of a standard work program would help to ensure that all required aspects of a credit claim are examined consistently and provide tax examiners a means of documenting their reviews in a straightforward and consolidated manner. Standard work programs and checklists would also help DOR ensure that it has received all required supporting documentation and tax forms from taxpayers before starting its review.

Second, although TPS has established an overall work flow, it lacks detailed written policies and procedures for reviewing conservation easement tax credit claims. Currently, the written guidance for tax examiners performing the tax credit reviews consists of a couple of process flowcharts, a list of triggers that warrant a Level 2 review, and a somewhat abstract list of considerations that the tax examiner uses during a Level 2 review to identify problems or concerns with conservation easement appraisals. For example, the written guidance does not detail (1) the statutory, regulatory, and other tax requirements that must be reviewed on each claim during a Level 1 or Level 2 review; (2) how tax examiners' reviews should be documented; and (3) how exceptions should be handled. Written policies and procedures are an important control; they help management establish and communicate key expectations and requirements, and they provide structure and guidance to staff when performing their work. Formulating written policies and procedures also helps agencies institutionalize existing staff knowledge, which is important for training new staff and mitigating

the loss of knowledge that occurs when experienced staff retire or leave the agency.

Finally, the two tax examiners assigned to review conservation easement tax credit claims generally have little substantive oversight of their work by their immediate supervisors or TPS's quality control staff. These two tax examiners have three different individuals in their direct reporting line to the TPS Division Director. DOR also has a staff person from its investigations unit assigned to perform quality control reviews of tax examiners' work. However, none of these individuals reviews, even on a sample basis, the work supporting the tax examiners' decisions to allow or disallow conservation easement tax credit claims. When needed, the tax examiners typically seek guidance and input directly from the TPS Division Director or staff in DOR's Tax Conferee Section.

DOR reported that other TPS staff, including immediate supervisors, do not have sufficient expertise to review the more specialized work performed for the conservation easement tax credit. We understand that tax returns with conservation easement tax credit claims may be more complicated than a review of the typical tax return. However, supervisors and quality control staff should have a basic level of competency with the work being performed by TPS's tax examiners. Moreover, the complexity of the credit, as well as the large dollar amount of the credits being claimed, increases the risk of errors, fraud, and abuse occurring and, therefore, increases the need for adequate supervisory or quality control review. Routine review by supervisors and/or quality control staff of at least a sample of completed conservation easement tax credit reviews each year is an important control for identifying problems with supporting documentation and conclusions reached or other errors that may have occurred during the review process. Supervisory review is also a direct means of providing important feedback to staff about their work performance.

DOR reported that it relies on taxpayers' protests of disallowed credits and the subsequent review of the disallowed credits by staff in the Tax Conferee Section to ensure that TPS's tax examiners have appropriately identified all issues. Relying on taxpayer protests is not an adequate or sufficient control to ensure quality in DOR's decision making. In particular, not every taxpayer whose credit may have been inappropriately disallowed will spend the additional time and money to protest the disallowance. Moreover, taxpayers are unlikely to protest a tax credit claim that may have been inappropriately allowed in their favor. DOR has a responsibility to implement controls to ensure a complete, accurate, and consistent review and appropriate decision making on all claims.

Recommendation No. 2:

The Department of Revenue (DOR) should ensure that its review of conservation easement tax credits claims is consistently applied and that the resulting decisions to allow or disallow claims are appropriate and substantiated by:

a. Developing and utilizing a standard work program or review tool to guide and document tax examiners' review of conservation easement tax credit claims.

b. Developing more complete and detailed written policies and procedures for reviewing conservation easement tax credit claims, including how reviews should be documented.

c. Instituting a quality review process whereby a supervisor and/or quality control staff routinely reviews a sample of conservation easement tax credit claim reviews completed by tax examiners. Supervisors and quality control staff performing the reviews should receive training to maintain at least a basic level of competency with the conservation easement tax credit and related issues.

Department of Revenue Response:

a. Agree. Implementation date: July 2013.

   DOR has further developed its checklists for employees to use as part of the Level 1 and Level 2 reviews of conservation easement tax credits and is currently updating these checklists to ensure that Recommendation No. 1 of the State Auditor's report be included.

b. Agree. Implementation date: July 2013.

   DOR will develop more complete and detailed written policies and procedures for reviewing conservation easement tax credit claims which will reference the checklists and their use as well as any additional documentation requirements.

c. Agree. Implementation date: July 2013.

   DOR currently sends cases with which it has concerns to the Division of Real Estate and the Conservation Easement Oversight Commission as part of its quality review process and will continue to do so. In addition, DOR will review its current staffing assignment of tax

examiners and identify changes to be made which will result in routine supervisory reviews of tax credits which have been both disallowed and not disallowed.

Information Management

Information management represents the ability to routinely compile, track, analyze, and report on key programmatic data in a manner that informs decision making, facilitates reporting to stakeholders and policy makers, enables internal and external monitoring and evaluation, and supports the achievement of program goals and objectives. Good information management practices are critical for the effective administration of the conservation easement tax credit.

In 2007, TPS developed an internal database where information related to conservation easement tax credit claims, uses, and transfers is kept. The TPS database is a primary resource for tax examiners' review of tax credit claims and for compiling, tracking, and reporting on credit availability and use on a taxpayer-specific basis and in the aggregate. DOR also works with the Governor's Office of Information Technology (OIT) to administer and oversee GenTax, which is the State's tax processing system for income and business taxes.

The TPS database consists of one large data table and is therefore more similar to a spreadsheet than a relational database. (A relational database stores and organizes data across multiple data tables that allow data to be linked, accessed, or queried in many different ways without having to reorganize or sort the underlying data.) Each time a donor or transferee uses a tax credit, a separate record is entered into the TPS database with the associated tax year. Thus, a single tax credit claim could have multiple records in the database. As of March 2012, the TPS database included approximately 21,460 individual records. To identify which credit is being used, each taxpayer record includes a donation number that identifies a specific conservation easement tax credit. However, the database does not have separate records or data tables for tax-credit-specific information, such as the total credit amount, donation date, donated value, county, parcel location, or conservation easement holder. Because the database is structured in this way, TPS staff must follow specific procedures when entering data. Tax-credit-specific information is included as part of the donor record for the year in which the tax credit was claimed.

The purpose of our audit was not to assess controls over DOR's information technology systems. Thus, we did not perform comprehensive testing of the TPS database or information in GenTax. However, we obtained and analyzed data from the TPS database to report background information on basic trends in conservation easement tax credit claims (see Chapter 1). As discussed earlier in

this chapter, we also conducted a file review for 10 sampled conservation easement tax credit claims, which required us to work with information maintained in the TPS database and GenTax. Overall, through our audit work in these areas, we identified concerns related to the completeness and accuracy of tax credit data maintained in the TPS database.

Incomplete Data

We found that data on conservation easement donations and tax credits are likely to be incomplete because of delays entering information into the TPS database. First, the list of donations and credits claimed are not up to date. The tax credit must always be claimed by the landowner in the tax year in which the donation is made. Specifically, Form DR1305 must be attached to any Colorado income tax return that claims or uses a conservation easement tax credit. However, DOR's current process does not capture data from Form DR1305 for entry into the TPS database if there is no corresponding *use* of the credit in that same year by either the donor or a transferee. For example, DOR may receive a claim from a donor for Tax Year 2010. Yet if the donor does not use the credit to offset a tax liability until Tax Year 2012, the claim would not be entered into the TPS database until the donor's 2012 tax return is processed.

Second, we found that even when the tax credit is used to offset a tax liability, the use is not entered timely. At the beginning of our audit fieldwork, in February 2012, TPS staff reported having completed all reviews for Tax Year 2010; however, staff estimated that they had only entered approximately one-third to one-half of the conservation easement credits and associated taxpayer information into the TPS database.

Inaccurate Data

As mentioned previously, we did not perform comprehensive testing of all records in the TPS database. However, while working with the TPS database to pull our sample of 10 tax credit claims and conduct our file review, we found several examples of inaccurate data in the database.

- **Donation Numbers.** The donation number should be a unique identifier for each conservation easement tax credit so that all taxpayer records associated with a single credit can be sorted and grouped together. However, we identified 171 records in the database for donors and transferees that had a donation number of "0"; 11 donations that were incorrectly assigned the donation number for another donation; and six donations that were entered more than once under a different donation number.

- **Total Credit Amounts.** Because the TPS database does not have any tax-credit-specific records and there are multiple donor and transferee records, TPS's procedures require that tax-credit-specific information, such as the total credit amount, be entered only once into the donor record for the year in which the tax credit was claimed. However, we identified seven donations for which the total credit amount was entered in both donor and transferee records. For two of these donations, the credit amount in the transferee record was different from the credit amount in the donor record. As a result of these duplicate and erroneous entries, a report on the total credit amount across these seven donations could be overstated by as much as $3 million. We identified two additional credits for which the total credit amount was entered for the wrong tax year.

- **Dates.** Credit claims for donations are supposed to be submitted in the tax year in which the conservation easement donations occurred and should be accurately reflected in the database. We found three donations for which the donation year and tax year for the claim did not match. These errors may have resulted from data entry errors and/or tax examiners not catching taxpayer errors, such as taxpayers mistakenly submitting the claim in the wrong tax year or incorrectly filling out their forms. In the first case, the donation was made in 2008 but was entered in Tax Year 2009 in the database. In the second case, the donation date was entered incorrectly in the database. In the third case, the same 2009 donation was entered in both Tax Years 2009 and 2010 and under different donation numbers.

- **Social Security Numbers/Account Identifiers.** Social security numbers or other account identifiers (e.g., Colorado Account Number) are used to uniquely identify individual and corporate taxpayers, which is important when matching taxpayer records between the TPS database and other systems such as GenTax. However, in working with OIT to pull information from GenTax, OIT informed us that some of the social security numbers and account identifiers from the TPS database appeared to be missing the leading zero (e.g., 012-34567 would be listed as 12-34567). Missing the leading zero can create mismatched records when trying to match or merge data across separate systems. We also found 45 records in the TPS database that had no social security number or account identifier (i.e., the field was blank), and one record for which this field was entered as "0."

Incomplete and inaccurate data in the TPS database could have negative effects in a couple of different ways. First, these issues add to the risk that DOR could inappropriately allow or disallow uses of the conservation easement tax credit.

Specifically, TPS's tax examiners rely on information in the database to evaluate compliance with various requirements, including that (1) donors do not claim more than one conservation easement tax credit at a time, (2) uses of the tax credit by donors and transferees do not exceed the total amount of the credit claim for the donation, and (3) all uses of the tax credit by donors and transferees are disallowed when the credit is disallowed.

Second, incomplete and inaccurate data limit DOR's ability to report aggregate information about conservation easement tax credits to the General Assembly and the public effectively. As a result of the delays entering data into the TPS database, DOR does not have a complete record of those tax credits that have been claimed but not used. However, having a current record of all conservation easement tax credits that have been claimed is important for establishing the total amount of state income tax revenues that could be foregone over the life of the credits, the amount already used, and the amount potentially still outstanding. Information in the TPS database also supports some of DOR's other statutory reporting requirements to the Joint Budget Committee and the House and Senate Finance Committees.

Controls Over Data

Overall, DOR has not created and maintained a database or system that effectively supports its administration of the conservation easement tax credit. First, the TPS database is not structured or designed properly to ensure the accuracy and integrity of information about the conservation easement donations and tax credits. As described earlier, the database structure is one large data table listing donors' and transferees' *uses* of the credits by tax year. There are no separate records or data tables for tax-credit-specific information. At a minimum, designing the database as a relational database with separate data tables for recording certain classes of information (e.g., tax-credit-level, taxpayer-level, credit-transaction-level information) could have helped prevent the data accuracy problems we found.

Second, DOR's data entry procedures do not ensure that the data are complete and as up-to-date as possible. As discussed previously, DOR does not capture tax credit claim information for entry into the TPS database when donors file a claim for the credit without a corresponding use of the credit by either the donor or a transferee. Also, TPS's tax examiners do not enter information into the TPS database as they are performing their reviews; rather, staff wait until all of the reviews are completed and then go back and perform data entry as they have time.

Third, TPS lacks sufficient data entry controls, which are important for preventing data inaccuracies from being introduced into the database in the first place. For example, if the tax credit is new and has not already been entered into the

database, TPS staff have to manually assign a new donation number to each claim and associated donor and transferee records. However, the problems we found with donation numbers suggest that DOR needs to provide more guidance and training to staff on how to identify whether or not a tax credit claim is already in the database, ensure that donation numbers are included with each record, and prevent assignment of the same donation number to different tax credit claims. Additionally, the TPS database does not require staff to enter information into certain fields or include other built-in edit checks to ensure that dates and other numeric fields are entered properly.

Finally, TPS does not regularly examine and clean its data. Data cleanup procedures that help with identifying and correcting data inaccuracies could include reviewing a sample of files entered into the database as well as running queries and reports to identify data anomalies, such as blank fields, out-of-range dates, data inconsistencies (e.g., donation year and tax year for the claim do not match), credits claimed that exceed allowable amounts, and duplicate donation numbers.

Recommendation No. 3:

The Department of Revenue (DOR) should ensure that its electronic data and information management systems effectively support the administration of the conservation easement tax credit by:

a. Utilizing a relational database to manage data at the donation and taxpayer levels in a manner that captures the complexity of the tax credit claims and uses over time. As part of this process, DOR should migrate the existing TPS data to a relational database.

b. Capturing data from Form DR1305 for all conservation easement tax credit claims in the year in which the claim is made, regardless of when the use of the credit occurs. Tax examiners should enter data on uses of the tax credit as they perform their reviews.

c. Instituting appropriate data entry controls to help prevent data inaccuracies, and routine cleanup procedures to help identify and correct any data inaccuracies that do occur.

Department of Revenue Response:

a. Agree. Implementation date: December 2013.

DOR will determine the options available with the primary focus being on incorporating the TPS database into our existing tax system, GenTax. Once all feasible options are determined, they will be reviewed and the most cost-effective option will be implemented.

b. Agree. Implementation date: December 2013.

DOR will enter information from Form DR1305 into the applicable database as identified in subpart (a) of this recommendation at the time returns are received from taxpayers, which will ensure data are captured more quickly and will eliminate the need for tax examiners to perform data-entry functions to any separate database.

c. Agree. Implementation date: December 2013.

Because DOR will change how and when data are entered into the applicable database as identified in subparts (a) and (b) of this recommendation, existing data-entry controls instituted by its data entry unit within the Central Department Operations Division will help prevent data inaccuracies. In addition, DOR will review data entered on a quarterly basis as reports are generated from the applicable database as identified in subpart (a) of this recommendation to be used in preparing statutorily required reports.

CEOC Consultations

State statute establishes the nine-member CEOC as part of an overall administrative process for ensuring the validity of conservation easement tax credits claimed by taxpayers. Specifically, Section 12-61-721(3)(a), C.R.S., states:

"The [CEOC] shall advise [DRE and DOR] regarding conservation easements for which a state income tax credit is claimed pursuant to section 39-22-522, C.R.S. At the request of [DRE or DOR], the [CEOC] shall review conservation easement transactions, applications, and other documents and advise [DRE and DOR] regarding conservation values consistent with section 170(h) of the federal 'Internal Revenue Code of 1986,' as amended, the

> capacity of conservation easement holders, and the integrity and accuracy of conservation easement transactions related to the tax credits."

Additionally, Section 39-22-522(3.5)(a), C.R.S., states:

> "In resolving disputes regarding the validity or the amount of a credit…, including the value of the conservation easement for which the credit is granted, the [DOR] executive director shall have the authority, for good cause shown and in consultation with [DRE] and the [CEOC]…, to review and accept or reject, in whole or in part, the appraisal value of the easement, the amount of the credit, and the validity of the credit based upon the internal revenue code and federal regulations in effect at the time of the donation."

The CEOC meets on at least a quarterly basis, and its meeting agendas typically include conservation easement transactions that are the basis for a tax credit claim and for which DOR has requested a consultation. As of January 2012, there were a total of 668 formal consultations between DOR and the CEOC. Of these 668 consultations, 41 (6 percent) consultations involved conservation easement transactions that occurred in 2008 or later. For these 41 consultations, our analysis showed that the CEOC recommended rejecting the tax credit claims for 20 transactions (49 percent) and accepting the tax credit claims for 19 transactions (46 percent). In the remaining two transactions (5 percent), the CEOC did not make a formal recommendation to accept or reject the associated tax credit claims.

During the consultation process, DOR provides available documentation, such as the appraisal report and deed of conservation easement, to the CEOC members in advance of the meeting. Because of confidentiality requirements for individual tax matters, the CEOC meets in executive session to discuss the specifics of each referred case, which may include issues regarding the appraisal methodology and valuation or the legitimacy of the donation's conservation purpose. The CEOC votes in open meeting to recommend that DOR accept or reject the credit claim. DOR is under no obligation to adhere to the CEOC's recommendations. In addition to the CEOC's review, DRE's staff appraiser conducts a separate review of the appraisal for each conservation easement transaction that DOR refers for consultation to determine whether there appear to be material violations of the Uniform Standards of Professional Appraisal Practice (USPAP) that could adversely impact the appraiser's analyses and conclusions and, therefore, the valuation of the land being donated.

One of the objectives of our audit was to determine whether DOR's consultation with DRE and the CEOC provide adequate support for decision making about conservation easement tax credit claims. To address this objective, we observed two CEOC meetings and listened to audio recordings of one additional CEOC

meeting related to our sampled tax credit claims. We also reviewed the CEOC's written orientation manual and interviewed all members of the CEOC as well as DRE and DOR management and staff about the CEOC's advisory role and the consultation process. Finally, we compiled and analyzed data on the CEOC's recommendations regarding the 41 conservation easement transactions occurring since 2008 that DOR referred for consultation as of January 2012.

Conservation easement transactions can be complex and nuanced. Overall, we found that the CEOC plays an important role in providing necessary expertise and stakeholder perspectives when scrutinizing conservation easement transactions for which tax credits are claimed. However, as described in the following sections, in practice, there is a misalignment in two key areas that we believe limits the CEOC's ability to effectively fulfill the purpose for which it was created, which is to help inform and facilitate DOR's decision making to allow or disallow tax credit claims.

Substantive Versus Strict Compliance

CEOC members differ from one another on what motivates their individual votes. However, we found that the CEOC as a whole tends to take a *substantive* compliance approach when reviewing conservation easement transactions that DOR refers for consultation. That is, when making recommendations to DOR, the CEOC's collective vote is generally more reflective of whether the conservation easement transaction overall is legitimate (e.g., the easement has a valid conservation purpose, the appraisal does not appear to be grossly inaccurate or purposefully misleading, the holder is a qualified organization) and the landowner has made a good faith effort to comply with applicable requirements, rather than whether the landowner has complied with each specific statutory and regulatory requirement. Overall, the CEOC appears to prefer the substantive compliance approach when reviewing appraisals.

Our analysis showed that the CEOC recommended approving the tax credit claim for 19 (46 percent) of the 41 conservation easement transactions occurring since 2008 that DOR referred for consultation as of January 2012. However, for 8 (42 percent) of these 19 transactions, the CEOC recommended accepting the tax credit claim despite DRE's opinion that there appeared to be material USPAP violations in the appraisal that could affect the valuation of the land being donated. For example:

- In one of our sampled cases, DRE's staff appraiser reported to the CEOC that there may be material USPAP violations in the appraisal. Specifically, the appraisal did not mention a number of other conservation easements in the area that could have been used to help establish the value opinion, the appraisal did not consistently adjust the value of comparable properties for

improvements on those properties, and the appraiser did not obtain title documentation for the property to determine whether there were any other encumbrances on the property, such as mineral rights or grazing leases. DRE's staff appraiser reported that these steps are standard practice for conservation easement appraisals and their omission could affect the value opinion. During the discussion, CEOC members voiced their opinions that the appraised value seemed reasonable and that this was a great piece of land that would be good to conserve. The CEOC voted unanimously to recommend approval of the tax credit. DOR ultimately denied this tax credit claim, citing problems with the appraisal.

We inquired with CEOC members about how they approach the consultation process in this type of situation. During our interviews, none of the CEOC members disputed the importance of the appraisal for substantiating the conservation easement transaction and the value of the tax credit. However, four CEOC members specifically reported that if the conservation purpose is sound, DOR should not disallow tax credit claims based on a problematic appraisal when a revised appraisal likely would not bring the fair market value of the donated easement low enough to reduce the amount of the credit claim. For example, in the case of an appraisal with apparent USPAP violations that values a conservation easement donation at $2 million, the total tax credit the landowner could claim is $375,000. Even if the landowner obtains a second appraisal without apparent USPAP violations that reduced the fair market value of the conservation easement donation by half to $1 million, the total tax credit the landowner could claim would still be $375,000. Thus, the position of these four CEOC members is that there is no net benefit to the State in disallowing the credit and requiring a second appraisal in such a case.

We understand the logic of the argument advanced by some of the CEOC members. However, we find the argument to be problematic because, in effect, it holds appraisals of higher-value donations to a lesser standard and fundamentally does not help to address the issue of overvalued conservation easement appraisals that House Bill 08-1353 was intended to fix. To ensure consistent application of the tax laws, conservation easement appraisals must be held to the same standards regardless of the value of the donation or the resulting tax credit. Additionally, it is important to recognize that valuation problems with a conservation easement appraisal could have a secondary negative effect if the appraisal is subsequently included in a comparable sales analysis as part of an appraisal of another property.

Although a particular piece of land may be desirable for a conservation easement, this does not mean that the transaction qualifies for claiming a tax credit. It is not necessarily problematic that the CEOC considers substantive aspects of conservation easement transactions as part of the consultation process. However, when making recommendations to accept or reject a tax credit claim, the CEOC

needs to understand that DOR, as the agency responsible for administering Colorado's tax laws, must apply the tax code consistently for all taxpayers and follow a *strict* compliance approach when determining whether taxpayers meet the statutory and regulatory requirements for claiming and using the credit. To do otherwise would undermine the assurances and safeguards that these requirements are intended to provide.

Landowner Versus General Taxpayer Perspective

As noted previously, CEOC members differ from one another on what motivates their individual votes. However, we found that the overall tenor of the CEOC's deliberations tends to focus more on the landowner's perspective than on its broader responsibility to the general taxpayer, which is to help ensure that conservation easement tax credits claimed are valid. Specifically, we found that this landowner-centered perspective was prevalent during the CEOC meetings we observed and the audio recordings of meetings we listened to, as well as during our interviews with some of the CEOC members. Additionally, DRE and the CEOC created a written orientation manual to help CEOC members understand their roles and responsibilities as well as other administrative processes. The manual states: "In all decisions [the CEOC] makes, the interest of the public should be paramount. *In particular, the Colorado landowner who wishes to preserve a piece of their land in a sound and secure conservation easement*" (emphasis added).

By statute, the CEOC membership is structured to include a number of different stakeholders (e.g., local land trust, state or national land trust, local government open space or state conservation agency, historic preservation organization, a landowner). At the CEOC's June 2012 meeting, the CEOC members spent time describing their organizations. During this discussion, one of the CEOC members described how their organization assisted landowners with conservation easement transactions, including the need to "protect landowners from DOR." This member was not speaking about the CEOC's official role when making this comment, nor is it necessarily indicative of all CEOC members' perspectives. Nonetheless, it is concerning that a member of the CEOC brings such a perspective to a consultation process that, by its very design, is intended to inform and facilitate DOR's decision making about tax credit claims. It is reasonable that the landowner perspective be considered when evaluating conservation easement tax credit claims referred for consultation. However, statute does not establish the CEOC as a landowner advocate.

Improving Communication and Common Understanding

All of the CEOC members acknowledged that the CEOC's role is advisory. However, the problems we identified are the result of an overall lack of

communication and common understanding about the purpose and goals of the consultation process. Ultimately, the consultation process should further the State's ability to determine whether landowners have complied with the statutory and regulatory requirements for claiming a conservation easement tax credit.

The CEOC held its first meeting in September 2008, and formal consultations with DOR began in October 2010. During our audit, DOR and DRE staff and CEOC members reported that communication between DOR and the CEOC has been strained for a number of years. CEOC members generally reported that DOR does not have an understanding and appreciation for the substantive aspects of conservation easement transactions or the landowner's perspective. DOR management and staff reported that the CEOC does not have an understanding and appreciation for the compliance requirements that DOR must strictly apply and adhere to when reviewing tax credit claims.

Recently, at the CEOC's June 2012 meeting, DOR and the CEOC began to address the lack of common understanding about the purpose and goals of the consultation process by directly communicating with one another about their respective roles and responsibilities. In particular, at this meeting, DOR staff explained internal procedures for processing taxes, including the need to take a strict compliance approach when reviewing tax credit claims. CEOC members provided information about the organizations they represent and their individual areas of expertise related to conservation easements. This level of communication has been lacking in the past and needs to continue.

In addition to communicating about processes, roles, and responsibilities, more communication is needed with respect to the tax credit claims that are referred to the CEOC for consultation. Currently, DOR does not detail why it refers tax credit claims to the CEOC. Thus, CEOC members do not always have a clear understanding about DOR's concerns with the transaction. CEOC members reported that knowing the basis for the consultation would help target their review efforts and ensure that DOR gets what it needs from the consultation. CEOC members also reported it would be beneficial to learn about the outcomes of the consultations (i.e., whether DOR allowed or disallowed the tax credit claim) as a means of improving the advice the CEOC provides to DOR. Additionally, we noted that there is little routine discussion among DOR, DRE, and the CEOC about the overall trends and issues being seen with conservation purposes, conservation easement appraisals, and landowner compliance with the statutory and regulatory requirements for claiming the conservation easement tax credit. This type of broader discussion can be helpful for informing discussions about specific tax credit claims.

Finally, the characterization of "the public interest" as it is currently outlined in the CEOC's written orientation manual falls too much on the side of the

landowner and lacks proper balance with the CEOC's broader responsibility to help ensure the validity of conservation easement tax credits being claimed by landowners. Also absent from the orientation manual is a specific acknowledgment that the CEOC's consultations are intended to help determine whether landowners have complied with the statutory and regulatory requirements for claiming the conservation easement tax credit and, therefore, inform and facilitate DOR's decision to allow or disallow tax credit claims.

Recommendation No. 4:

The Department of Revenue (DOR), the Division of Real Estate (DRE), and the Conservation Easement Oversight Commission (CEOC) should improve communication efforts and continue to build a common understanding about the purpose and goals of the consultation process. This should include using the consultation process to hold routine discussions about the general issues and trends being observed with conservation easement transactions associated with tax credit claims.

Department of Revenue Response:

Agree. Implementation date: June 2012 and Ongoing.

DOR is currently working on improving its communication with DRE and the CEOC. DOR, DRE, and the CEOC will continue this effort by changing and formalizing the consultation process to be more useful to DOR and to better utilize the expertise of DRE and the CEOC in determining whether taxpayers have complied with the requirements for claiming a conservation easement tax credit.

Division of Real Estate Response:

Agree. Implementation date: June 2012 and Ongoing.

DRE has worked over the past two years to improve communication, understanding, and cooperation between DOR and the CEOC. These efforts have proven fruitful and will continue through informal discussions between staff and at CEOC meetings. Specifically, DRE will work with DOR staff to identify a process in which the two agencies will routinely discuss issues. Issues will then be brought to the CEOC for input at regularly scheduled meetings. DRE will work with DOR and the CEOC to increase the effectiveness and efficiency of the consultation process.

Conservation Easement Oversight Commission Response:

Agree. Implementation date: June 2012 and Ongoing.

The CEOC is committed to continuing to work to improve communication with DOR and DRE to build a common understanding about the purpose and goals of the consultation process. Discussions about conservation issues and trends should include concerns identified by the CEOC, including the cost to the State of legal expenses and staff time pursuing tax credit claims that the CEOC believes are appropriate. The CEOC has recommended disallowance of more than 600 conservation easement tax credits and strongly supports disallowances where parties have abused the law. However, the CEOC strongly believes that sound, legitimate conservation easement tax credit claims are being disallowed based upon strict and perhaps unrealistic standards. Finding a way to address this concern as the consultation process moves forward will be an important part of the CEOC's ongoing communication efforts with DOR and DRE.

Auditor's Addendum

Some of the views expressed by the CEOC in its response, such as the need to review State legal expenses and staff time related to the review of conservation easement tax credit claims and to address the CEOC's perception that legitimate tax credit claims are being disallowed based on strict and unrealistic standards, go beyond the scope of the CEOC's statutory responsibilities. Section 12-61-721(3)(a), C.R.S., states:

> *"At the request of [DRE] or [DOR], the [CEOC] shall…advise [DRE] and [DOR] regarding conservation values…, the capacity of conservation easement holders, and the integrity and accuracy of conservation easement transactions related to the tax credits."*

The requirements for claiming a conservation easement tax credit are clearly established in federal and state statutes and regulations, and legitimate conservation easement tax credit claims are those that comply with these statutory and regulatory requirements.

Recommendation No. 5:

The Department of Revenue (DOR) should provide the Conservation Easement Oversight Commission (CEOC) with more information, such as areas of concern or specific questions that need to be addressed, when referring individual

conservation easement tax credit claims to the CEOC for consultation. DOR should also communicate its final decisions to allow or disallow tax credit claims that are referred for consultation.

Department of Revenue Response:

Agree. Implementation date: December 2012.

DOR will provide more information to the Division of Real Estate (DRE) and the CEOC regarding DOR's specific questions and concerns about appraisals and/or deeds submitted for consultation. DOR will also provide information on a quarterly basis to DRE and the CEOC about DOR's actions on cases previously submitted for consultation.

Recommendation No. 6:

The Division of Real Estate (DRE) and the Conservation Easement Oversight Commission (CEOC) should revise the CEOC's written orientation manual to better address the CEOC's broader responsibility to the general taxpayer when defining "the public interest." The manual should explicitly recognize that the consultation process should further the State's ability to determine whether the landowner has complied with the statutory and regulatory requirements for claiming the conservation easement tax credit.

Division of Real Estate Response:

Agree. Implementation date: March 2013.

DRE will work with the CEOC to review and revise the written orientation manual to further define the responsibility that CEOC members have to the general taxpayers as part of the duty to protect the public interest. Revisions will include a discussion of the role the CEOC plays in the consultation process and how the CEOC will further the State's ability to determine compliance with statutory and regulatory requirements. DRE staff will prepare recommended changes for discussion at the December 3, 2012 CEOC meeting. Additionally, DRE staff and the CEOC's legal counsel will review the responsibilities and roles of CEOC members at the yearly CEOC retreat taking place in the first quarter of 2013.

Conservation Easement Oversight Commission Response:

Agree. Implementation date: March 2013.

The CEOC will revise the written orientation manual, which was written prior to consultation with DOR, to address the CEOC's role in the consultation process. The CEOC was created by statute to advise DRE and DOR on conservation easement transactions. When advising these agencies the CEOC tries to protect the financial interest of all taxpayers, including those who donate conservation easements. A designated seat on the CEOC for a landowner/donor supports the CEOC's position that part of its responsibility is to consider the landowner perspective. The CEOC represents various stakeholders with significant expertise on conservation easement transactions, and its members believe it is appropriate for the CEOC, in its advisory capacity, to question the basis for DOR's and DRE's decisions and to ensure that all perspectives are considered. The CEOC will continue to use its diverse expertise and the various member perspectives (e.g., state agencies, a local government, land trusts, and a landowner) to advise both the DOR and DRE on all aspects of conservation easement transactions associated with tax credit claims.

Auditor's Addendum:

Some of the views expressed by the CEOC in its response, such as questioning the basis for DOR's and DRE's decisions, go beyond the scope of the CEOC's statutory responsibilities. Section 12-61-721(3)(a), C.R.S., states:

> *"At the request of [DRE] or [DOR], the [CEOC] shall…advise [DRE] and [DOR] regarding conservation values…, the capacity of conservation easement holders, and the integrity and accuracy of conservation easement transactions related to the tax credits."*

We acknowledge that CEOC members represent a number of different interests, including landowners donating conservation easements. However, none of these interests should take priority over the CEOC's broader responsibility to help ensure the integrity and accuracy of conservation easement transactions related to tax credits being claimed by taxpayers.

Review of Conservation Easement Appraisals

To claim a conservation easement tax credit, the fair market value of the conservation easement donation must be established by a qualified appraisal completed by a qualified appraiser no more than 60 days prior to the donation and no later than the due date of the donor's tax return. Fundamentally, the fair market value of a conservation easement is what drives (1) the financial benefit the taxpayer receives by claiming the tax credit and (2) the corresponding loss in tax revenue for the State. Thus, without an appraisal that uses a sound methodology in accordance with applicable professional standards, the State lacks assurances that the dollar value of any tax credit claimed by the taxpayer is reasonable and appropriate.

As discussed in Chapter 1, the General Assembly enacted House Bill 08-1353 during the 2008 Legislative Session, in part to help ensure the validity and proper valuation of conservation easements that are donated by landowners and used as the basis for claiming a tax credit. Specifically:

- Section 12-61-719(1), C.R.S., requires any appraiser who conducts an appraisal for a conservation easement to submit a copy of the completed appraisal to DRE within 30 days following the completion of the appraisal. Conservation easement appraisal reports must be submitted to DRE regardless of whether a tax credit will be claimed. The appraiser also must complete and submit an affidavit that (1) attests to certain specific appraisal values (e.g., the unencumbered land value, the total easement value, values for minerals), (2) describes the ownership of nearby land parcels, and (3) provides details of the appraiser's licensure status and compliance with continuing education requirements.

- Section 12-61-719(3), C.R.S., requires DRE to review submitted conservation easement appraisals and corresponding affidavits for completeness and to track the affidavit information in an electronic database. As mentioned previously, DRE conducts a separate review of the appraisal for each conservation easement transaction that DOR refers to the CEOC for consultation.

The General Assembly also authorized DRE to charge an administrative fee, thereby providing a dedicated revenue source to cover the cost of DRE's appraisal review activities. The amount of the fee is determined by DRE. Currently, appraisers pay a $265 fee for each conservation easement appraisal they submit to DRE.

Appraisal Review Process

DRE has established a review process for the conservation easement appraisals it receives. First, DRE staff review the appraisal and corresponding affidavit to ensure they are complete and enter basic information, such as the names of the appraiser and the conservation easement holder, the county of the donation, and the easement's acreage and fair market value, into a spreadsheet. At this point, DRE staff verify that the appraiser is licensed and has attested to completing the continuing education requirements. DRE also retains an electronic copy of the appraisal report and completed affidavit.

Second, DRE staff select some conservation easement appraisals to undergo a more in-depth desk review by DRE's staff appraiser. Appraisals are selected for desk review based on several different risk factors, including whether the appraisal will be used to substantiate a tax credit claim, the appraiser has had practice problems in the past, or the conservation easement donation is part of a phased transaction. It is important to note that appraisals are only opinions of value and that values may vary depending on the appraiser and his or her methodology. DRE's staff appraiser reviews the appraisal *methodology* but does not determine whether the appraiser's value opinion is "correct." To do so would require another independent appraisal for the property. Examples of potential USPAP violations and other concerns that have been identified through DRE's desk review include failing to take into account an adjacent property; evaluating the wrong property; using inappropriate comparable properties to establish a possible sale value; failing to take into account the zoning uses for the property; and inflating the value of the property resources, such as gravel and water, without taking into account the cost and likelihood of extracting these resources.

Finally, if DRE's staff appraiser identifies any significant concerns with a conservation easement appraisal, such as a potential licensure or USPAP violation, the matter is referred as a complaint to DRE's enforcement section for investigation. DRE enforcement staff conduct an investigation and present the findings and conclusions to the Board of Real Estate Appraisers (BOREA), which has the authority to take disciplinary action against the appraiser. If, as the result of an investigation, BOREA determines that a material USPAP violation or a substantial misstatement of value has occurred, Section 12-61-719(5), C.R.S., requires that DOR be notified and provided with a copy of the conservation easement appraisal and a summary of findings.

One of the objectives of our audit was to determine whether DRE's process for reviewing conservation easement appraisals is sufficient to ensure that appraisals used to substantiate tax credit claims are performed by licensed appraisers and adhere to applicable professional standards and that any violations are communicated to DOR. To address this objective, we analyzed data on all

conservation easement appraisals submitted to DRE since 2008. We also reviewed a nonstatistical judgmental sample of 10 conservation easement appraisals and related documentation that were submitted to DRE between April 2009 and December 2010 and were specifically related to a conservation easement tax credit claim filed in Tax Years 2009 or 2010. We selected our sample items to provide representation of conservation easement appraisals that DRE subjected to a desk review, as well as conservation easement appraisals that DRE did not subject to a desk review.

DRE reported that its appraisal review process is intended to try to identify and address problematic conservation easement appraisals before a tax credit is claimed. However, we identified problems with DRE's review process that limit DRE's ability to accomplish this goal effectively.

- **Not all conservation easement appraisals undergo a desk review.** Although all conservation easement appraisals submitted to DRE undergo a basic review for completeness to ensure that all of the necessary documents are submitted, we found that not all conservation easement appraisals undergo a more in-depth desk review by DRE's staff appraiser. Specifically, only 286 (31 percent) of 919 conservation easement appraisals have had a desk review since DRE started receiving conservation easement appraisals in July 2008. The percentage of conservation easement appraisals undergoing a desk review also varies significantly from year to year, ranging from a low of 17 percent in 2009 to a high of 42 percent in 2011.

Conservation Easement Appraisals Received and Reviewed by the Division of Real Estate
(As of July 31, 2012)

Calendar Year[1]	Conservation Easement Appraisals Received[2]	Desk Review Performed	
		Count	Percent of Total
2008	105	41	39%
2009	253	44	17%
2010	243	73	30%
2011	224	93	42%
2012	94	35	37%
Total	**919**	**286**	**31%**

Source: Office of the State Auditor's analysis of the Division of Real Estate's conservation easement appraisal log.

[1]Only partial year data are reflected for 2008 and 2012. The Division of Real Estate started receiving conservation easement appraisals effective July 1, 2008, and we pulled data from the Division of Real Estate's appraisal log through July 31, 2012.

[2]Not all conservation easement appraisals received by the Division of Real Estate were related to a potential tax credit claim.

DRE reported that it attempts to conduct a desk review of as many conservation easement appraisals as possible and that in recent years it has prioritized its review efforts on appraisals supporting tax-credit-generating conservation easements. Starting in February 2009, DRE began identifying which conservation easement appraisals were likely to support a tax credit claim and the estimated tax year of the claim.

To provide an analysis of DRE's prioritization efforts, we limited our analysis to those conservation easement appraisals that DRE determined would likely be used to substantiate a tax credit claim. We also grouped the data based on the estimated tax year for the claims as determined by DRE. This analysis shows that only 223 (46 percent) of 483 tax-credit-generating conservation easement appraisals had a desk review, with the year-to-year percentages varying significantly from a low of 26 percent in 2010 to a high of 95 percent in 2011.

Tax-Credit-Generating Conservation Easement Appraisals Received and Reviewed by the Division of Real Estate
(As of July 31, 2012)

Estimated Tax Year[1]	Conservation Easement Appraisals Received[1]	Desk Review Performed	
		Count	Percent of Total
2009	175	73	42%
2010	155	41	26%
2011	78	74	95%
2012	75	35	47%
Total	**483**	**223**	**46%**

Source: Office of the State Auditor's analysis of the Division of Real Estate's conservation easement appraisal log.

[1]This is the Division of Real Estate's estimate of the tax year for which a tax credit supported by the conservation easement appraisal will be claimed. Figures for 2012 are based on partial year data; we pulled data from the Division of Real Estate's appraisal log through July 31, 2012.

Both of our analyses demonstrate that DRE's coverage of conservation easement appraisals through desk reviews could be improved. Increased coverage is important if DRE's review process is to be effective at identifying and addressing problematic conservation easement appraisals before a tax credit is claimed. For example, we identified one conservation easement appraisal in our sample that did not receive a desk review at the time DRE received the appraisal. However, DOR discovered problems with the appraisal when it reviewed the tax credit claim and requested a review by DRE. DRE conducted an investigation and concluded that "the value opinion may not be appropriate or adequately supported given the

data and analysis presented" and that "the appraisal may not meet the requirements defined in the Internal Revenue Code." DRE took disciplinary action against the appraiser, including requiring the appraiser to re-perform and resubmit the appraisals at his own cost. This case also illustrates the efficiencies that could potentially be gained through an up-front desk review by DRE. It is likely that the issues with this appraisal could have been identified and resolved sooner had DRE performed a desk review, as opposed to waiting for DOR to receive a tax credit claim and raise concerns at that point in the process.

- **Not all problems are identified through desk reviews.** As discussed previously, the intent of DRE's appraisal review process is to try to identify and address problematic conservation easement appraisals before a tax credit is claimed. However, even when DRE performs a desk review, we found that not all problematic issues are identified. Of the eight conservation easement appraisals in our sample that underwent a desk review, there was one in which DRE's staff appraiser did not identify any issues warranting further investigation, although it was noted that some information was omitted from the appraisal report. Upon receiving a tax credit claim supported by this appraisal, DOR raised questions about the appraisal and requested a consultation with DRE and the CEOC. During the consultation, DRE's staff appraiser stated that the information omitted from the appraisal report should have been included to support the value conclusions and that the appraisal may have had material USPAP violations. DOR subsequently denied the tax credit, citing problems with the appraisal. The landowner has since protested the denial, and the case is currently with DOR's Tax Conferee.

  We recognize that a desk review is limited only to the information contained in the appraisal report. It is also reasonable that additional questions and concerns may be raised through subsequent reviews and scrutiny by DOR and/or the CEOC that were not initially considered during DRE's desk review. However, at a minimum, the scope of DRE's desk review should be rigorous enough to provide reasonable assurance that it is effectively identifying and referring potential problems for further investigation. Identifying and referring potential problems for further investigation is important because the investigation process is the only means by which DRE and BOREA are able to officially conclude that a material USPAP violation or a substantial misstatement of value has occurred in a conservation easement appraisal.

The fact that not all conservation easement appraisals undergo a desk review and that not all problems with conservation easement appraisals are identified through desk reviews are the result of several factors:

- **Resources.** Despite year-to-year fluctuations in the number of conservation easement appraisals being submitted, DRE only has one staff appraiser assigned to perform desk reviews. From a risk perspective, it is reasonable for DRE to focus its desk reviews on appraisals of tax-credit-generating conservation easements. However, DRE has not obtained or allocated additional resources to perform desk reviews of such appraisals when demand increases. For example, our earlier analysis showed that DRE reviewed about 95 percent of all tax-credit-generating conservation easement appraisals for Tax Year 2011. However, DRE's ability to achieve this higher coverage was largely because its workload decreased. Only about half as many tax-credit-generating conservation easement appraisals were submitted for Tax Year 2011 (78 appraisals) as in the previous two years (155 appraisals in 2010 and 175 appraisals in 2009). Although DRE has had more coverage in recent years, the number of conservation easement appraisals supporting tax credit claims will likely increase once the aggregate cap on the total dollar amount of credits available expires in 2013.

  During our audit, DRE reported that a primary factor affecting its resources and ability to conduct desk reviews of *new* conservation easement appraisals was that, historically, a significant portion of its staff appraiser's time has been spent conducting desk reviews of appraisals referred by DOR. However, as discussed in Recommendation No. 4, as of January 2012, there were a total of 668 formal consultations between DOR and the CEOC and DRE, only 41 (6 percent) of which involved conservation easement transactions that occurred since 2008. Thus, the demand on the DRE staff appraiser's time related to DOR referrals may not be as significant going forward.

  As noted earlier, the General Assembly provided a dedicated source of fee revenue to cover the cost of DRE's appraisal review activities. DRE reported a desire to keep administrative fees as low as possible. We recognize the need to keep fees low; however, DRE should ensure that, at a minimum, all conservation easement appraisals expected to be used to substantiate a tax credit claim undergo a desk review. This may require that DRE adjust administrative fees and work through the state budget process to obtain the additional staff resources necessary (e.g., hiring additional in-house staff appraisers or contracting for appraisal review services) as workload demands change.

- **Formal Procedures.** DRE's conservation easement appraisal review process lacks formal procedural definition. As discussed previously, DRE staff consider a number of different risk factors when selecting appraisals for further desk review, including whether the appraisal will be used to

substantiate a tax credit claim, the appraiser has had practice problems in the past, or the conservation easement is part of a phased transaction. However, none of these risk factors is formally established in policies and procedures. Additionally, DRE does not use a standard review template when it conducts the desk reviews. Thus, it is unclear what attributes of each appraisal should be and are examined during the desk review; the review process is generally only defined by the DRE staff appraiser's individual work practices. Review templates are a basic control for ensuring a consistent review and that all required and/or significant attributes are examined. Review templates also help to document the relevant judgments made and conclusions reached during the review, as well as any subsequent actions taken as a result of the review.

- **Statutory Intent.** State statute is not entirely clear regarding the intended purpose and scope of DRE's review of conservation easement appraisals. In the legislative declaration to House Bill 08-1353, the General Assembly stated its intent that the desired results and benefits of the new requirements were, in part, "to have the division of real estate *review* appraisals of conservation easement and affidavits of appraisers submitted to the division and maintain the information in an electronic database" (emphasis added). Given the issues that precipitated House Bill 08-1353, it appears that the General Assembly intended for DRE to establish a review process that is rigorous enough to identify potential problems with conservation easement appraisals before a tax credit is claimed. However, DRE indicated that the specific requirement put in place by House Bill 08-1353 suggests that the General Assembly intended for DRE's review to be more limited in scope. Specifically, Section 12-61-719(3), C.R.S., states that "[DRE] shall *review* the information submitted…*to ensure that it is complete* and shall record and maintain the information submitted as part of the affidavit in an electronic database" (emphasis added). During our audit, DRE reported that statutory clarification on this issue is important for ensuring that its reviews and resources are aligned with what was intended by the General Assembly.

An up-front desk review of conservation easement appraisals can be an effective and efficient means of identifying and addressing problematic appraisals before a tax credit is claimed. Ensuring that sufficient staff resources are available, review processes are formalized, and the intended purpose and scope of the reviews are clearly defined are all critical to strengthening DRE's conservation easement appraisal review process and gaining the level of assurance over conservation easement appraisals that we believe the General Assembly envisioned by enacting House Bill 08-1353.

Recommendation No. 7:

The Division of Real Estate (DRE) should ensure that the conservation easement appraisal review process is effective at identifying and referring problematic appraisals for investigation before a tax credit is claimed by:

a. Performing a desk review of, at a minimum, all conservation easement appraisals for which a tax credit will be claimed.

b. Developing standard operating procedures that outline the general parameters of the desk review, including the risk factors warranting a desk review and the required and/or significant attributes that should be examined on every desk review.

c. Developing and utilizing a standard review template, or other similar tool, to ensure the consistency and completeness of the desk review and to document the significant judgments made, conclusions reached, and subsequent actions taken.

d. Working with the General Assembly to further clarify in statute the intended purpose and scope of the conservation easement appraisal review requirement.

Division of Real Estate Response:

a. Agree. Implementation date: January 2013.

DRE staff will identify and review all appraisals used to substantiate a tax credit claim. DRE's continued goal is to complete a review of conservation easement appraisals used as substantiation for tax credit claims within the calendar year the appraisal is received by DRE. The ability to accomplish this goal is complicated by limited staff resources, fiscal constraints, difficulties predicting the number of appraisals that must be reviewed, and the additional workload resulting from the consultation process. Despite these complications, DRE has reviewed 95 percent of all appraisals for tax-credit-generating easements in 2011 and has since completed reviews of the remaining four appraisals. DRE will ensure resources are available to effectively administer reviews of all conservation easement appraisals substantiating conservation easement tax credit claims.

b. Agree. Implementation date: January 2013.

DRE will formalize risk factors used to prioritize reviews of conservation easement appraisals. Staff will also develop a procedure that identifies attributes of the appraisal that must be reviewed in every case as well as unique circumstances that require further review. The process will address situations where additional information should be sought as well as the process for referring problematic appraisals for investigation.

c. Agree. Implementation date: January 2013.

DRE will create a new review template allowing for consistent documentation and reporting of review findings. The template will be used in all reviews to ensure the consistency and completeness of reviews and to document conclusions and subsequent actions taken by DRE. It will also allow flexibility in cases where staff reviewers identify unique issues that require additional review or information.

d. Agree. Implementation date: July 2013.

DRE will work with the General Assembly as appropriate to clarify the desired scope and purpose of conservation easement appraisal reviews. Any additional level of review beyond what is recommended in this audit report likely will require the allocation of additional resources. DRE will also address the scope and purpose of appraisal reviews as part of our report to the General Assembly requested in Recommendation No. 11.

Certification of Conservation Easement Holders

As discussed in Chapter 1, state statute requires the holder of a conservation easement to be a governmental entity or a nonprofit organization. Additionally, if a tax credit will be claimed for a donated conservation easement, state statute requires the governmental entity or nonprofit organization receiving the donation to be certified by DRE. The purpose of the certification requirement is to establish minimum qualifications for organizations that hold conservation easements to encourage professionalism and stability and to identify fraudulent or unqualified applicants. Certification, which must be renewed annually, is a key control for ensuring that tax-credit-generating conservation easements are donated to qualified organizations.

As of March 2012, DRE had received a total of 46 completed applications for certification (31 applications from nonprofits and 15 applications from governmental entities); however, only 43 applications were complete. Of the 43 completed applications, DRE certified 37 applicants through its standard certification process. DRE certified the remaining six applicants based on their accreditation by the Land Trust Alliance, which is a national nonprofit land conservation organization that has established standards and practices widely accepted in the conservation and land trust community for the responsible operation of a land trust. State statute [Section 12-61-720(5), C.R.S.] allows for expedited certification of nonprofits and quasigovernmental land conservation entities that are accredited by national land conservation organizations. Currently, there are 42 certified conservation easement holders in Colorado. With the exception of one nonprofit organization that allowed its certification to expire, all other certified holders renewed their certifications for 2012.

Certification Process

State statute [Section 12-61-720(1), C.R.S.] charges DRE with establishing and administering a certification program for organizations that accept tax-credit-generating conservation easement donations. DRE has the authority to (1) determine whether an applicant possesses the necessary qualifications for certification and (2) deny certification or the renewal of a certification if it determines that an applicant does not possess the applicable qualifications for certification or that the applicant has violated any provisions of statute or rules.

Governmental entities and nonprofit organizations applying for certification submit an organizational profile, which includes basic documents about the entity, proof of nonprofit status if the applicant is not a governmental organization, and a list of the conservation easements held by the organization. DRE staff perform a preliminary review of this information to determine whether the applicant generally appears to be eligible for certification. Once the applicant is determined to be generally eligible for certification, DRE staff conduct an in-depth review of a sample of three to five conservation easements held by the organization. Applicants provide DRE with additional documentation for the sampled conservation easements, including appraisal reports, internal checklists, monitoring dates and reports for the previous 3 years, and any known violations of the easements' terms and conditions. Applicants also submit more detailed information about the organization, such as stewardship and selection practices, conflict of interest policies, and other internal policies and procedures.

DRE staff review the application materials and assign one of four ratings—strong response, area for improvement, concern, or critical concern—to 25 different evaluation factors. Staff prepare an evaluation report and submit it to the CEOC and the DRE Division Director. The purpose of the staff evaluation report is to

inform the CEOC and the DRE Division Director about those areas in which the applicant may not be meeting the minimum qualifications. The CEOC reviews and discusses the staff evaluation report before making a recommendation to the DRE Division Director, who makes the final decision to grant or deny certification.

One of the objectives of our audit was to determine whether DRE's process for certifying conservation easement holders is sufficient to ensure that only qualified entities are certified to accept tax-credit-generating conservation easement donations. To address this objective, we reviewed the CEOC's recommendations and the DRE Division Director's certification decisions for all 46 organizations that had applied for certification as of March 2012. We compiled and analyzed DRE staff ratings from all 37 summary evaluation reports (evaluation reports were not completed for the six organizations that received an expedited review). Finally, we conducted a detailed file review of a nonstatistical judgmental sample of 25 certification applications and related documentation. We selected our sample items to provide representation of approved and denied applications, governmental entities and nonprofit organizations, different sized organizations, and organizations located in different areas of the state.

Overall, we found that DRE has an extensive and systematic process for reviewing and evaluating certification applications based on broad principles and best practices that are well established within the land trust community for effective conservation easement stewardship. DRE staff and CEOC members reported that the certification requirements have been effective at eliminating the systematic abuses of the tax credit that existed prior to 2008.

Conditional Certification

DRE's certification process can generally be relied upon to provide positive assurance that the applicant has met all applicable requirements established in statute and rules. In particular, the process appears to be effective at indicating when applicants clearly meet or clearly do not meet the minimum qualifications for certification. However, some applicants fall into a gray area. Historically, DRE has taken one of two approaches to certification in these situations:

- **Certification with Concerns.** According to DRE's rating criteria, a "concern" rating means that DRE staff determined the organization may not be in compliance with a particular certification requirement (e.g., lack of a required policy or failure to implement or follow the policy). Of the 37 organizations DRE certified, we found that 14 received a "concern" rating on at least one of the 25 different evaluation factors. In these cases, DRE fully certified the organizations but required them to provide a detailed description of how each area of concern was addressed—

including all actions taken, by whom, and on what date—before DRE *renewed* the certification. All 11 organizations in our sample that were certified with a "concern" rating responded to the concerns with their subsequent renewal applications.

- **Conditional Certification.** For two applicants in 2010 and one applicant in 2011, DRE denied certification because the organizations had not met the minimum qualifications. For each of these three applicants, DRE staff assigned "concern" and "critical concern" ratings in several areas, and the CEOC also expressed concerns during its discussions that these three organizations were not meeting minimum requirements. These three organizations subsequently reapplied for certification and provided additional information to DRE demonstrating changes they had made, such as new policies and procedures and staff education and training efforts. However, instead of fully certifying these organizations, DRE granted a *conditional* certification and imposed additional requirements for the applicants to achieve full certification. One organization must provide detailed project documentation for the next four conservation easements it accepts, and the easements must be co-held with another certified organization of DRE's choosing. The remaining two organizations must provide detailed project documentation for the next three conservation easements they accept. DRE reported that each of the applicants had policies and procedures that met the minimum qualifications for certification. However, DRE also wanted more assurance that the organizations would be complying with these policies and procedures for new easements.

When a conservation easement holder is certified, DRE is providing positive assurance that the holder has met all applicable requirements established in statute and rules. Although the staff-assigned ratings do not necessarily dictate the final certification decision, on its face it is problematic when DRE fully certifies organizations when the staff-assigned "concern" ratings indicate that minimum requirements may not have been met. DRE is also exposed to criticism that not all applicants are being held to the same certification standards.

The use of conditional certification provides DRE with a more straightforward and effective means of certifying organizations when the minimum requirements may not have been met. In particular, conditional certification is easily distinguished from full certification and clearly indicates there are additional requirements that must be satisfied before the applicant can achieve full certification. However, DRE has not formally established "conditional certification" in rule. Consequently, DRE lacks sufficient authority to set additional requirements on applicants as a condition for certification. Additionally, without establishing conditional certification in rule, it is not

transparent to organizations applying for certification or other agencies, such as DOR, what conditional certification means or those situations or circumstances in which conditional certification is appropriate.

Reviewing an organization's capacity to hold conservation easements is complicated and nuanced. Conditional certification reasonably allows organizations to be certified to accept tax-credit-generating conservation easements while putting additional requirements in place to address those areas where the State needs additional assurance. DRE already uses conditional or probationary licensure in other areas of its regulatory responsibilities (e.g., real estate brokers).

Recommendation No. 8:

The Division of Real Estate (DRE) should strengthen the conservation easement holder certification process by formally establishing "conditional certification" in state rule. This should include specifying the appropriate purpose and use of conditional certification, what evaluation criteria would result in conditional certification versus full certification or denial of certification, and any other administrative requirements that are necessary to implement conditional certification.

Division of Real Estate Response:

Agree. Implementation date: March 2013.

Conditional certification is a useful tool that DRE will work towards formalizing through rule. It provides an additional safeguard ensuring that organizations continue to meet the minimum requirements for certification. DRE will specify criteria used to determine which organizations qualify for conditional certification and any additional requirements they must adhere to. The formalized rule will allow DRE to apply requirements consistently but maintain the flexibility necessary to address the specific concerns identified. Staff drafted a conditional certification rule prior to the initiation of the audit with the intention of formalizing conditional certification. DRE will move forward with adoption of a conditional certification rule in the first quarter of 2013.

Ensuring Long-Term Value and Benefits

According to state statute [Section 39-22-522(2), C.R.S.], the conservation easement tax credit is only allowed for donations that meet the requirements for a qualified conservation contribution under federal laws and regulations. One such requirement is that the donated conservation easement must be perpetual in nature, which is important for protecting and preserving the conservation easement's value and benefit over the long term.

The requirement that conservation easements be perpetual in nature places certain responsibilities on the landowner and the conservation easement holder. Current and future landowners have a responsibility to manage and maintain the property in accordance with the easement's terms and conditions. Conservation easement holders have a responsibility to ensure that landowners abide by the easement's terms and conditions.

State statute [Section 12-61-720(8), C.R.S.] also requires governmental entities and nonprofit organizations accepting conservation easement donations for which tax credits will be claimed to be a certified conservation easement holder at the time of the donation. This certification requirement is intended, in part, to ensure that the governmental entities and nonprofit organizations have strong conservation easement stewardship practices and the capacity (e.g., financial and nonfinancial resources) to maintain, monitor, and defend the purposes of the easements in perpetuity. Thus, the certification requirement is important for protecting the "investment" of public funds in tax-credit-generating conservation easements.

We reviewed the conservation easement holder certification requirements and process and identified two concerns contributing to a lack of assurance that conservation easements will continue to be protected over the long term should the holder no longer be able to meet its responsibilities or remain certified. As discussed in the following sections, we found that (1) DRE's current certification renewal process is insufficient to ensure that conservation easement holders continue to meet certification requirements and (2) the State lacks adequate protections when governmental entities and nonprofit organizations holding tax-credit-generating conservation easements are no longer certified.

Certification Renewal

Governmental entities and nonprofit organizations that wish to continue to accept new conservation easements for which tax credits will be claimed must renew their certification annually. In accordance with state rules (4 C.C.R., 725-4, A-2), certification expires on December 31 following the date of issuance. Certified

holders submit a renewal application to DRE, including a list of any new conservation easements accepted during the previous year, and pay a renewal application fee of $740. As mentioned previously, all but one of the 43 originally certified holders renewed their certifications for 2012.

We reviewed all renewal applications for the 22 certified conservation easement holders in our sample that had applied for recertification as of April 2012. Because of the timing when DRE implemented the certification process, the nonprofit organizations in our sample generally had renewals for 2011 and 2012, and the governmental entities in our sample had renewals for 2012. Overall, we found that the current renewal process is not adequate to ensure that governmental entities and nonprofit organizations that hold tax-credit-generating conservation easements continue to meet the certification requirements. Specifically, DRE does not perform any review of documentation for new conservation easement donations the holder has accepted since being certified.

DRE's lack of a documentation review was of particular concern for those circumstances in which DRE's initial certification review only encompassed conservation easement holders' policies and procedures. State rules require that conservation easement holders must have *and follow* reasonable policies and procedures to ensure compliance with the different certification requirements. However, for 11 of the 22 applicants in our sample with a completed application, the applicants had policies and procedures at the time of initial certification that met the certification requirements, yet the applicants could not demonstrate to DRE that these policies and procedures were being followed. For example, state rules require conservation easement holders to have and follow policies and procedures to receive and review a copy of the appraisal that is used to determine the fair market value of each property. One applicant in our sample had a policy governing the receipt and review of documentation, including the appraisal, supporting each donation. However, the organization was unable to demonstrate its compliance with this policy to DRE at the time of certification. DRE certified this applicant for 2010 but did not verify that the organization had followed its policy for newly accepted conservation easements when the organization renewed its certification for 2011 and 2012. This organization accepted three new tax-credit-generating conservation easements in 2010 (the year leading up to its 2011 renewal) and four new tax-credit-generating conservation easements in 2011 (the year leading up to its 2012 renewal). Without a more in-depth review of documentation for new conservation easements as part of the certification renewal process, DRE is unable to verify that organizations such as the one on our example are actually following their policies and procedures, as required by state rules.

DRE's annual certification renewal process does not provide meaningful monitoring of conservation easement holders on an ongoing basis. Thus, the renewal process is little more than a mechanism to obtain an updated list of

conservation easements and collect a fee. During our interviews with CEOC members, four members specifically stated that there should be a more stringent renewal process or other periodic review by DRE to ensure that conservation easement holders are maintaining the level of diligence that they were required to display at the time of their initial certification. To minimize the burden that a more in-depth review would have on DRE staff and conservation easement holders, DRE could stagger and cycle the reviews such that each certified conservation easement holder undergoes such a review at least once every two or three years. Alternatively, DRE could take more of a risk-based approach and target its reviews to more problematic conservation easement holders with some holders still being randomly selected to ensure coverage. Consistent with its approach to the initial certification review, DRE could select the specific conservation easement projects for review on a sample basis.

Recommendation No. 9:

The Division of Real Estate (DRE) should strengthen the certification process to ensure that conservation easement holders continue to meet the certification requirements on an ongoing basis. At a minimum, DRE should periodically conduct an in-depth review of documentation for conservation easements that holders have accepted since their initial certification or most recent certification renewal.

Division of Real Estate Response:

Agree. Implementation date: January 2013 and Ongoing.

DRE staff will implement a schedule for reviewing conservation easement project documentation as a requirement of certification. The process will ensure projects from all certified conservation easement holders are reviewed on a periodic basis. DRE will identify risk factors that will trigger automatic project reviews as well as conduct random reviews. Staff review of project documentation will be similar to that conducted during the initial certification process. Project documentation reviews will occur throughout the year.

Statutory and Regulatory Framework

Conservation easement holders that accept tax-credit-generating conservation easement donations must be certified by DRE at the time of the donation. However, as discussed in this section, the statutory and regulatory framework for Colorado's conservation easement tax credit does not adequately protect the State

in those situations and circumstances in which governmental entities and nonprofit organizations holding tax-credit-generating conservation easements are no longer certified.

The certification requirement places a number of requirements on conservation easement holders at the time of the donation. However, once the donation has been made, the certification requirement technically no longer applies. Conservation easement holders may choose not to renew their certification. DRE may also suspend or revoke certification for cause (e.g., the holder no longer meets the minimum requirements for certification), although this has not happened since the certification requirement was put in place in 2008. When a conservation easement holder is no longer certified, current laws and rules would prevent the organization from accepting any *new* conservation easement donations for which tax credits will be claimed. However, the holders are allowed to continue to hold *existing* easements for which tax credits have already been claimed.

We are concerned that allowing uncertified holders to hold easements for which tax credits have already been claimed undermines the purpose of the certification requirement and potentially places the State's investment of public resources in existing easements at risk. First, when a conservation easement holder is no longer certified, the State effectively loses its ability to ensure the holder's ability to maintain, monitor, and defend the purposes of the tax-credit-generating conservation easements in perpetuity. Specifically:

- Notwithstanding efforts to strengthen the certification renewal process (see Recommendation No. 9), unless a conservation easement holder remains certified, DRE has no authority to continue to oversee the organization. For example, DRE would be unable to obtain and review documentation from the holder to ensure that the holder monitors tax-credit-generating conservation easements on at least an annual basis and that any potential violations of the easement's terms and conditions are followed up on and resolved in a timely manner. One nonprofit organization did not renew its certification for 2012. This organization did not hold any tax-credit-generating conservation easements; however, it is highly likely that, as time progresses, other governmental entities and nonprofit organizations holding tax-credit-generating conservation easements will not renew their certifications. Since tax credits can be carried forward for up to 20 years, it is possible that, in some cases, credits could be used for many years after the conservation easement holder is no longer certified. Additionally, because easements are to be maintained in perpetuity, it is possible that the State will be relying on noncertified holders to maintain easements that were supported by tax credits.

- State statute [Section 12-61-720(11), C.R.S.] only grants DRE the authority to investigate complaints or take disciplinary action against governmental entities and nonprofit organizations that are required to be certified. Thus, if the conservation easement holder is no longer certified, DRE no longer has the authority to investigate complaints against the holder, even if it continues to hold tax-credit-generating conservation easements. As of August 2012, DRE had received five complaints about conservation easement holders but did not have the jurisdiction to investigate four of these complaints because the conservation easement holders were not certified. We confirmed that two of these four conservation easement holders held tax-credit-generating easements that were donated in Tax Years 2000 through 2006 and 2001 through 2008, respectively, prior to the certification requirement taking effect. DRE's lack of authority to investigate complaints against uncertified conservation easement holders that continue to hold tax-credit-generating easements is a large gap in the State's ability to identify when the holders are no longer providing appropriate stewardship of their easements for the public's long-term benefit.

Second, the State currently does not have the ability to require an uncertified conservation easement holder to transfer tax-credit-generating conservation easements to a certified holder. Assignment clauses outline the terms of reassignment or transfer of a conservation easement to another qualified organization and are included in deeds of conservation easement to provide a backup or contingency in the event that the governmental entity or nonprofit organization holding the easement is dissolved or is unable to meet its ongoing stewardship responsibilities. For example, the Great Outdoors Colorado Trust Fund (GOCO) helps governmental entities and nonprofit organizations fund the acquisition of conservation easements throughout Colorado. To protect its investment of funds, GOCO requires that an assignment clause be included in the deed of conservation easement. Specifically, the assignment clause reserves GOCO's right to require transfer of the easement to a different organization if the original conservation easement holder (1) ceases to exist; (2) is unwilling, unable, or unqualified to enforce the terms and provisions of the easement; or (3) is unwilling or unable to effectively monitor the property for compliance with the easement on at least an annual basis. GOCO has never had to use this provision, but it provides strong protections for GOCO and a means of ensuring the long-term value and benefit of the conservation easements that GOCO helps to fund.

Conservation easement holders may include an assignment clause in their deeds of conservation easement as a matter of their own organizations' policies or based on established best practices in the land trust community. However, currently, state statute and rules governing the conservation easement tax credit do not require that assignment clauses be included in deeds of conservation easement.

Moreover, there is no requirement that assignment clauses, when used, reserve the State's right to require that tax-credit-generating conservation easements be transferred to another certified holder when the original holder is no longer certified. When a tax credit is claimed on a donated conservation easement, the State, by virtue of foregoing tax revenue, in essence becomes a funding agency for the acquisition. Thus, we believe that DOR and DRE should consider adopting GOCO's approach.

The statutory and regulatory environment surrounding conservation easements is complex. In addition to the issues we identified related to uncertified conservation easement holders, staff at the Office of the Attorney General reported that efforts by some landowners and conservation easement holders (even those that are certified) to subsequently amend or dissolve conservation easements pose additional risks. It is a challenge to provide the assurances necessary to protect the public interest in what is essentially a private transaction between the landowner and the organization acquiring the easement. Nonetheless, given the significant investment of public resources in conservation easements through tax credits, we believe it is prudent that the State identify and pursue solutions that help ensure the easements' value and benefit over the long term.

Recommendation No. 10:

The Division of Real Estate (DRE) and the Department of Revenue (DOR) should evaluate options for protecting the State's investment of public resources in tax-credit-generating conservation easements when the conservation easement holder is no longer certified. DRE and DOR should report back to the Legislative Audit Committee and the House and Senate Finance Committees by July 1, 2013, on viable options and pursue statutory and/or regulatory change, as appropriate.

At a minimum, options that should be considered include:

a. Strengthening DRE's ability to investigate complaints against conservation easement holders that hold tax-credit-generating conservation easements, regardless of whether or not the holder is certified.

b. Utilizing assignment clauses in the deeds for tax-credit-generating conservation easements that reserve the State's right to require the transfer of the easement to another certified conservation easement holder when the original holder ceases to exist; is no longer certified; or is unwilling, unable, or unqualified to enforce the terms and provisions of the easement.

Division of Real Estate Response:

a. Agree. Implementation date: July 2013.

DRE will explore options allowing for the investigation and enforcement of regulatory or statutory requirements for non-certified conservation easement holders. Regulatory programs do not typically have jurisdiction over entities that are not required to be certified or licensed. Creating a framework allowing DRE to investigate and enforce regulations for non-certified conservation easement holders will require statutory changes providing the required jurisdiction and resources. DRE will explore statutory and regulatory options and report back to the General Assembly as requested.

b. Agree. Implementation date: July 2013.

DRE has met with staff at the Great Outdoors Colorado (GOCO) to discuss the assignment clause required for conservation easements utilizing GOCO funds. DRE staff will continue to investigate appropriate conservation easement language and other options to ensure conservation easements are appropriately managed and enforced in perpetuity. DRE will work with DOR to identify practical options for reserving the State's right to require the transfer of tax credit generating easements to another holder. DRE is committed to ensuring the long-term management of conservation easements involving the state tax credit and will work to identify and report back to the General Assembly on a viable process that further protects the State's investment of public resources in tax-credit-generating conservation easements.

Department of Revenue Response:

a. Agree. Implementation date: July 2013.

DOR will meet with DRE to discuss options for strengthening DRE's ability to investigate complaints against conservation easement holders and, in conjunction with DRE, will report back to the General Assembly.

b. Agree. Implementation date: July 2013.

DOR will meet with DRE to discuss options for addressing the issues related to conservation easement holders' failures or refusals to

enforce the terms and provisions of a conservation easement and, in conjunction with DRE, will report back to the General Assembly.

Pre-Approval of Tax Credit Claims

Taxpayers claiming the conservation easement tax credit often receive substantial reductions in their income tax obligations, and the State foregoes a significant amount of general fund revenues in return for assurances that lands will be conserved and protected in perpetuity. Given the tax credit's significant financial impact on the State's revenues (i.e., $639 million foregone through 2009), it is important that the State have the appropriate mechanisms in place to ensure that conservation easement tax credits are supported by qualified conservation easement transactions. Throughout this chapter, we have made a number of recommendations to ensure that conservation easement tax credits being claimed by taxpayers comply with applicable statutory and regulatory requirements and are supported by land donations that have valid conservation purposes, are properly valued, and are donated to organizations that have the capacity to maintain, monitor, and defend the purposes of the easements in perpetuity.

Colorado's conservation easement tax credit is administered through a series of interrelated processes performed by DOR, DRE, and the CEOC, many of which were established through the enactment of House Bill 08-1353. Improving each of these individual processes will strengthen the State's administration of the conservation easement tax credit. However, as discussed in this final section of the chapter, we also believe that the State should fundamentally shift the manner in which the conservation easement tax credit is administered by adopting a pre-approval process.

Audit-Based Approach for Reviewing Tax Credit Claims

Currently, DOR's review of conservation easement tax credit claims occurs only *after* taxpayers (donors or transferees) file a tax return that uses the credit to offset their tax liabilities. Use of the tax credit is allowed unless a subsequent review or audit of the taxpayer's tax return and supporting documentation disallows the credit. This is often referred to as an "audit-based" approach because there is no prior approval by the State of the tax credit claim. The State's review occurs entirely after the fact.

In many ways, an audit-based approach to the conservation easement tax credit is advantageous for the State because it relies on tax administration infrastructure and processes that already exist within DOR. However, based on our audit work,

including interviews with management and staff at DOR and DRE and the members of the CEOC, we identified two key disadvantages to this type of approach to administering the conservation easement tax credit.

- **Uncertainty for the Taxpayer.** One disadvantage of Colorado's audit-based approach is that DOR does not technically "approve" conservation easement tax credit claims. Rather, credit claims are not disallowed. This lack of a positive approval of the tax credit creates uncertainty for donors and transferees attempting to use the credit because DOR could disallow the credit after the tax return is filed. The timing of DOR's review adds to the overall uncertainty taxpayers experience. As discussed earlier in this chapter, DOR does not review a conservation easement tax credit claim until the credit is used to offset a tax liability. Thus, a taxpayer filing a credit claim in 2010 may not find out there are problems with the claim until 2012. During our interviews, several CEOC members reported that landowners and the conservation easement holders are often caught off guard when the tax credit claim for a conservation easement donation is disallowed several years after the donation took place. Moreover, in the meantime, landowners may have sold the credit to a transferee, which results in additional tax returns that are called into question if the credit is disallowed.

  Donors make significant financial decisions when entering into a conservation easement agreement. These decisions may be based, in part, on the expected availability of the tax credit. Donors are giving up valuable development rights on their land in exchange for the ability to offset up to $375,000 in tax liabilities over 20 years, or for income from the sale of the tax credit to transferees. Similarly, when buying credits, transferees are expecting to gain a financial benefit by using the credit to offset their tax liabilities. However, it is important to note that (1) these financial benefits are only gained if the tax credit is allowed and (2) the disallowance of a tax credit does not have any impact on the easement agreement itself. Therefore, when a credit is subsequently disallowed, landowners are faced with the situation in which the conservation easement and its restrictions remain in place, yet the expected financial benefits no longer exist. As a result, it is possible that the State could be losing the benefit of legitimate conservation easement donations because landowners are unwilling to enter into a complex financial transaction for fear that their tax credit claim could be disallowed at some future date.

- **Decision Making Authority Is Not Well Aligned with Areas of Expertise.** A second disadvantage of Colorado's audit-based approach is that although the decision-making authority to allow or disallow conservation easement tax credit claims rests with DOR, the expertise

necessary to review certain aspects of conservation easement tax credit claims currently rests outside DOR. Both DRE and the CEOC operate in an advisory position to DOR regarding conservation easement tax credit claims. For example, DRE has a fully licensed appraiser on staff who conducts desk reviews of conservation easement appraisals and reviews appraisals referred by DOR; however, DRE does not make the determination that appraisals supporting conservation easement tax credits comply with the minimum requirements for a qualified appraisal completed by a qualified appraiser. Similarly, the CEOC members collectively possess sufficient expertise to assess and evaluate an easement's conservation purpose; however, the CEOC does not make the determination that the conservation purpose complies with the statutorily allowable purposes for claiming a tax credit.

We question whether the current process provides for the most efficient and effective decision making. DOR's tax examiners are skilled and trained in the application of tax laws and regulations when reviewing conservation easement tax credit claims. However, they are not licensed appraisers nor do they currently assess or evaluate some of the more substantive aspects of conservation easement transactions, such as conservation purposes and the easements' terms and conditions to ensure that these purposes will be safeguarded (e.g., no inconsistent land uses are allowed). As discussed earlier in this chapter (see Recommendation Nos. 1 and 7), conservation purpose and appraisals are two areas in which the State needs better review coverage to ensure taxpayers' compliance with minimum requirements.

Adopting a Pre-Approval Process

The primary alternative to an audit-based approach that some other states use involves the certification or pre-approval of conservation easement tax credit claims. Under this approach, states have processes to certify or approve conservation easement tax credit claims *before* the taxpayers are allowed to file a tax return using the credits. For example, although the specific requirements vary for each state, of the 14 other states that offer tax credits for conservation easement donations, we identified 10 states that have application and approval processes that must occur before a taxpayer can use the credit in a tax return filing. These states include Arkansas, California, Delaware, Georgia, Maryland, Massachusetts, Mississippi, New Mexico, North Carolina, and Virginia.

We believe that adopting a pre-approval process would provide the State with stronger assurances that conservation easement tax credits are supported by qualified transactions while also yielding increased efficiencies and more certainty for the taxpayers when claiming and using the tax credits. Adopting a

pre-approval process will require statutory change as well as a realignment of resources. Therefore, DOR, DRE, and the CEOC will need to work with the General Assembly and affected stakeholders to consider a number of factors, as discussed in the following section.

Goals for the Pre-Approval Process

One clear advantage of a pre-approval process is that the State would issue an approval or denial of the tax credit claim before a donor or transferee files a tax return to use the associated credit. Having a positive approval (as opposed to the lack of a disallowance under the current process) provides more certainty to donors about the validity of their tax credits. Additionally, the State would have stronger assurances that conservation easement tax credit claims are valid before they are used because the State's approval would be based on a review of all conservation easement tax credit claims for compliance with all minimum requirements, including easements' conservation purposes. Ultimately, the State's goals for the pre-approval process will dictate the scope of the review of conservation easement tax credit claims. For example:

- If the goal of the pre-approval process is to identify and reject clearly abusive transactions (e.g., those that lack any real conservation values, have overinflated appraised values, or have unqualified entities accepting the donation), the State could adopt a more limited review of taxpayer documentation.

- If the goal of the pre-approval process is to ensure that only the highest-quality transactions qualify for the tax credit, the State's review would have to be much more thorough. For example, for each claim, the State might need to conduct a detailed examination of (1) the deed of conservation easement and the baseline report (i.e., documentation of the present condition of the property) to ensure that conservation purposes are sound and (2) the appraisal to ensure that the fair market value of the donation is determined based on a solid appraisal methodology in accordance with professional standards.

The solution likely rests between these two ends of the spectrum. Ideally, the pre-approval process would provide a more detailed review of conservation easement donations and taxpayers' compliance with minimum requirements than what currently exists without the process being too onerous for the taxpayer or requiring extensive review time frames to complete.

Decision Making

House Bill 08-1353 took an important step forward by including more perspectives and expertise into the process for evaluating conservation easement tax credit claims. However, these perspectives and expertise are generally only advisory. One advantage to a pre-approval process is that it could allow the State to assign decision-making responsibilities for approving the different components of conservation easement tax credit claims to those with the appropriate expertise. For example:

- DRE could have the responsibility for determining whether appraisals supporting conservation easement tax credits comply with the minimum requirements for a qualified appraisal completed by a qualified appraiser. This responsibility could include determining whether the appraisals have methodological issues that could affect the valuation of the land being donated. House Bill 08-1353 started to move in this direction by at least requiring that all conservation easement appraisals be submitted to DRE.

- The CEOC could have the responsibility for assessing and evaluating the quality of conservation easement transactions, including determining whether easements associated with tax credit claims are for qualified conservation purposes and whether the easements' terms and conditions sufficiently protect these conservation purposes. The makeup of the CEOC could also be adjusted as necessary. If DRE is responsible for reviewing appraisals, we are uncertain whether there would be a need for a licensed appraiser on the CEOC. Also, the CEOC does not presently include an individual with expertise in tax matters; having someone with this expertise could be beneficial when determining whether conservation purposes associated with tax-credit-generating easements comply with the tax code.

- DRE, with input from the CEOC would retain responsibility for certifying conservation easement holders. DOR already relies on the certification process established in accordance with House Bill 08-1353 to ensure that conservation easement holders have the capacity to maintain, monitor, and defend the purposes of tax-credit-generating easements.

- DOR would retain responsibility for ensuring compliance with all other tax-related statutory and regulatory requirements for claiming and using the tax credit, such as ensuring that the donation occurred before the end of the donor's tax year, all forms and documents required to substantiate the credit claim have been submitted, and the donor has not claimed or used more than one conservation easement tax credit for the same tax year. DOR would also retain responsibility for reviewing uses of approved

credits on filed tax returns, such as ensuring that the taxpayer has a tax liability to offset, the total amount of the credit used by donors and transferees does not exceed the total credit amount allowed, and the amount being used does not exceed any carry-forward amounts.

Because this is a tax credit, as the State's tax agency, DOR should still retain the final sign-off on conservation easement tax credits under a pre-approval process. Substantively, however, DOR could rely on the decisions and approvals provided by DRE and the CEOC regarding conservation easement appraisals, conservation purposes, and the certification of conservation easement holders. Additionally, because decision making would be shared among several agencies, avenues for appealing decisions made during the pre-approval process should be clearly established and communicated to the taxpayer. Finally, it may also be important for taxpayers to understand that the pre-approval process would not limit the State's ability to audit the transaction at a later date if the taxpayer is selected for audit through DOR's routine audit processes for individual and corporate taxpayers.

Timeliness

One common criticism of pre-approval processes is that they often add to the length of time for claiming tax credits. For example, many conservation easement transactions are supported by complex and sophisticated appraisals, and an in-depth review of such appraisal documentation would require time to complete. In adopting a pre-approval process, the State will need to determine how best to maintain a timely decision-making process. For example, Georgia tries to achieve a 90-day turnaround from the time donors file a tax credit claim to the time the claim is approved or denied. However, to make this work, Georgia requires donors to provide all documentation by October so that decisions can be made in time for donors or transferees to use the tax credits when filing their tax returns in April of the following year.

Adopting a pre-approval process comes with its own challenges, and we do not presume that it will, by itself, correct all of the existing problems with the State's administration of the conservation easement tax credit. However, in conjunction with the improvements recommended throughout the rest of this report, pre-approval should provide for a more effective and efficient administrative process that provides more certainty for donors and transferees while maintaining the necessary protections for the State. We recognize that DOR, DRE, and the CEOC may need to adjust their implementation of the other recommendations contained in this report if the State adopts a pre-approval process.

Recommendation No. 11:

The Department of Revenue (DOR), the Division of Real Estate (DRE), and the Conservation Easement Oversight Commission (CEOC) should work together to design a pre-approval process for reviewing and approving conservation easement tax credit claims. These agencies should report to the Legislative Audit Committee and the House and Senate Finance Committees by July 1, 2013, on a proposed pre-approval process, including any statutory and regulatory changes that are necessary for implementation.

At a minimum, the proposed pre-approval process should ensure that:

a. The State has reasonable assurances that conservation easement tax credits being claimed by taxpayers are valid and comply with all statutory and regulatory requirements.

b. Conservation easement tax credit claims are approved or denied separately from and prior to any uses of the tax credit. Avenues for appealing decisions made during the pre-approval process should be clearly established and communicated to the taxpayer.

c. All essential elements related to conservation easement tax credit claims are reviewed and approved by those with the most appropriate and relevant expertise.

d. The review and approval of tax credit claims is timely.

Department of Revenue Response:

Agree. Implementation date: July 2013.

DOR will meet with DRE and the CEOC to discuss and provide options for designing a pre-approval process for reviewing and approving conservation tax credits and report back to the General Assembly. The discussion will include the issues raised in the State Auditor's report and in Recommendation No. 10 subparts (a) through (d).

Division of Real Estate Response:

Agree. Implementation date: July 2013.

DRE will work with DOR and the CEOC to explore processes by which the State would approve conservation easement tax credit claims prior to the tax credit being used. There are likely many viable options for implementing an approval process that meets the minimum requirements of this recommendation. DRE will work to ensure proposals are aligned with the expertise of DRE, DOR, and the CEOC. A report outlining the identified options for a pre-approval process will be provided to General Assembly as requested.

Conservation Easement Oversight Commission Response:

Agree. Implementation date: July 2013.

The CEOC is committed to working with DRE and DOR to develop a process that provides certainty to landowners who do qualified transactions with licensed appraisers and certified conservation easement holders, and which provides reasonable assurances to the State that the credits claimed comply with statutory and regulatory requirements. It is the consensus of the CEOC's members that, while HB 08-1353 eliminated the occurrence of fraudulent tax credit claims and unqualified easement holders, the current process fails to provide a clear path for legitimate conservation easement tax credit claims to move forward. It is the CEOC's opinion that, as stated in the audit, the review and decision-making processes should be reassigned to those agencies with appropriate expertise. The CEOC members believe it is necessary for all parties to fully participate in the design of a process that accomplishes these goals and that the process must provide for a binding decision-making process not subject to administrative discretion.

Auditor's Addendum

Some of the specific items expressed in the CEOC's response, such as reassigning review and decision-making responsibilities and the extent to which such decisions are binding, should be considered and evaluated in collaboration with DOR and DRE as part of the implementation of this recommendation.

This page intentionally left blank.

Effectiveness of the Conservation Easement Tax Credit

Chapter 3

Colorado uses tax policy as a means of incentivizing land conservation. As recently as the 2011 Legislative Session, the General Assembly has affirmed its policy commitment to the conservation easement tax credit. Specifically, the legislative declaration to House Bill 11-1300 made the following statements:

- Colorado's conservation easement tax credit is an important preservation tool used to balance economic needs with natural resources, such as land and water preservation.

- Colorado's conservation easement tax credit and the federal tax deduction have allowed many farmers and ranchers the opportunity to donate their development rights to preserve a legacy of open spaces in Colorado for wildlife, agriculture, and ranching.

- Citizens throughout Colorado believe good, sound conservation practices are important to Colorado's quality of life, agriculture, and wildlife heritage.

One of the objectives of our audit was to assess the conservation easement tax credit's overall effectiveness. To address this question, we gathered and analyzed information on general trends in conservation easements in Colorado, compared and contrasted Colorado's conservation easement tax credit with similar programs in other states, reviewed various reports and research on conservation easement tax credits more generally, and interviewed DOR and DRE management and staff and members of the CEOC.

There are no statewide land conservation or conservation-easement-specific plans against which we could measure the effectiveness of Colorado's conservation easement tax credit program. Therefore, in this chapter, we have developed three different measures of effectiveness as a way to frame the discussion about the tax credit. Based on our first measure, the tax credit appears to be effective as a general incentive for protecting land and spurring conservation activity. Based on our second measure, the tax credit appears to be effective at reducing the average tax liability of those taxpayers claiming the credit. However, when we consider our third measure—an assessment of costs and benefits—we are left in a more

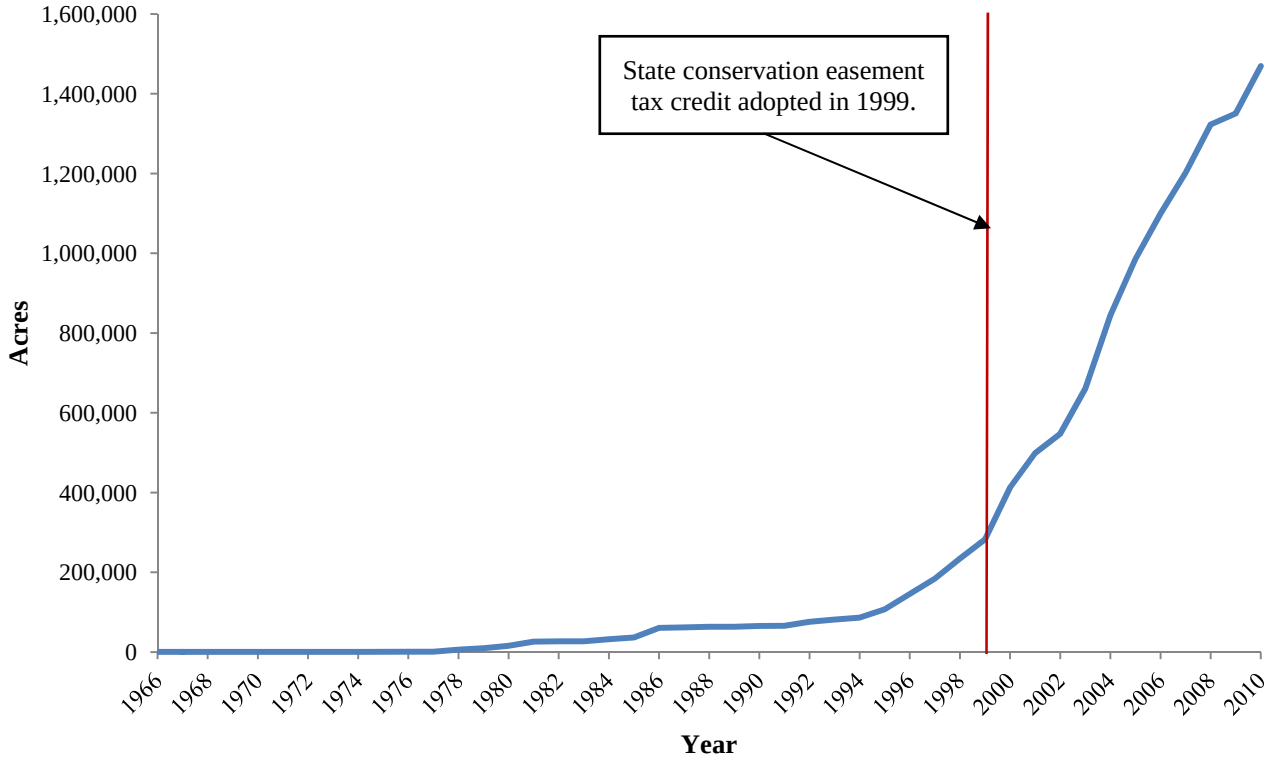
tenuous position as to the tax credit's effectiveness because the costs are generally easily quantified, but quantifying the benefits is more elusive.

Effectiveness Measure 1: The Conservation Easement Tax Credit Appears to Encourage Additional Land Protection

One measure of the conservation easement tax credit's effectiveness is whether it results in more acres of land being protected through conservation easements. Through our interviews with various agencies and stakeholders, we learned that the most comprehensive source of data on protected lands in Colorado is the Colorado Ownership, Management, and Protection (COMaP) project at Colorado State University. The COMaP database is a standardized geographic information systems database and set of core attributes based on primary data obtained from a number of federal, state, and local government agencies, as well as nonprofit land trusts and other nongovernmental organizations.

We worked with COMaP project staff to obtain and understand general trend data on conservation easements in Colorado. The following chart shows the cumulative conservation easement acreage by year for calendar years 1966 through 2010.

Cumulative Conservation Easement Acreage In Colorado
Calendar Years 1966-2010



Source: Colorado Ownership, Management, and Protection (COMaP) v9 Database, Colorado State University, Fort Collins, CO (September 2011).
Note: COMaP includes an additional 125,000 acres of conservation easements with unknown dates of establishment that are not reflected in this chart.

Overall, it appears that the tax credit has been effective at encouraging conservation activity in Colorado. Specifically, the total acres of land protected through conservation easements increased by about 430 percent since the tax credit was made available. In 1999, land trusts and governmental agencies reported holding conservation easements on about 283,000 acres of land in Colorado. By 2010 the total acreage of reported conservation easements jumped to about 1.5 million acres. (These figures do not include the 125,000 acres of conservation easements for which the date of establishment is unknown, as noted in the previous chart.) We cannot conclusively state that these lands would not have been preserved had the tax credit not been available, nor can we attribute all of this increase solely to the existence of the tax credit. Nonetheless, the data show a compelling trend. Similar analyses performed by audit and evaluation offices in Montana and Virginia show upward trends in the number of acres under

conservation easement subsequent to those states' adoption of a conservation easement tax credit.

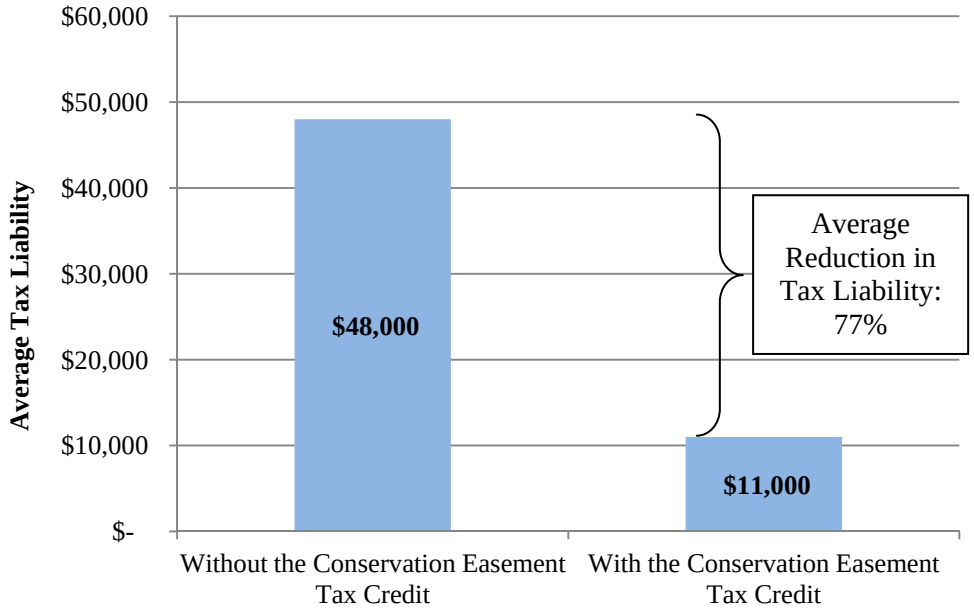
Effectiveness Measure 2: The Conservation Easement Tax Credit Allows Taxpayers to Reduce Their Tax Burden

The conservation easement tax credit seeks to incentivize land conservation efforts by allowing taxpayers to reduce their tax burden. Therefore, a second way to measure the effectiveness of the tax credit is from the perspective of taxpayers using the credit, including both easement donors and transferees who purchase tax credits on the secondary market. That is, the tax credit is effective if taxpayers are actually taking advantage of it to reduce their taxes.

We analyzed tax return data from DOR's GenTax system for all 910 taxpayers (donors and transferees) that used the tax credit to offset a tax liability in Tax Year 2010. Overall, we found that these 910 taxpayers lowered their tax burden by a total of about $33.3 million through the conservation easement tax credit. The following chart represents the difference in the average tax liability before and after applying the conservation easement tax credit for these 910 taxpayers. Our analysis shows that in Tax Year 2010, the tax credit lowered the average state income tax liability for those taxpayers who used the credit from about $48,000 to about $11,000 (77 percent reduction), resulting in an average tax savings of about $37,000.

Average State Income Tax Liability Among Taxpagers Who Used the Conservation Easement Tax Credt

Tax Year 2010



Source: Office of the State Auditor's analysis of Department of Revenue data.

Overall, our analysis demonstrates that the conservation easement tax credit provides donors and transferees with a substantial financial benefit. However, we are limited in our ability to further evaluate the average tax savings represented in the chart above. Although the data show that the tax credit is working to reduce tax liabilities for those taxpayers who are able to use it, determining whether this average percentage reduction in tax liabilities should be higher or lower is a policy matter that is beyond the scope of our audit. It is also important to note that the average percentage reduction in tax liability could fluctuate over time as a result of various factors, such as the number and value of conservation easements being donated and changes in the demand for tax credits among potential transferees in the secondary market.

Effectiveness Measure 3: It Is Unclear Whether the Conservation Easement Tax Credit Protects Conservation Values at a Reasonable Cost

The State is foregoing a significant amount of annual tax revenues to incentivize land conservation. Therefore, a final measure of the conservation easement tax credit's effectiveness would be to determine whether its public benefits outweigh its costs.

Quantifying Costs

Unlike other state programs and services where cost is typically measured in terms of expenditures, the public cost of the conservation easement tax credit is an opportunity cost—the revenues the State would have otherwise collected and used to fund state programs and services.

According to data from DOR, as of Tax Year 2009, landowners had claimed about $639 million worth of tax credits for donated conservation easements since the credit was first made available for Tax Years beginning on or after January 1, 2000. This total includes credit amounts used by landowners or transferees, as well as credit balances that may be used in future tax years (e.g., carry-forward amounts). The actual final cost to the State for these credits may be less, however, since some claims have been denied by DOR and are in various stages of dispute resolution. It is also possible that some donors will not use or transfer the full value of their credit before the 20-year carry-forward period expires.

As of the conclusion of our audit work, DOR had not finished processing new conservation easement tax credit claims that occurred in Tax Year 2010; therefore, data on the "costs" added in 2010 were not available. For tax years beginning in calendar years 2011 through 2013, the General Assembly limited the total dollar amount available for new conservation easement tax credits to $78 million. As of August 17, 2012, DRE had issued tax certificates for about $44 million (56 percent) of the $78 million available.

Quantifying Benefits

Although measuring the public cost of the conservation easement tax credit is generally straightforward, measuring and demonstrating the aggregate benefit the public has received in return is more difficult and limited because of a lack of available data. We attempted to quantify the public benefit of the conservation easement tax credit using two separate measures: (1) the fair market value of the conservation easements for which tax credits have been claimed and (2) the specific conservation purposes that have been protected.

- **Fair Market Values.** Tax-credit-generating conservation easements are primarily held by other parties and cannot be considered financial assets of the State. However, the State and its taxpayers are receiving the benefit of protecting land at a cost that is significantly less than what the State would pay to directly reimburse landowners for the full fair market value of their easements. We examined data that DOR has collected from taxpayers since 2007 for public reporting purposes pursuant to state statute [Section 39-22-522(3), C.R.S.]. These data consistently show a 3:1 ratio between the appraised value of the conservation easements and the tax credit amounts claimed. That is, the fair market value of tax-credit-generating conservation easements tends to be about three times the amount the State foregoes in the form of tax credits for those easements. We found this ratio to be consistent with other data that DRE has collected from landowners since 2011 as part of its management of the tax credit cap.

- **Conservation Purposes.** One of the advantages of Colorado's conservation easement tax credit is that each of the four allowable conservation purposes is defined broadly to include a wide variety of lands and values (i.e., public benefits) for which land may be protected and a tax credit claimed. However, given limitations in available data, which we describe in more detail later in this section, it is not possible to quantify specifically how much land has been protected for each of the allowable conservation purposes. For example, it is not possible to determine how many of the 925,000 acres associated with tax-credit-generating conservation easements are for open space preservation versus habitat protection. Without the ability to associate acreage statistics with conservation purposes in this manner, quantifying the public benefits of the conservation easement tax credit is limited significantly.

Despite efforts by the General Assembly to obtain information from landowners about their conservation easement donations, currently, neither DOR nor DRE collect data from landowners in a manner that permits the type of aggregate analysis of the conservation purposes associated with tax-credit-generating conservation easements that could be useful for measuring and demonstrating the public benefits of the conservation easement tax credit. Moreover, as discussed in Chapter 2, DOR does not currently examine an easement's conservation purpose as part of the tax credit claim review process.

In 2007, the General Assembly attempted to provide the public with information about the conservation purposes that landowners cite when claiming tax credits on their conservation easement donations through a reporting provision included in House Bill 07-1361. Codified in Section 39-22-522(3)(c), C.R.S., this provision explicitly requires each landowner donating a tax-credit-generating easement to report to DOR information about the conservation purposes that are protected by

the easement. The landowner must also report information about the county, township, and range where the easement is located; the number of acres subject to the easement; the amount of the tax credit claimed; and the name of the organization holding the easement. Statute further requires DOR to make all of this landowner-reported information publicly available. To implement the reporting provisions of House Bill 07-1361, DOR promulgated rules that require landowners to file Form DR1304, which can be completed either online or in hard-copy format. This form allows landowners to report all statutorily required information about their conservation easements, including the easements' conservation purposes. DOR provides a compilation report of this landowner-reported information on its website.

During our audit, we analyzed Form DR1304, as well as the resulting compilation report available on DOR's website that is based on DR1304 forms completed by landowners, and found this current reporting mechanism to be limited in three ways. First, descriptions of conservation purposes are captured only in text format. As a result, there is very little consistency among the entries—landowners have written as little as two words and as much as a paragraph of more than 300 words to describe their easements. Although this may be sufficient for analyzing conservation easement donations on a case-by-case basis, it does not allow the data to be quickly aggregated and grouped according to common conservation purposes. For example, Form DR1304 does not provide check boxes that allow the landowner completing the form to select the allowable conservation purposes applying to the easement. The form also does not include check boxes to capture more detail on the specific land attributes supporting the conservation purposes, such as the types of wildlife habitats that are being protected or the types of public recreational opportunities that are present.

Second, landowners claiming conservation easement tax credits do not always file Form DR1304. Specifically, we estimated that DOR received the form for only about 70 percent of the conservation easement tax credits that were claimed between Tax Years 2007 and 2009. Consequently, the reports DOR has made publicly available on its website do not exhibit all the conservation easement tax credits that were claimed during this period. Although landowners are required to submit Form DR1304, DOR staff reported that they do not disallow credit claims solely for failure to submit the form. Additionally, current rules require taxpayers to file Form DR1304 separately from the other documentation that must be submitted as part of the tax credit claim.

Finally, we believe there are opportunities for DOR to streamline the collection and reporting of data on conservation easement tax credit claims. For example, in addition to requiring landowners to submit Form DR1304, DOR also requires conservation easement holders to complete Form DR1299, which must be submitted to both DOR and DRE. However, through our discussions with staff from both agencies, we found that DOR and DRE do not actually use Form

DR1299, and information on the form (e.g., list of all currently held conservation easements and acreage) is duplicative of information that is already submitted through the conservation easement holder certification process. Additionally, DOR maintains two separate public reports on its website that both derive from the same core data, but each report contains information that is not included in the other. We believe DOR can fulfill its reporting requirements through a single, consolidated report that would ultimately prove more useful to the public.

Ensuring Public Benefits

The specific public benefits derived from the conservation easement tax credit may be difficult to quantify. However, there are indicators that tax-credit-generating conservation easements are providing benefits that are important to the public. We interviewed all members of the CEOC, who represent different stakeholder interests. When we asked about the benefits of the tax credit, each member reported that there have been important conservation benefits achieved and that the tax credit is accomplishing what it was intended to do, such as preserving scenic corridors and open space while maintaining ranching and other agricultural uses of the land, providing outdoor recreational opportunities for the public, and protecting important fish and wildlife habitats.

We found there are some general requirements the public can rely on to provide at least a minimum level of assurance that donated lands hold value and benefits for the public. Specifically, in order to be certified by DRE to accept tax-credit-generating conservation easements, governmental entities and nonprofit organizations must have a process for reviewing, selecting, and approving any potential conservation easements, including processes to identify and document the conservation values and the public benefits achieved by protecting those values prior to accepting the conservation easement. DRE staff and CEOC members reported that many conservation easement holders will not accept donations that do not meet the organization's conservation standards or further their organization's mission.

We compiled and analyzed the mission statements and other related information from the application materials for the 42 governmental entities and nonprofit organizations that were certified conservation easement holders as of June 30, 2012. The following table shows a breakdown of how these conservation easement holders' mission statements generally relate to the four conservation purposes outlined in the Internal Revenue Code and regulations. The most common conservation purpose cited in holders' mission statements and application materials referenced the preservation of open space as one of the goals driving their land conservation efforts. Many mission statements referred to more than one conservation purpose.

Analysis of Mission Statements for Certified Conservation Easement Holders
(As of June 30, 2012)

General Conservation Purpose	Count of Certified Conservation Easement Holders*	Percent of Total Certified Conservation Easement Holders*
Open Space	37	88.1%
Fish, Wildlife, Plants, or Similar Ecosystem	24	57.1%
Outdoor Recreation and Education	11	26.2%
Historically Important Land Area or Structure	6	14.3%

Source: Office of the State Auditor's analysis of conservation easement holder certification application materials provided by the Division of Real Estate.

***** There were a total of 42 certified conservation easement holders, 25 of which had mission statements that referred to more than one conservation purpose.

Finally, we reviewed the results of the January 2012 "Conservation in the West Survey," which is a bipartisan poll of 2,400 registered voters in six western states (Arizona, Colorado, Montana, New Mexico, Utah, Wyoming) commissioned by the State of the Rockies Project at Colorado College. The survey data show that 86 percent of Colorado respondents agreed or strongly agreed with the statement that "even with state budget problems, we should still find money to protect Colorado's land, water, and wildlife." These general attitudes about conservation indicate that Coloradoans may see an overall public benefit from the conservation easement tax credit that is worth the cost.

Recommendation No. 12:

The Department of Revenue (DOR) should help ensure the State's ability to measure the public benefits of the conservation easement tax credit by:

a. Improving taxpayer forms to capture data in a format that facilitates aggregate analysis and reporting on the specific conservation purposes and land attributes that are being protected by conservation easements.

b. Ensuring that taxpayers donating tax-credit-generating conservation easements submit Form DR1304.

c. Eliminating unnecessary or duplicative data collection forms and consolidating public reports when possible.

Department of Revenue Response:

a. Agree. Implementation date: July 2013.

DOR will help ensure the State's ability to measure the public benefits of the conservation easement tax credit by improving required forms used to capture data about conservation easements and the associated tax credits.

b. Agree. Implementation date: July 2013.

DOR will review its procedures in obtaining Form DR1304 from taxpayers and make changes to ensure the form is submitted.

c. Agree. Implementation date: July 2013.

DOR will review the forms associated with conservation easement tax credits and eliminate any unnecessary or duplicative data requests that are not statutorily required and consider options for consolidating public reports. In addition, DOR will review its publication of information on its website to ensure it is easily accessible.

This page intentionally left blank.

Appendix

This page intentionally left blank.

Appendix A
Conservation Easement Income Tax Credit Incentives by State

State	How Is the Credit Calculated?	Credit Claim Limits	Annual Usage Limits	Statewide Credit Caps	Maximum Carry-forward Period	Transferable to Other Taxpayers?
Arkansas	50% of the donation's fair market value	$50,000 maximum per donation; 1 donation per taxpayer per year	Up to $5,000 may be used per year.	Credits will cease being available one year after the end of the calendar year in which the total of credits used exceeds $500,000.	9 years	No
California	55% of the donation's fair market value	None	None	$100 million total	8 years	No
Colorado	50% of the donation's fair market value	$375,000 maximum per donation; 1 donation per taxpayer per year	None	None, except for 2011, 2012, and 2013 ($22 million for 2011 and 2012, $34 million for 2013)	20 years	Yes
Connecticut	50% of the donation's fair market value	None; only available to corporations	None	None	25 years	No
Delaware	40% of the donation's fair market value	$50,000 maximum per taxpayer per year	None	$1 million per year; $10 million total	5 years	No
Georgia	25% of the donation's fair market value	$250,000 maximum per year for individuals, $500,000 for corporations and partnerships	None	None	10 years	Yes
Iowa	50% of the donation's fair market value	$100,000 maximum per taxpayer per year	None	None	20 years	No
Maryland	100% of the donation's fair market value	$80,000 maximum per taxpayer per year	Up to $5,000 may be used per year.	None	15 years	No
	100% of local property taxes paid each year on conserved land	None	None	None	This credit may be claimed annually for 15 years following an easement donation.	No
Massachusetts	50% of the donation's fair market value	$50,000 maximum per donation; taxpayers must allow 3 years to elapse between donations	None	$2 million per year	Carry forward not allowed. Credit in excess of tax liability is refundable.	No

Appendix A
Conservation Easement Income Tax Credit Incentives by State

State	How Is the Credit Calculated?	Credit Claim Limits	Annual Usage Limits	Statewide Credit Caps	Maximum Carry-forward Period	Transferable to Other Taxpayers?
Mississippi	50% of allowable transaction costs such as for appraisals, baseline inspections, and surveying and legal fees.	Lifetime maximum of $10,000	None	None	10 years	No
	$5.50 per acre on land allowed to be used as a natural preserve; wildlife refuge, habitat, or management area; or for public recreation.	None	None	None	Credit may be claimed annually. Unused credits may be carried forward for 5 years from the year in which the land was approved for use.	No
New Mexico	50% of the donation's fair market value	$250,000 maximum per donation; 1 donation per taxpayer per year	None	None	20 years	Yes
New York	25% of local property taxes paid each year on conserved land	$5,000 per taxpayer per year	Up to $5,000 may be used per year.	None	Carry forward not allowed. Credit in excess of tax liability is refundable.	No
North Carolina	25% of the donation's fair market value	$250,000 maximum per year for individuals, $500,000 for corporations, pass-through entities, and joint filers	None	None	5 years	No
South Carolina	25% of the donation's fair market value	No maximum per taxpayer; $250 maximum per acre	Up to $52,500 may be used per year.	None	Indefinite	Yes
Virginia	40% of the donation's fair market value	None	Up to $100,000 may be used per year.	$100 million per year (inflation adjusted after 2008)	10 years	Yes

Source: Office of the State Auditor's analysis of statutes and regulations in states that offer income tax credit incentives for conservation easement donations.

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

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

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

Report Control Number 2171

Report Control Number 2171

Unemployment Insurance Program
Department of Labor and Employment

Performance Audit
October 2011

OFFICE OF THE
STATE AUDITOR

LEGISLATIVE AUDIT COMMITTEE
2011 MEMBERS

Senator Lois Tochtrop
Chair

Representative Cindy Acree
Vice-Chair

Representative Deb Gardner
Senator Lucia Guzman
Representative Jim Kerr
Senator Steve King
Representative Joe Miklosi
Senator Scott Renfroe

OFFICE OF THE STATE AUDITOR

Dianne E. Ray
State Auditor

Jonathan Trull
Deputy State Auditor

Eric Johnson
Legislative Audit Manager

Beverly Mahaso
Trey Standley
Nathan White
Legislative Auditors

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

Office of the State Auditor

Dianne E. Ray, CPA
State Auditor

October 19, 2011

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of the Unemployment Insurance Program. The 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 Labor and Employment.

TABLE OF CONTENTS

Glossary of Terms and Abbreviations

CUBS – Colorado Unemployment Benefits System

Department – Department of Labor and Employment

DOR – Department of Revenue

FTE – Full-time-equivalent staff

UI – Unemployment Insurance

UI Program – Unemployment Insurance Program

USDOL – U.S. Department of Labor

UNEMPLOYMENT INSURANCE (UI) PROGRAM

Performance Audit, October 2011
Report Highlights

Dianne E. Ray, CPA
State Auditor

Department of Labor and Employment

PURPOSE

Evaluate the UI Program's procedures for ensuring that only eligible individuals receive benefits, making timely benefits payments, recovering overpayments, and providing customer service to claimants.

BACKGROUND

- The UI Program aims to stabilize the economy by providing benefits to workers who lose employment through no fault of their own.
- Benefits payments are funded through premiums paid by Colorado employers.
- During Calendar Year 2010, the program paid about $2.4 billion in benefits compared to $298 million in Calendar Year 2006.
- Claims volume increased 190 percent from January 2007 to March 2009 and remains above historical levels.
- About 80 percent of the UI Program's administrative costs are paid by federal funding, with the remainder paid through state cash funds.

OUR RECOMMENDATIONS

The Department of Labor and Employment should:

- Ensure that claimants provide valid identification and attest to their lawful presence in the United States in compliance with House Bill 06S-1023's requirements.
- Increase the information it collects online, such as establishing an online system for employers to provide claims information and requiring more work search information from claimants.
- Reallocate additional staff to identify and recover overpayments.
- Increase the number of staff available to answer claimant phone calls.
- Evaluate whether UI eligibility should be based on only the claimant's most recent employer.

The Department generally agreed with these recommendations.

EVALUATION CONCERN

The UI Program has made a significant amount of overpayments in recent years. In addition, while staffing levels and information system limitations have made it difficult for the UI Program to keep up with increased workload and meet federal performance standards, opportunities exist for the UI Program to increase efficiency by eliminating labor-intensive processes and reallocating staff.

KEY FACTS AND FINDINGS

- The UI Program does not have adequate controls in place to verify that claimants are legally present in the United States, as required by House Bill 06S-1023. We estimate that the program paid $60 million during Calendar Year 2010 to claimants who did not meet House Bill 06S-1023's identification requirements.
- In Calendar Year 2010, the UI Program paid an estimated $169 million in overpayments (benefits for which people were not eligible), which represents 19 percent of all state benefits payments. Almost half of these overpayments, $83 million, resulted from claimants reporting that they had searched for work when they had not or could not provide proof of these searches.
- Sixteen percent of the Department of Labor and Employment's (the Department) 239 nonmanagement full-time-equivalent (FTE) staff could be reallocated to more efficient functions if the Department reduces the use of paper forms, requires most claimants to apply online, further automates claims processing, and pursues statutory changes to simplify eligibility determination.
- The UI Program did not meet any federal performance standards for making timely payments, evaluating claimants' eligibility, and identifying overpayments during Calendar Years 2009 and 2010. The program did not meet most of the standards in Calendar Years 2006 through 2008.
- Claimants have had great difficulty reaching the UI Program's customer call center, usually receiving a busy signal, being directed to a self-service menu with no option to speak with an agent, or experiencing hold times of more than an hour when they do get through to the center.

FINANCIAL BENEFITS

Based on a statistical sample, we determined that the UI Program paid about $60 million, or about 3 percent of the $2.4 billion in state and extended UI benefits paid in Calendar Year 2010, to claimants who did not or could not meet House Bill 06S-1023's identification requirements and, therefore, should not have received benefits.

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

RECOMMENDATION LOCATOR
Agency Addressed: Department of Labor and Employment

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
1	24	Ensure that claimants meet the attestation requirements of House Bill 06S-1023 and federal law by (a) changing the application form so that claimants are clearly affirming that they are legally present in the United States, (b) requiring all applicants to affirm legal presence before receiving benefits, and (c) eliminating the use of the current paper affidavit form for affirming legal presence.	a. Agree b. Agree c. Partially Agree	a. December 2011 b. December 2011 c. November 2011
2	27	Ensure that claimants meet the requirements of House Bill 06S-1023 for affirming their lawful presence in the United States by (a) requiring claimants to provide a valid Colorado driver's license or identification card or other acceptable documents and (b) establishing procedures to verify that the person applying for benefits is the same person depicted by the identification number or document that the person provides on his or her application.	Agree	December 2012
3	35	Improve the collection of information from claimants by (a) eliminating or reducing the use of the "Request for Facts—Employee" form, (b) increasing the number of employers who electronically submit information currently collected by the "Request for Facts—Employer" paper form, (c) adding an open-ended question to the application that asks claimants to provide more detailed information regarding the circumstances of their layoff, and (d) adding language to the continued claims filing systems indicating that claimants must conduct a work search and requiring all claimants to provide the number of job contacts made each week and information for each job contact.	a. Partially Agree b. Agree c. Partially Agree d. Partially Agree	a. December 2011 b. June 2012 c. December 2011 d. December 2012

RECOMMENDATION LOCATOR
Agency Addressed: Department of Labor and Employment

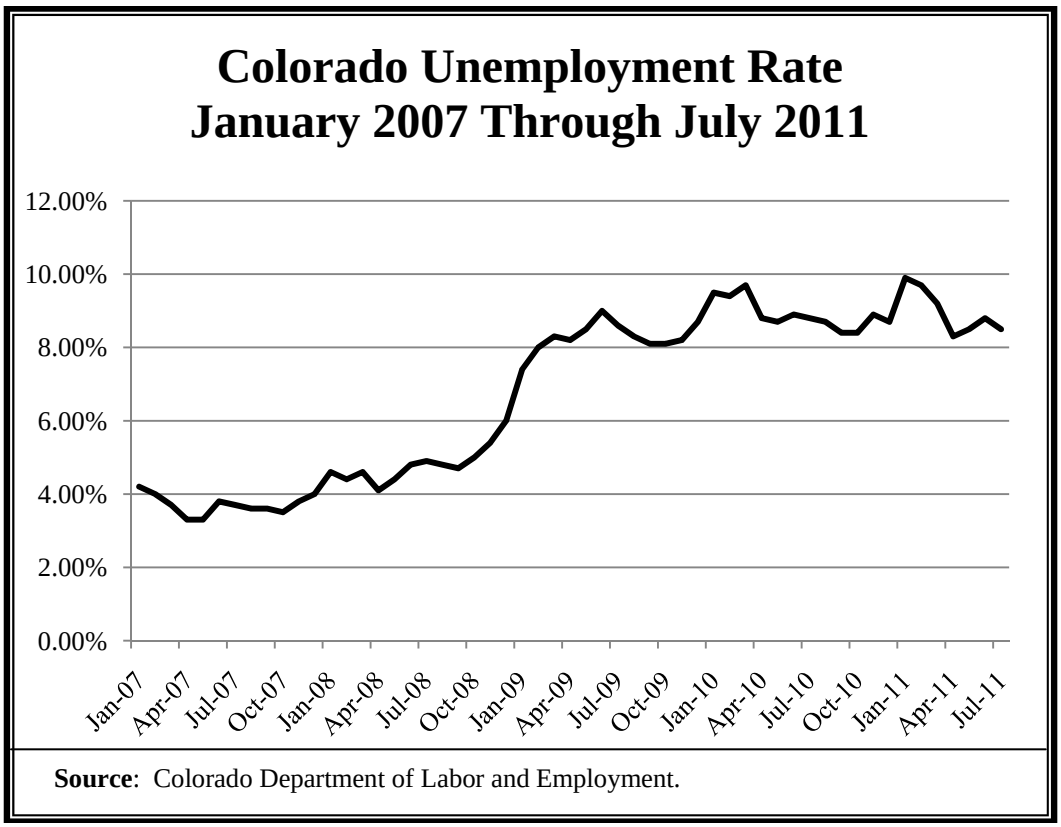
Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
4	43	Improve the efficiency of claims review by (a) reprogramming the Colorado Unemployment Benefits System to increase automated processing of claims; (b) making changes to claims filing rules to require claimants to file earlier and ensuring that the deadlines for resolving claims eligibility issues align with federal deadlines; and (c) working with the General Assembly to change statute to allow for the determination of eligibility based solely on the last employer, if the Department's analysis determines that this is in the best interests of the State.	a. Partially Agree b. Partially Agree c. Agree	a. September 2012 b. July 2013 c. July 2013
5	50	Increase the number of overpayments detected and recovered by (a) reviewing the current staffing levels and determining if there are opportunities to reassign additional staff to the Benefit Payment Control unit and (b) giving priority to detecting and collecting more recent overpayments.	a. Agree b. Agree	a. November 2011 b. Implemented
6	54	Improve its customer service functions by (a) eliminating or restricting the use of customer call backs; (b) requiring most claimants to apply for UI benefits online; and (c) implementing strategies to increase the number of staff answering customer service calls, including evaluating the UI Program's flex schedule policy.	a. Agree b. Partially Agree c. Agree	a. March 2012 b. May 2012 c. July 2012

Overview of the Unemployment Insurance Program

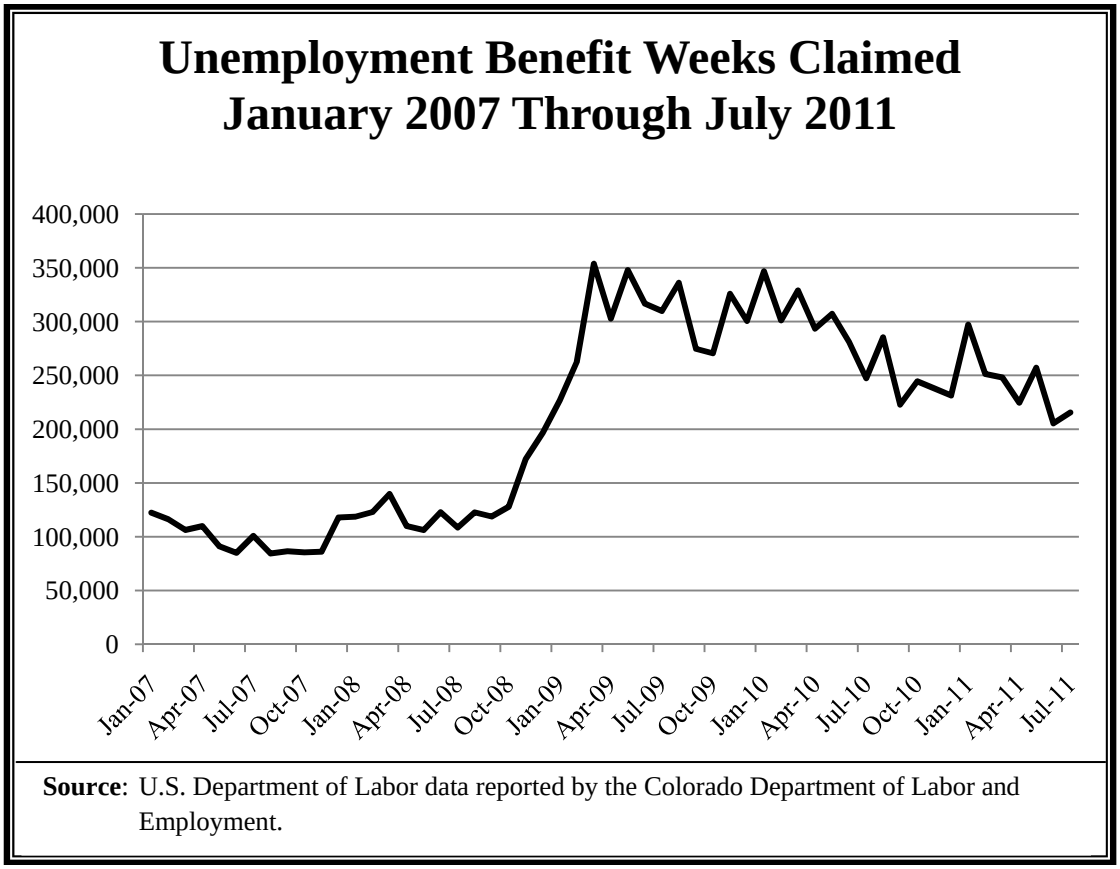
Chapter 1

The Unemployment Insurance Program (UI Program), within the Colorado Department of Labor and Employment (the Department), provides financial assistance to workers who lose employment through no fault of their own. Under the program, employers pay premiums for each employee, which the UI Program uses to provide benefits payments to unemployed workers. According to statute (Section 8-70-102, C.R.S.), the key purposes of the program are to stabilize the economy during periods of high unemployment, maintain purchasing power, and support workers who lose their jobs.

As shown in the following graph, Colorado's unemployment rate has increased significantly over the last 4 years due to the national economic recession that began in 2007. From January 2007 through July 2011, the percentage of unemployed workers in Colorado increased from 4.2 percent to 8.6 percent, peaking at 9.9 percent in January 2011. As of July 2011, out of the Colorado labor force of about 2.7 million, a total of 231,000 (8.6 percent) workers were unemployed.



The large increase in unemployment has led to a corresponding increase in unemployment claims processed by Colorado's UI Program. A key measure of claims volume is the number of weekly benefits claims per month. Because claimants must file requesting benefits for every week that they remain eligible, a single claimant can claim several weeks each month. As shown in the graph below, from January 2007 to March 2009, the weeks of unemployment claimed each month increased from about 122,000 to 354,000, an increase of 190 percent. The weeks of unemployment claimed each month fell to about 216,000 in July 2011, which still represents a significant increase over the level of weeks claimed each month in Calendar Years 2007 and 2008.



Source: U.S. Department of Labor data reported by the Colorado Department of Labor and Employment.

Federal Unemployment Insurance Framework

State unemployment insurance (UI) programs operate under federal-state partnerships. Federal laws establish broad UI coverage and benefits provisions, the federal unemployment tax base and rate, and administrative requirements. Within this framework, states design the key components of their own UI programs, such as benefits eligibility criteria, benefits amounts, and premium rates assessed to employers to support the benefits paid. Three agencies within the federal government are charged with different responsibilities related to unemployment insurance, as described below.

- **U.S. Department of Labor (USDOL).** USDOL oversees states' compliance with federal requirements related to unemployment insurance and distributes funding to states to administer their UI programs. Among its responsibilities, USDOL ensures that state laws, regulations, rules, and operations comply with federal law; sets overall policy for administering

the programs; monitors states' performance; and provides technical assistance to states, as needed.

- **Internal Revenue Service (IRS).** At the time of our audit, the Federal Unemployment Tax Act authorizes the IRS to collect an annual federal tax from employers of 6.2 percent on wages up to $7,000 paid to an employee each year. An offset credit of up to 5.4 percent is available to employers if they pay their unemployment taxes in a timely manner and their state complies with federal requirements. Because the State is in compliance with federal requirements, Colorado employers receiving this credit pay a net tax rate as low as 0.8 percent.

- **U.S. Treasury.** The U.S. Treasury manages the federal UI Trust Fund, which consists of 53 accounts for states and U.S. territories and six additional federal accounts. Premiums collected by states' UI programs are deposited in each state's UI Trust Fund account and are held by the U.S Treasury until they are used to pay UI benefits. Federal unemployment taxes collected by the IRS are deposited into three of the federal accounts and are used to (1) finance the administration of state UI and employment services programs, (2) reimburse states for the federal share of extended benefits (which we describe later in this chapter), and (3) provide loans to states with insufficient reserves in their trust funds to cover benefits.

Eligibility Requirements

As previously mentioned, federal law outlines general eligibility requirements for UI benefits, and each state is responsible for establishing eligibility laws within the general framework. In Colorado, the Colorado Employment and Security Act (Sections 8-70-101, et seq., through 8-82-101, et seq., C.R.S.), House Bill 06S-1023 (Sections 24-76.5-101, et seq., C.R.S.), and Department regulations provide eligibility rules for UI benefits. Generally, to receive benefits, claimants must:

- **Earn Wages**. Claimants must have earned at least $2,500 in wages through qualified employment during the "base period," which is the first four completed calendar quarters within the last five completed calendar quarter period. In some cases, claimants may instead qualify using an "alternative base period," which is the four most recent completed calendar quarters.

- **Be Unemployed Through No Fault of Their Own**. Claimants who are fired for good cause or who voluntarily quit their jobs are generally not eligible for UI benefits.

- **Be Able to and Available for Work**. If claimants cannot work due to illness or injury, or are not available for reasons such as lack of transportation, child care responsibilities, or enrolling in an academic program, they are generally not eligible for benefits.

- **Be Legally Present.** Claimants must provide proof that they are lawfully present in the United States before they can receive benefits payments.

- **Seek Employment**. With some exceptions, program rules require claimants to make five job contacts each week to receive benefits.

- **Be Willing to Accept Work.** If claimants are offered work of an equal or higher skill level than their previous employment and refuse the offer, then they are typically not eligible to continue to receive UI benefits.

Though claimants must generally meet these requirements to receive benefits, statute provides numerous exceptions. For example, if claimants quit employment due to reduced wages, harassment, or an unsafe work environment, they may still qualify for benefits.

Colorado offers two types of unemployment benefits, regular and extended, to eligible individuals. Regular benefits are available to all claimants for up to 26 weeks and are paid by the State with monies in its federal UI Trust Fund account. Extended benefits beyond these initial 26 weeks may be authorized by federal or state law during periods of high unemployment. Federal and state extended benefits were authorized in Colorado through December 2011 and allowed some claimants to receive benefits for as long as 99 weeks if their periods of unemployment corresponded with federal and state extended benefits time lines.

Unemployment Insurance Program Organization

During Fiscal Year 2011, the UI Program employed about 600 full-time-equivalent (FTE) staff. As of July 2010, the UI Program was composed of eight operating branches responsible for different aspects of the program, which we describe below.

- **Benefits (313 FTE)—**Responsible for accepting applications for benefits, processing claims, and issuing decisions on claims. Also operates the customer contact center, which takes claims and assists claimants with questions or problems regarding their claims by phone.

- **Appeals (64 FTE)—**Conducts hearings to make final eligibility decisions on processed claims that have been appealed by either the claimant or the claimant's employer.

- **Support Services (90 FTE)—**Identifies and recovers overpayments, processes completed benefits eligibility forms provided by claimants and employers, maintains employer and claimant records, verifies the legal presence of alien claimants, and provides administrative support.

- **Staff Services (19 FTE)—**Conducts quality assurance reviews of UI Program activities and develops and communicates program policy to staff.

- **Telephone Operations (11 FTE)—**Develops and maintains the UI Program's phone systems that claimants use to file initial claims, obtain information about their claims, file for weekly benefits, and make changes to their accounts. Also provides technical support to customer contact center staff.

- **Technology (21 FTE)**—Develops and maintains the internal and external electronic applications used by the UI Program to process and pay benefits claims. This includes maintaining the Colorado Unemployment Benefits System (CUBS), which is the UI Program's main database, in conjunction with the Governor's Office of Information Technology. CUBS collects and stores claimant information, automatically flags certain eligibility issues, and processes claims payments. Staff rely on CUBS as the primary source of information about claims and use the system to identify possible eligibility issues and ensure that payments are timely.

- **Internet Operations (2 FTE)—**Maintains the UI Program's website that claimants use to access information on their claims, apply for benefits, modify claim information, or acquire general information to learn how the UI Program works.

- **Employer Services (86 FTE)—**Determines and collects employer premiums, and collects wage reports.

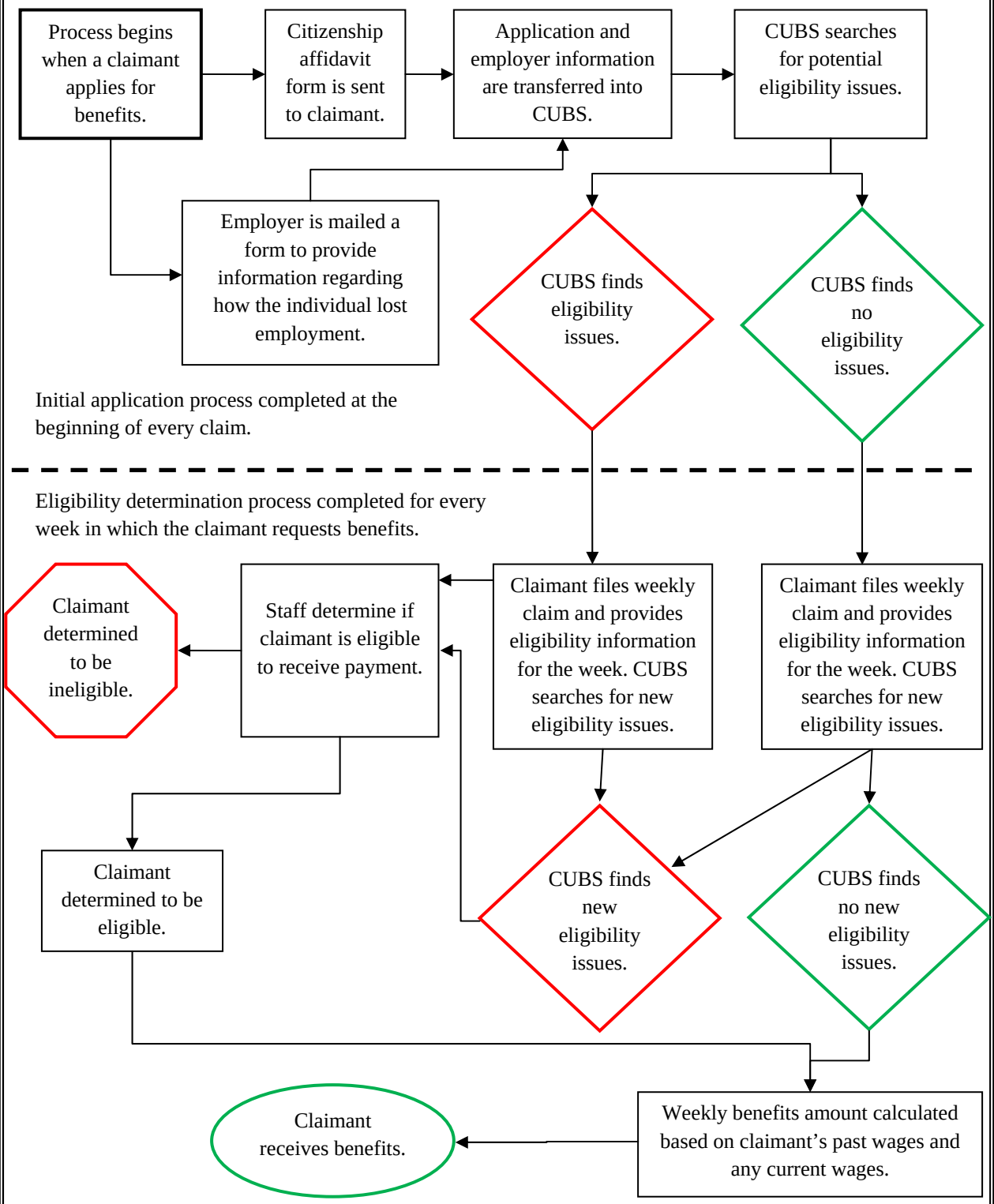
During our audit, the UI Program was in the process of evaluating its organizational structure. In August 2011, after we completed the fieldwork stage of the audit, the UI Program announced a major program reorganization plan. As a result, the number of operating branches was reduced from eight to four, which now include (1) Claimant Services; (2) Employer Services; (3) Appeals; and (4) Policy, Integrity, and Program Support. The reorganization was designed to better align organizational activities, reduce operating costs, improve

communication, and increase the number of staff delivering direct services to the public.

Claims Processing

The UI Program is responsible for ensuring that claimants meet eligibility requirements and are paid in a timely manner. To receive benefits, claimants must complete a two-part process. First, claimants must complete an initial new claims application, which the UI Program uses to collect claimants' personal information and determine whether the claimants earned wages in Colorado and lost employment through no fault of their own. Second, claimants must file requests for benefits payments on a biweekly basis. Because several eligibility requirements, such as whether the person was able to and available for work and looked for work, can change on a weekly basis, claimants must provide this information for every week when they file a request for benefits payment, and the UI Program must determine eligibility for each week separately. Though there are some exceptions, the following chart shows the typical process that the UI Program uses to review benefits claims, determine eligibility, and pay claimants. The top half of the chart shows the processes that occur once, when claimants initially apply for benefits, and the bottom half shows the process used to determine eligibility for each week that the claimants request benefits payments.

UI Program Benefits Application Process



Source: Office of the State Auditor's review of the UI Program's application process.

As shown, unemployed workers initially apply for UI benefits using an online application or by calling the UI Program's call center. The application requires claimants to provide their recent work history, the reason they lost employment from each employer, information on their current availability and ability to work, and citizenship status. Once claimants submit the application, the UI Program sends the claimants' most recent and base period employers a form to provide information explaining why the individuals lost employment (e.g., fired, quit, or no work available). The UI Program also sends the claimants an affidavit to provide identifying information and to attest to their legal presence in the United States. If a claimant indicates that he or she is not a U.S. citizen, the UI Program requires the claimant to provide an alien registration number, which the program verifies using a federal immigration database. Information from the online application and forms is then transferred to CUBS, where it is processed electronically to identify any potential eligibility issues, such as the claimant not earning adequate wages or being terminated from employment for good cause. If issues exist, CUBS flags the claim and holds benefits payments until the issues are resolved.

After submitting an initial application, claimants cannot receive benefits until they file a weekly claim requesting benefits. To file a weekly claim, the claimants must complete a form online or provide information through an automated telephone filing system. In each case, the claimants must provide information related to each week for which they are claiming unemployment, including whether they were able and available to work, registered at a workforce center, conducted a job search, or earned any wages during the week. The claimants must continue to file every 2 weeks, providing information for each week claimed, for the life of the benefits claims. This information is also entered into CUBS, and if any new eligibility issues arise based on the claimants' responses, CUBS will place a hold on the claims until the issues are resolved.

A hold may be placed on a claim if the claimant or employer reports information that could make the claimant ineligible for benefits or affect the amount of benefits the claimant can receive. If a hold is placed on the claim, which occurs in about 94 percent of claims, the claim is forwarded to UI staff for further review. UI staff review relevant information related to the claim, contact the claimant and his or her previous employers to obtain detailed information regarding the claim, and apply applicable laws to reach an eligibility decision on the claim. If the claimant is found to be eligible for benefits, he or she will be paid, and each employer for which the claimant lost employment through no fault of his or her own during the base period will have its premium rate adjusted accordingly, with employers that lay off more employees over time generally having to pay higher premiums. If the claimant or employer disagrees with the decision, either may file an appeal.

Once a claimant has filed for weekly benefits and any holds have been removed from the claim, the UI Program will pay the claimant according to a statutorily determined payment formula that is based on the wages earned by the claimant during his or her base period. As required by statute (Section 8-73-102, C.R.S.), the UI Program determines weekly benefits amounts through one of two formulas:

- 60 percent of one twenty-sixth (1/26) of the highest wages earned in two consecutive calendar quarters during the base period. Under this formula, the benefits amount is typically 60 percent of 1-week's wages if wages were constant during the entire 6-month base period.

- 50 percent of one fifty-second (1/52) of the total base period wages. Under this formula, the benefits amount is typically 50 percent of 1-week's wages if wages were constant during the 1-year period.

The Department uses the formula that gives the claimant the higher weekly benefits amount, without exceeding the maximum benefits amount. The weekly maximum benefits amount is adjusted annually based on the State's average weekly wage earned and was $489 during Calendar Year 2010. During the same year, Colorado paid claimants an average weekly benefits amount of $346 and Colorado workers earned, on average, weekly wages of $910.

Fiscal Overview

Funding for UI benefits payments comes from premiums paid by Colorado employers, which employers pay in addition to federal unemployment taxes. The UI Program bases employers' premiums on the number of workers they have hired and laid off in recent years. Employer premiums are deposited in the State's UI Trust Fund, which is held by the U.S. Treasury. Employers also pay federal unemployment taxes, which are deposited into a separate federal account and can be used to pay extended benefits during periods of high unemployment.

From Calendar Years 2006 through 2010, the amount of benefits the UI Program paid to claimants increased significantly. As shown in the following table, total benefits paid increased from about $298 million during Calendar Year 2006 to nearly $2.4 billion in 2010, an increase of about 700 percent. In addition to the large increase in the number of claims filed, total payments increased due to the authorization of federal and state extended benefits, which allows claimants to receive benefits for up to 99 weeks, instead of the normal 26 weeks. Although federal extended benefits are administered by Colorado's UI Program, they are not paid from the State's UI Trust Fund account.

Unemployment Insurance Payments, Calendar Years 2006 Through 2010[1] (Dollars in Millions)

2006	2007	2008	2009	2010	Percentage Change
$297.6	$314.1	$515.1	$1,875.6	$2,374.2	698%

Source: Colorado Department of Labor and Employment.
[1] Includes both regular and state and federal extended benefits payments.

As discussed in our *Evaluation of the Unemployment Insurance Trust Fund* (June 2010), due to the high volume of benefits payments and declining premium collections in recent years, Colorado's UI Trust Fund has become insolvent. As a result, the State must pay benefits claims using federal funds, which must be repaid. As of September 2011, the State's UI Trust Fund deficit was $289 million. During the 2011 Legislative Session, the General Assembly passed House Bill 11-1288, which makes changes to the calculation of employer premiums to address trust fund solvency issues.

The UI Trust Fund cannot be used to pay the program's administrative costs. Instead, as shown in the table below, federal grants funded $40.7 million (83 percent) of the $49.2 million that the UI Program used to administer the program during Federal Fiscal Year 2011. In addition to federal funding, the UI Program receives cash funds generated by statutory fees paid by employers based on their payrolls. These fees are deposited in the Employer Support Fund and the UI Revenue Fund and can be used to fund the administrative costs of the program. The UI Program also received temporary increases in administrative funding in Federal Fiscal Years 2009 and 2010 from the federal American Recovery and Reinvestment Act of 2009 (Recovery Act). Recovery Act funds allowed the UI Program to increase staffing to help accommodate the large influx of UI claims caused by the recent economic recession. However, Recovery Act funds have been exhausted. Overall, the UI Program experienced a 31 percent decrease in total funding for administrative costs from Federal Fiscal Years 2010 to 2011.

Unemployment Insurance Program Revenue and Full-Time-Equivalent Staff Federal Fiscal Years 2008 Through 2011 (Dollars in Millions)

	2008	2009	2010	2011	Percentage Change
Federal Grant Funds	$ 35.3	$ 50.6	$ 53.1[1]	$ 40.7[1]	15%
Federal Recovery Act Funds	$ 0.0	$ 1.1	$ 7.5	$ 0.0	-
Cash Funds	$ 7.4	$ 9.9	$ 10.1	$ 8.6	16%
Total	**$ 42.7**	**$ 61.6**	**$ 70.7**	**$ 49.3**	**15%**
FTE[2]	440.1	493.6	660.0	586.0[3]	33%

Source: Colorado Department of Labor and Employment.
[1] Estimates provided by the Colorado Department of Labor and Employment.
[2] FTE levels provided for state fiscal years except as noted.
[3] FTE levels as of August 2011.

Audit 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 state government. Audit work was performed from September 2010 through May 2011. We acknowledge the cooperation and assistance provided by staff at the Department of Labor and Employment.

The objective of the audit was to determine if the Department has sufficient controls for ensuring that the UI Program makes timely and accurate UI benefits payments to eligible claimants. Specifically, we evaluated whether the UI Program has:

- Implemented sufficient procedures for verifying that UI claimants are legally present in the United States, as required by House Bill 06S-1023.
- Established adequate controls over the claims application process to prevent improper benefits payments.
- Instituted procedures to ensure that claims review processes are fair, timely, and accurate and in accordance with state and federal laws.
- Established effective mechanisms for identifying and recovering improper payments.

To accomplish our audit objectives, we interviewed and observed program staff, reviewed the program's policies and procedures, analyzed program data, and mapped out the program's processes to identify opportunities to increase efficiency and effectiveness. Our audit work did not include a review of the methods the UI Program employs to charge and collect UI premiums from Colorado employers or of the claims appeals process.

Our testing of eligibility controls included a review of three samples. First, we sampled 56,000 claimants paid during the last week of December 2010 to determine if the Department complied with House Bill 06S-1023's requirements. We took our sample from the last week of December 2010 to ensure that the sample contained as many active claimants as possible. We subsequently verified that this week of claims payments did not exhibit different characteristics than other weeks' claims payments. From our original sample of 56,000 claimants, we then selected a random, statistically valid sample of 213 claimants to perform additional testing to determine whether claimants provided identification acceptable under House Bill 06S-1023. Our sample was designed to allow the extrapolation of the results to all claimants paid during Calendar Year 2010. Finally, we randomly selected 100 claimants who were paid benefits in December 2010 to determine if they had returned the paper affidavit form attesting to their lawful presence in the country.

We conducted the 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 evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Lawful Presence Controls

Chapter 2

As discussed in Chapter 1, Unemployment Insurance Program (UI Program) claimants must meet several requirements to be eligible to receive benefits. In this chapter, we discuss the requirement that claimants be lawfully present in the United States. House Bill 06S-1023 (Section 24-76.5-101, et seq., C.R.S.) and federal law prohibit the payment of public benefits, including unemployment insurance (UI) benefits, to individuals who are not lawfully present in the United States. We reviewed the UI Program's controls designed to ensure that only lawfully present individuals receive UI benefits and assessed whether these controls are effective and comply with state and federal laws. Specifically, we observed and interviewed staff responsible for verifying lawful presence, reviewed program policies and procedures, evaluated system controls, and analyzed claims data. Overall, we found that the UI Program's application procedures do not always ensure that claimants comply with state and federal laws designed to verify that individuals applying for public benefits are lawfully present in the United States.

Both state and federal laws provide specific procedures that state agencies providing public benefits must follow to confirm that claimants are lawfully present. As shown in the table below, not all of House Bill 06S-1023's provisions are required by federal law. However, federal laws allow states to develop their own procedures to affirm lawful presence as long as they do not conflict with federal law. Therefore, all of the following requirements apply to Colorado's UI Program.

Unemployment Insurance Program State and Federal Lawful Presence Requirements		
Requirement	**State Law (House Bill 06S-1023)**	**Federal Law**
Claimants must provide social security numbers.		X
Claimants must indicate whether they are U.S. citizens.	X	X
Claimants must attest to being lawfully present.	X	X
State agencies must collect and verify alien registration numbers from claimants who indicate that they are not U.S. citizens.	X	X
Claimants must provide one of several acceptable forms of identification, such as a valid Colorado driver's license or identification card, military or coast guard identification card, Native American tribal document, or other documents acceptable under Department of Revenue rules.	X	
Source: Section 24-76.5-101, et seq., C.R.S., and 8 USC 1611.		

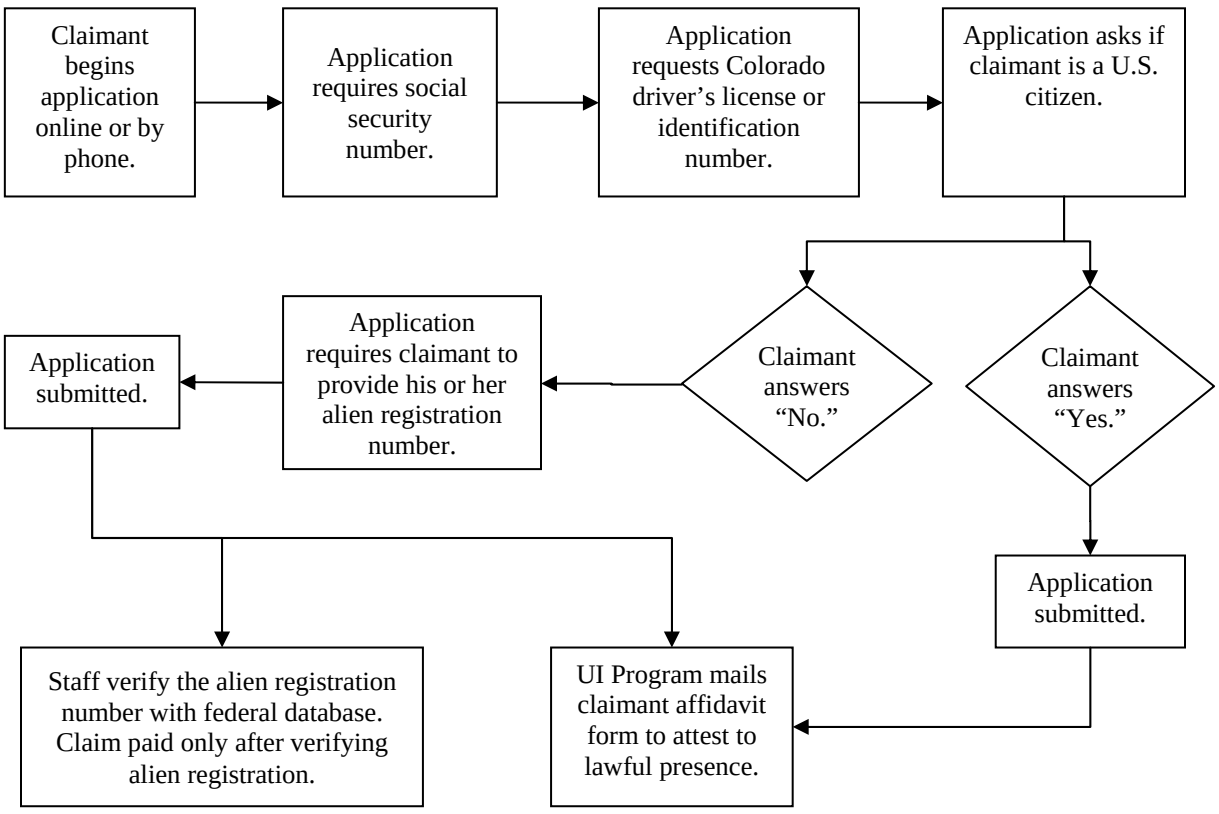
In 2006, the Colorado Office of the Attorney General provided all state agencies with informal guidance to assist agencies in interpreting and implementing the requirements of House Bill 06S-1023. According to this guidance, agencies are not required to collect the identification documentation, such as a Colorado driver's license, from claimants in person. Instead, agencies may develop alternate procedures for collecting the identification as long as they have a process for verifying that the person applying for benefits is the rightful owner of the identification document used to show lawful presence. To assist agencies in verifying the validity of Colorado driver's licenses and identification cards, the Department of Revenue (DOR) created an online system, available to all state agencies, that allows agency staff to immediately determine whether an identification document was issued to the same person applying for benefits, and whether the identification document is currently valid (i.e., not expired, suspended, revoked, or cancelled). In addition, the guidance provided by the Office of the Attorney General indicated that claimants may submit affidavits affirming legal presence through online application systems as long as the benefits application requires the claimants to provide an electronic signature.

Based on our review of House Bill 06S-1023 and guidance provided by the Office of the Attorney General, because the UI Program uses an online application form and does not collect identification documentation in person, it must have procedures in place to verify that each claimant is the rightful owner of the identification document he or she uses to show lawful presence.

We reviewed the UI Program's procedures to ensure that claimants are legally present, as required by state and federal laws. As discussed in Chapter 1, claimants can apply for benefits online or over the phone. As shown in the

flowchart below, when claimants apply for benefits, the UI Program's application process requires that they provide a social security number and requests their Colorado driver's license or identification card number. In addition, the application asks claimants whether they are U.S. citizens. If the claimants indicate that they are not U.S. citizens, the application requires that they provide their alien registration number, and a hold is placed on the claim until UI staff verify the alien registration number using a federal database. After the claimants submit the application, the UI Program mails the claimants an affidavit to affirm citizenship status and to provide additional identification information.

Unemployment Insurance Program Lawful Presence Application Controls



Source: Office of the State Auditor's review and observation of UI Program controls.

During the audit, we identified two control weaknesses that impact the UI Program's ability to ensure that claimants are legally present. Specifically, the UI

Program does not require applicants to provide an attestation affirming legal presence, and the UI Program's procedures do not ensure that claimants provide valid identification, as required. We discuss these concerns below.

Attestation Controls

As discussed above, House Bill 06S-1023 and federal law require claimants to affirm that they are legally present in the United States as a condition of receiving benefits. The UI Program has two procedures that are intended to ensure that claimants attest to being legally present in the United States. First, the UI Program requests that claimants provide a signed affidavit form attesting to their legal presence in the United States and, second, the program requires that claimants answer a question regarding their citizenship during the application process. Overall, we found that most claimants attested to being legally present in accordance with House Bill 06S-1023 and federal law; however, we found weaknesses in both of the UI Program's procedures that could allow claimants to receive UI benefits without affirming their legal presence in the United States. Further, we found that the procedures are duplicative and that with changes to its application, the UI Program could reduce staff workload while still ensuring that all claimants meet House Bill 06S-1023 and federal requirements.

Affidavit Form. During the audit, we reviewed a sample of 100 claimant files from claims paid during December 2010 to determine whether each claimant had submitted the affidavit form attesting to legal presence. We found that 98 of the 100 claimants sampled returned the form. Thus, it appears that most claimants are meeting the requirements of House Bill 06S-1023 and federal law to affirm their legal presence in the United States. However, the UI Program's controls over the affidavit process do not ensure that all claimants affirm legal presence. Historically, the UI Program did not pay benefits to claimants until they returned the signed affidavit affirming their legal presence in the United States. If claimants did not return the affidavit forms, the UI Program would place a hold on the claims, and UI staff would follow up with the claimants to obtain the affidavits. However, in February 2009, UI Program management instructed staff to no longer place holds on claims when claimants do not return the affidavit. Although the UI Program has continued to indicate to claimants since February 2009 that the affidavit form is required, claimants can now receive UI benefits even if they do not return a signed affidavit. Therefore, the UI Program cannot rely on the current procedure to ensure that all claimants affirm legal presence.

Application Citizenship Question. According to informal guidance provided by the Office of the Attorney General, agencies can comply with House Bill 06S-1023's affidavit requirement through online applications as long as the application requires claimants to affirm their lawful presence and complete an electronic signature. The UI Program's application during the period we reviewed asked

claimants if they were U.S. citizens and included an attestation that was intended to require claimants to affirm that all the information they provided on the application, including their citizenship status, was true. However, the UI Program's application did not ensure that claimants affirmed their lawful presence. Specifically, if claimants indicated that they were not a U.S. citizen, they were asked to provide an alien verification number but were never required to positively affirm their legal presence, as required by both House Bill 06S-1023 and federal law. In addition, the attestation language intended to require claimants to affirm that the information they provided on the application is true contained ambiguous language. Specifically, the two responses available to applicants following the attestation language read, "Yes, I want to sign up for unemployment" or "No, I do not want to sign up for unemployment." Thus, it was not clear that the claimants were actually affirming that all information they provided was true and not simply stating that they wanted to apply for benefits.

Following our review, the UI Program changed the language in its application. However, we found that, as of August 2011, the new language in the application still does not require the claimants to directly state that they are lawfully present. Specifically, the application requires claimants to mark a checkbox affirming their understanding that they "*must* be a U.S. citizen or legal permanent resident or be lawfully present in the United States according to federal law (emphasis added)." Thus, the claimants appear to be affirming that they understand the legal requirement, but not that they are actually legally present.

Finally, although the UI Program must have a process in place requiring claimants to affirm their lawful presence to comply with state and federal laws, we found that the affidavit and application procedures described above are duplicative. Specifically, both procedures are intended to collect information from claimants about their citizenship status and to ensure that claimants affirm their legal presence in the United States. Therefore, we believe that both procedures are not necessary, provided that the UI Program takes steps to address the problems we discussed above. As a result, the UI Program has an opportunity to reduce its current workload. For example, currently UI Program staff must scan each affidavit form received from claimants and add the documents to claimants' files. By contrast, if claimants were to affirm citizenship online or during a recorded phone statement when they apply for benefits, the UI Program would have an electronic record of the affirmation without having to dedicate staff time to processing affidavit forms. According to House Bill 06S-1023, agencies may adopt alternative procedures to collect an affidavit form, as long as the alternative procedures are no less stringent. Further, as previously mentioned, informal guidance provided by the Office of the Attorney General indicates that collecting affidavits electronically would be an acceptable alternative. Thus, if the UI Program made changes to the application language to address the problems we identified above, the UI Program would no longer need to request that claimants send in signed affidavits, which could reduce workload. We discuss this reduction

in workload further, in conjunction with other opportunities to reduce the number of forms processed by the UI Program, in Recommendation No. 3.

Recommendation No. 1:

The Department of Labor and Employment (the Department) should ensure that unemployment insurance claimants meet the requirements of House Bill 06S-1023 and federal law for attesting to their lawful presence in the United States by:

a. Changing the language in the Unemployment Insurance Program application form so that claimants are clearly affirming through the application that they are legally present in the United States.

b. Requiring all applicants to affirm legal presence before receiving benefits.

c. Eliminating the use of the current paper affidavit form for affirming legal presence.

Department of Labor and Employment Response:

a. Agree. Implementation date: December 2011.

   We will tighten the language on the current online initial claim application. Wording will clearly demonstrate that claimants not only affirm that they understand the legal requirement, but also that they attest that they are actually legally present.

b. Agree. Implementation date: December 2011.

   Most claimants file online, and they will be required to affirm lawful presence in order to complete the online application. All claimants who file over the telephone will attest to their legal presence and those responses are already being recorded.

c. Partially agree. Implementation date: December 2011.

   The Department will mail the affirmation of legal presence form to claimants who file a claim over the telephone to ensure the integrity of the telephone recordings and because recordings are stored for only 10 to 11 months due to capacity issues. The call center script will be changed to be more specific. We will eliminate sending forms to those who apply online once our language has been changed.

Identification Controls

When claimants apply for benefits, the UI Program requires that they enter a nine-digit Colorado driver's license or identification number. To determine whether claimants provided valid driver's license or identification numbers, as required by House Bill 06S-1023, we reviewed the driver's license numbers on file for a sample of about 56,000 paid claimants from the last week of December 2010, which represents about 20 percent of the 277,000 total claimants who received unemployment benefits in Calendar Year 2010. We found that about 4,800 (9 percent) paid claimants had provided clearly invalid numbers, such as "000000000." Our results are consistent with similar testing conducted by the UI Program. For example, during Calendar Years 2006 through 2009, the UI Program found that about 6 percent of the claimants it sampled did not provide a valid identification number.

In addition, we selected a statistically valid sample of 213 claimants, drawn from our original sample of 56,000, to determine how many of these claimants had provided or could provide acceptable identification under the requirements of House Bill 06S-1023. We chose a statistically valid sample so that we could extrapolate our error rate to the entire population of Calendar Year 2010 claimants.

We tested whether the 213 claimants in our sample had complied with House Bill 06S-1023's identification requirements by first matching the driver's license or Colorado identification number they provided on their UI Program claim application to DOR records. If DOR did not have a record of the claimants' having been issued the number they provided to the UI Program, or if the number provided to the UI program was for an invalid license and DOR had no other record of valid identification, we then requested that the UI Program follow up with the claimants. Specifically, the UI Program asked each of these claimants to provide a photocopy of one of the forms of identification acceptable under House Bill 06S-1023. At the completion of this process, we were unable to establish any record of acceptable identification for 25 of the 213 claimants in our sample. Because our sample was statistically valid, we were able to extrapolate our findings to the entire Calendar Year 2010 population. Based on this process, we estimate that in Calendar Year 2010, as many as 8,900 (3 percent) of the 277,000 total paid claimants did not or could not provide acceptable documentation to comply with House Bill 06S-1023 requirements. We were also able to estimate that the UI Program paid about $60 million, or about 3 percent of the $2.4 billion in state and extended UI benefits paid in Calendar Year 2010, to these claimants who did not or could not meet House Bill 06S-1023's identification requirements and, therefore, should not have received benefits.

It is important to note that we could not conclude whether the claimants who were unable to fulfill House Bill 06S-1023's requirements were lawfully present in the United States. Specifically, the inability to provide the identification documents required by House Bill 06S-1023 does not, by itself, prove that an individual is in the United States illegally. Ultimately, lawful presence is determined by federal law and administrative proceedings.

We identified three weaknesses in the UI Program's processes that increase the risk that claimants will not provide the identification documentation required by House Bill 06S-1023 before receiving benefits, as described below.

- **The UI Program has no mechanism to flag claims when claimants provide invalid identification numbers**. The online application system is not programmed to flag claims when claimants provide clearly invalid numbers, such as "000000000," or other numbers that do not conform with DOR's numbering system for Colorado driver's licenses and identification cards. Further, UI Program staff responsible for taking claims applications over the phone ask for the claimants' Colorado driver's license or identification numbers as part of the benefits application process. However, if the claimants indicate that they do not have a Colorado identification number available, UI Program management instruct agents to enter "000000000" or "999999999" into the identification field and allow claims to move forward without requiring any identification. These claims are not flagged for later follow up and review to ensure that the claimants provide acceptable identification.

- **The UI Program does not verify that the Colorado identification numbers provided by claimants correspond with valid identification documents on file with DOR.** As a result, the UI Program cannot ensure that claimants do not provide fictitious or invalid numbers or numbers for identification documents that do not belong to them.

- **The UI application does not provide instructions for applicants who do not have a Colorado driver's license or identification card.** Although House Bill 06S-1023 and DOR regulations allow applicants for public benefits to provide several forms of identification other than a Colorado driver's license or identification card, during our review the application did not provide a method for applicants to provide these documents. This is particularly problematic for out-of-state applicants, who can apply for benefits in Colorado as long as they worked in Colorado during the base period that determines UI eligibility. In Calendar Year 2010, about 6 percent of Colorado's UI claimants resided in other states, but these claimants have not been able to provide out-of-state identification on the application and may have entered invalid

identification numbers, such as "000000000," on their applications to move their claims forward. Following our review, the UI Program changed its application to allow claimants to indicate that they do not have a Colorado driver's license or identification card. However, there is still no procedure in place to follow up with these applicants to collect and verify their alternative identification information.

UI Program management indicated that they do not currently verify identification provided by claimants and did not deny any claimants benefits based on the verifications they conducted on samples of claims from Calendar Years 2006 through 2009. According to management, the UI Program does not conduct verifications because management do not believe that this procedure is required by House Bill 06S-1023 and are concerned that doing so would be time consuming and could place an undue burden on claimants, which would violate federal law. Further, management are concerned that some of the claimants' driver's license numbers may be invalid for reasons not related to lawful presence (e.g., revoked or suspended license) and that these reasons might not be appropriate grounds to deny UI benefits.

We question whether the UI Program's current procedures can accomplish the purpose of House Bill 06S-1023 without verifying that the Colorado identification numbers provided are valid. As previously mentioned, according to guidance provided by the Office of the Attorney General, agencies must have procedures to ensure that the person applying for benefits is the rightful owner of the document he or she presents to confirm lawful presence. Further, DOR regulations indicate that any Colorado identification used to confirm lawful presence must be current (i.e., not invalid). Although UI Program management's concerns regarding the time it would take to verify identification documents are understandable, it is important that the UI Program take steps necessary to comply with all requirements related to the verification of lawful presence. If necessary, the UI Program should seek legal guidance to specifically determine what application controls it should have in place to meet House Bill 06S-1023 requirements.

Recommendation No. 2:

The Department of Labor and Employment (the Department) should ensure that unemployment insurance (UI) claimants meet the requirements of House Bill 06S-1023 and federal law for affirming their lawful presence in the United States by:

a. Requiring all claimants to provide the number of their valid Colorado driver's license or Colorado identification card, or a copy of other documents acceptable under House Bill 06S-1023, before paying benefits.

In addition, the Department should establish a process to collect acceptable forms of identification other than a Colorado driver's license or identification card and provide claimants with instructions on the application for submitting this documentation.

b. Establishing procedures to verify that the person applying for UI benefits is the same person depicted by the identification number or document that the person provides on his or her application. These procedures could include verifying all Colorado driver's license and identification numbers provided by claimants using Department of Revenue records. If necessary, the Department should seek legal counsel from the Office of the Attorney General to clarify the procedures that the Unemployment Insurance Program must follow to satisfy House Bill 06S-1023 while complying with federal requirements.

Department of Labor and Employment Response:

a. Agree. Implementation date: December 2012.

The Department will require all claimants to provide the number of their valid Colorado driver's license or Colorado identification card, or a copy of other documents acceptable under House Bill 06S-1023, before paying benefits. The Department will develop a process and an IT plan that will include mechanisms for flagging claims with invalid identification numbers for follow up and instructions for applicants who do not have a Colorado driver's license or identification card. The Department is concerned that federal guidelines for first pay promptness will be negatively impacted for claimants who are legally present but do not supply the required documentation in a timely manner.

b. Agree. Implementation date: December 2012.

Working with the Department of Revenue, we will establish procedures to verify that the person applying for benefits is the same person depicted by the identification number or document that the person provides on his or her application. We will work with the Department of Revenue to develop and/or enhance the automated mass interface between the two departments' IT systems.

Benefits Claims Processing and Review

Chapter 3

As discussed in Chapter 1, Unemployment Insurance Program (UI Program) staff are responsible for three key functions related to the payment of unemployment insurance (UI) benefits: (1) reviewing claims for eligibility and paying benefits in a timely manner, (2) recovering funds from claimants who should not have been paid benefits, and (3) providing customer service to claimants who have questions or who may have had holds placed on their claims that prevent them from receiving benefits. During the audit, we assessed the UI Program's performance in each of these areas. Specifically, we observed and interviewed staff, reviewed claims and call center data, and compared the program's claims performance to applicable U.S. Department of Labor (USDOL) standards.

As discussed in this chapter, we found problems in each of the three key functional areas we reviewed. For example, we found that the UI Program has not met USDOL standards for reviewing claims and detecting overpayments. In addition, the program has had difficulty providing claimants with adequate access to customer service through its call center. Together, these problems increase the risk of improper decisions about whether claimants should receive benefits, possibly delay benefits payments, and reduce the program's ability to recover overpayments. Further, when claimants do not have access to customer service, they may not be able to file claims or receive help with questions or holds that are placed on their claims.

UI Program management stated that insufficient staffing to meet a substantial increase in workload is the major cause for the problems identified during our audit. As shown in the following table, the number of benefits weeks claimed per UI Program staff member has increased about 92 percent from Fiscal Years 2008 to 2010, which has led to substantial increases in workload for staff responsible for reviewing claims, identifying improper payments, and providing customer service.

**Comparison of Unemployment Insurance Program (UI Program)
Full-Time-Equivalent (FTE) Staff to Claims Volume
State Fiscal Years 2008 Through 2010**

	2008	2009	2010	Percentage Change
Weeks Unemployment Claimed	1,280,000	2,660,000	3,680,000	188%
UI Program FTE	440.1	493.6	660.0	50%
Weeks Claimed Per FTE	2,908	5,389	5,576	92%

Source: Office of the State Auditor's analysis of Unemployment Insurance Program data.

In addition to a lack of staff to accommodate the increase in claims volume, we also found that the UI Program's processes for processing claims and identifying overpayments are less efficient due to limitations of the Colorado Unemployment Benefits System (CUBS). CUBS was created in 1986 and, according to UI Program management, it does not have the capabilities of modern systems. As a result, UI Program staff must manually account for some claims, necessary programming changes are labor-intensive, and the UI Program's process for reviewing claims takes additional time. The Department began a project in 1999 to replace its entire UI Program computer system, including CUBS, but the project was halted before completion in 2005 due to problems with the contractor. We reviewed this project in our *Genesis Project Memo* (August 2007) and *SUPER System Project Recovery Assessment Memo* (October 2006). According to current management, the UI Program has lacked the funding necessary to replace the system in recent years. However, in September 2011, the UI Program entered a consortium of four states to make improvements to its information technology systems. The federal government has committed $72 million to the consortium as a whole to help fund the project, which is expected to take several years to complete. According to the Department, the UI Program will need to obtain additional funds to finish its UI Program system replacement.

We recognize that staffing levels and CUBS limitations have made it more difficult for the UI Program to keep up with workload, as claims volume has increased to unprecedented levels without similar increases in staff or improvements to CUBS' capabilities. However, during the audit we identified several opportunities for the UI Program to increase efficiency by eliminating labor-intensive processes and reallocating staff. As a result, we estimate that about 38.6 full-time-equivalent (FTE) staff, or 16 percent of the 239 nonmanagement FTE assigned at the time of our audit to the three key benefits payment functions we reviewed, are not being used as efficiently as possible. We also estimate that these 38.6 FTE account for about $2.1 million in salary and benefits costs annually, costs that could be reallocated within the UI Program. We also identified several instances in which the UI Program could make changes to CUBS that would have a significant impact on the UI Program's productivity.

We discuss these problems and opportunities to improve efficiency in the following three sections. In the first section, we discuss the eligibility review process, including the UI Program's procedures for collecting information regarding claims and staff performance in reviewing claims. In the second section, we provide our review of the UI Program's efforts to identify and recover overpayments. In the final section, we assess the customer service provided by the UI Program to claimants through its customer call center.

Eligibility Review

As mentioned in Chapter 1, the UI Program relies on several procedures to ensure that claimants are initially eligible for benefits and continue to be eligible during each week that they remain unemployed and request benefits. First, the UI Program collects information regarding claimants' eligibility for benefits through the initial application, additional forms mailed to the claimants and each of the claimants' base period and most recent employers, and the continued claims filings that claimants complete for each week that they claim benefits. Second, CUBS processes the information and flags claims that have potential eligibility issues. Third, UI Program staff manually review claims with potential eligibility issues, issue decisions regarding claimants' eligibility, and pay eligible claims.

We reviewed each step in the initial and continuing eligibility determination process and compared the UI Program's performance in making eligibility decisions and timely benefits payments to USDOL performance standards. As discussed in the following sections, we identified several opportunities to increase the efficiency and effectiveness of the eligibility process, including reducing the number of forms used to collect information, increasing the amount of information collected online, and strengthening controls over work search requirements. In addition, we found that the UI Program has not met USDOL standards for claims review quality and timeliness and identified several opportunities to improve this process. We discuss these concerns below.

Benefits Application Process

We found that the UI Program could improve the efficiency of its application process and strengthen application controls designed to prevent overpayments by reducing its use of forms to collect information and increasing the amount of information it collects online from employers and claimants.

Eligibility Forms

As previously discussed, the UI Program requires all claimants to complete an online application or have UI Program staff complete the application for them

over the phone. On the application, claimants must provide personal information, information regarding their citizenship status, and information related to their employment and wage history. However, the online application form does not collect all the information from claimants that the UI Program needs to determine eligibility and calculate benefits payments. To collect this additional information, the UI Program uses several forms during the application process, including three frequently used forms described in the table below.

Unemployment Insurance Program
Selected Eligibility Forms

Type of Form	Description
Request for Facts—Employee	Sent to claimants to request additional information about why they no longer work for an employer; the duration of employment; their rate of pay; and any other types of compensation they may have received from the employer, such as vacation, severance, or pension payments. Only sent to claimants when this information is not provided on the initial online application or when the claimants apply over the phone.
Request for Facts—Employer	Sent to all of the claimants' base period employers (i.e., employers for whom the claimants have worked in the first four completed calendar quarters within the last five completed calendar quarter periods) and most recent employers to request information about why the claimants no longer work for the employers, the duration of employment, the rate of pay during employment, and any other types of compensation the employers may have paid to the claimants. One large payroll company currently submits this information electronically and does not receive the form.
Verification of Personal Information (Affidavit Form)	As discussed in Chapter 2, this form is sent to all claimants to verify personal information, obtain attestations of the claimants' being lawfully present in the United States, and collect additional identification information.

Source: Office of the State Auditor's review of Unemployment Insurance Program forms.

As discussed below, we found that the UI Program could lessen workload by eliminating or reducing the use of all three of the forms listed in the table above and instead collecting the information online.

- **Request for Facts—Employee Form—**As of October 2011, the UI Program had implemented changes to its online application to collect all of the information currently collected by the "Request for Facts—Employee" form when claimants apply online. However, when claimants apply by phone, the program still uses the form to collect information regarding claimants' separation from employment. If separation information was collected over the phone along with other application information, the UI Program could significantly reduce the need to use the form.

- **Request for Facts—Employer Form—**We found that other states, such as Florida, South Carolina, and Texas, have UI benefits filing systems on their websites that allow all employers to report the information that Colorado's UI Program collects from employers through the "Request for Facts—Employer" form. In addition, USDOL has worked with states to develop the State Information Data Exchange System (SIDES). SIDES is a web-based system that allows employers to provide relevant information about claimants to state UI programs. USDOL considers the implementation of SIDES as a core strategy for reducing improper UI payments. Currently, only one company submits claimant information electronically to Colorado's UI Program. If the UI Program expanded the use of SIDES or created another online form that all employers could use to provide claimant information to the UI Program, it could eliminate the need to process this form.

- **Verification of Personal Information (Affidavit Form)—**As discussed in Chapter 2, Recommendation No. 1, the "Verification of Personal Information" form could be eliminated if the UI Program modified its application to enable claimants to electronically attest to being lawfully present in the United States.

By eliminating or reducing the use of the three forms discussed above, the UI Program could significantly reduce staff workload. Currently, UI Program staff must sort and scan each form, manually enter the information on the form into CUBS, and add the form to the claimants' files. At the time of our review, the UI Program had 13 FTE dedicated to scanning and processing these forms and other correspondence received by claimants and employers. According to UI Program management, these three forms represent about 80 percent of the workload for these 13 FTE. Therefore, we estimate that if the UI program stopped using the two forms and the affidavit and instead obtained the information provided on the forms electronically, the UI Program could reallocate 10.4 FTE, whose salary and benefits totaled about $487,000 in Fiscal Year 2011, to other program functions.

Layoff Information

Currently, the UI Program's initial application provides a space for claimants to provide a description, in their own words, of why they lost employment if they indicate that they were fired or quit. UI Program staff use this additional information when determining the claimants' eligibility. However, we found that when claimants indicate that they lost employment because of a layoff, the claimants are not given an opportunity to provide additional information about the layoff that would allow UI Program staff reviewing the claims to determine if the claimants truly were laid off and, therefore, are eligible for benefits. In cases in which employers dispute claimants' assertions about being laid off, UI Program staff must contact the claimants to obtain more information about the circumstances leading to the claimants' losing their jobs, which takes additional time. Thus, by adding a space in the initial application to allow claimants to provide more information in their own words when they report being laid off, the UI Program could reduce the processing time for some claims. Due to CUBS limitations, the UI Program did not have information showing the number of claims in which claimants' reported layoffs were disputed by employers and, therefore, we could not measure the potential effect of this change.

Work Search Information

Claimants must look for work during each week in which they receive UI benefits to remain eligible for the program. According to program rules, claimants generally must make contact with at least five employers each week for the purposes of finding employment. In addition, claimants must keep documentation of each contact they make, although currently most claimants are never asked to provide this documentation. The claimants must then report whether they completed a work search for the week when they file for continued benefits. If the claimants fail to conduct the work searches, then the claimants are not eligible for benefits for the week.

We found that the UI Program could improve the information it collects from claimants about their work searches, which could reduce the amount of UI overpayments related to work searches. Currently, claimants can file for continued benefits through either an online form or through an automated phone system. When claimants file for continued benefits online, they are asked, "During this week, did you look for a job?" However, the form never asks the claimants how many job contacts they made or for any detail about the employers they contacted. Thus, if claimants made one job contact during the week, they could truthfully answer "yes" on the online form and receive benefits, even though they did not complete the UI Program's work search requirements. In addition, claimants who file for continued benefits over the phone are asked only

to confirm the number of job contacts they made and are not required to provide any details about the employers contacted.

We found that claimants who do not search for work or do not document their work search as required are currently paid a substantial amount in UI benefits for which they are not eligible. The UI Program performs federally required reviews on a quarterly basis using statistical samples to estimate the amount of state benefits paid to ineligible claimants and determine the causes of the overpayments. According to these reviews, during Calendar Year 2010, the UI Program made an estimated $169 million (19 percent of total state benefits payments) in overpayments. Of this amount, $83 million (49 percent) was paid to claimants who did not fulfill work search requirements. Despite reporting that they completed a work search, these claimants either did not make the required number of job contacts or did not document their work search, as required.

According to UI Program management, reviewing claimant work search records and verifying job contacts is a labor-intensive process. For example, when staff verify work searches, they must contact the claimant to collect documentation of each job contact made and then contact each employer to verify that the claimant contacted the employer regarding a job. Therefore, it is not possible for the UI Program to verify most claimants' reported work search activities. However, by requiring claimants to provide more information about their work search contacts when they apply for continuing benefits, the program may be able to deter some claimants from falsely reporting that they completed the required number of work searches. For example, if the UI Program reminded claimants about the work search requirement and required all claimants to provide the number of job contacts and detailed information for each contact made, such as the employer's name, address, and telephone number, claimants might perceive a greater risk of being caught if they report false information when filing a continued claim. Further, claimants would be more likely to document their work search activities, as required. Deterring even a small percentage of claimants who would otherwise receive improper payments could save a substantial amount of UI benefits from being improperly paid. For example, based on the $83 million in work search-related overpayments in Calendar Year 2010, if work search-related overpayments had declined by just 5 percent, $4.2 million in overpayments could have been averted.

Recommendation No. 3:

The Department of Labor and Employment should improve its processes for collecting information from unemployment insurance (UI) claimants by:

a. Collecting information regarding claimants' separation from employment when they apply for benefits over the phone, and eliminating or reducing

the use of the "Request for Facts—Employee" form during the initial application process.

b. Increasing the number of employers who electronically submit information currently collected by the "Request for Facts—Employer" paper form.

c. Adding an open-ended question to the new UI claims application that asks claimants who report they were laid off to provide more detailed information regarding the circumstances of the layoff.

d. Adding language to the online and telephone-based continued claims filing systems indicating that claimants must conduct a work search, including a minimum number of job contacts, to continue receiving benefits and requiring all claimants to provide the number of job contacts made each week and information for each job contact when they file for continued benefits.

Department of Labor and Employment Response:

a. Partially agree. Implementation date: December 2011.

Currently, approximately 30 percent of claims are filed via telephone. A cost-benefit analysis will be conducted that will compare the cost of mailing and processing the forms versus the cost of staff salaries required to collect the claimants' separation information verbally during the phone calls. The major benefit to mailing the "Request for Facts—Employee" form is that the claimants have the opportunity to provide detailed separation information for consideration during the eligibility and entitlement processing. Also for consideration in the analysis, historical data indicate that verbal collection of this information will add an additional 10-12 minutes to the average call length and, thus, could impact caller wait times.

b. Agree. Implementation date: June 2012.

The UI Program is working on a new system that will allow employers to optionally provide separation information electronically and should have that in place by June 2012. The program continues to collaborate with the U.S. Department of Labor to expand employers' participation with the State Information Data Exchange System. Due to federal requirements to notify employers separately of a claim and of potential charges, and some employers' need for paper processing, we cannot completely eliminate the use of the employer request form.

c. Partially agree. Implementation date: December 2011.

The current online application does not provide an opportunity for detailed information collection on layoff separations and will be phased out by the end of the year. The new online application, however, provides the claimants with seven options to explain the primary reasons for the layoff. These reasons are: lack of work, weather, reduction-in-force, position eliminated, company closed, company moved, and health. We will be adding an open text box to the ISS application form for those who file online. We are unable to add an open text box for people who file by phone.

d. Partially agree. Implementation date: December 2012.

We can add language by December 2011 to both the phone application script and the online application clearly outlining claimants' job search responsibilities to collect benefits. We will also include a form for this data collection in the new UI Handbook by March 2012 with clear language that indicates, if requested, claimants must provide the completed form. Collecting this information online will not be feasible until new technology is in place. We will do a cost-benefit analysis of actually adding this information to the new online application system once the new online employer system is fully up and running. This analysis will be completed by December 2012.

Review of Eligibility Issues

After claimants apply for benefits, CUBS analyzes the information provided by claimants and employers and flags claims that have potential issues that may affect claimants' eligibility for benefits or the amount of weekly benefits they may be paid. UI Program staff review these issues to determine whether the claimants are eligible for UI benefits and to calculate the proper payment amounts. Generally, according to UI Program procedures, claims flagged for potential eligibility issues cannot be paid until they are reviewed by UI Program staff.

Potential eligibility issues can fall into two broad categories: separation issues and nonseparation issues. Separation issues relate to whether the claimants lost employment through no fault of their own, as opposed to quitting or being fired, which would generally make them ineligible for benefits. Nonseparation issues are related to any other type of eligibility requirement, such as the claimants not being able and available for work or not making the required work searches. According to UI Program data, about 94 percent of claims have at least one type

of eligibility issue that requires UI Program staff to manually review the claims. Common eligibility issues include the claimants quitting their jobs, not being able and available to work, and earning additional pay, such as severance or vacation pay, as part of their separation from employment.

USDOL regulations establish standards related to due process, accuracy, and timeliness for states to follow when reviewing claims for eligibility issues. Generally, these standards require staff responsible for reviewing claims to make a reasonable attempt to gather all information necessary to make a decision, properly apply state UI laws in making a decision, and issue a notice of decision to claimants that properly explains the legal basis for the decision.

To measure states' performance in complying with its review standards, USDOL requires each state's UI program to conduct several types of statistically valid quarterly reviews of its eligibility review process, and has established benchmarks to assess the program's performance in each area. These reviews assess both the timeliness and quality of the UI Program's eligibility review process. Federal standards assess timeliness based on the percentage of claimants who receive their first payments on time and also on the amount of time the UI Program takes to make decisions on claims with potential eligibility issues. The standards measure the quality of the UI Program's eligibility decisions based on whether the program followed federal procedural standards for reviewing claims. During the audit, we compared Colorado's UI Program performance to federal standards over the last 5 years, as shown in the following table.

Comparison of Federal Timeliness and Quality Review Standards for Unemployment Insurance Claims Review and Payment to Colorado's UI Program Performance[1] Calendar Years 2006 Through 2010

Type	Description	USDOL Standards	Colorado UI Program Performance Calendar Years 2006-2010				
Timeliness Reviews			**2006**	**2007**	**2008**	**2009**	**2010**
First Payment Timeliness	Measures the timeliness of all first payments made on eligible claims during the quarter.	87% of claims must be paid within 14 days of the first week of eligibility.	90%	91%	89%	*85%*	*84%*
Separation Decision Timeliness	Measures the timeliness of the UI Program's decisions on potential separation issues during the quarter.	80% of issues must be decided within 21 days of detection.	*37%*	*36%*	*37%*	*37%*	*41%*
Non-Separation Decision Timeliness	Measures the timeliness of the UI Program's decisions on potential nonseparation issues during the quarter.	80% of issues must be decided within 21 days of detection.	*69%*	*70%*	*70%*	*64%*	*75%*
Quality Reviews			**2006**	**2007**	**2008**	**2009**	**2010**
Separation Decisions Quality	Measures the quality of the review process the UI Program used to make decisions on a sample of 50 separation issues decided during the quarter.	75% of issues sampled must pass the review.	*40%*	*52%*	*63%*	*55%*	*45%*
Non-Separation Decisions Quality	Measures the quality of the review process the UI Program used to make decisions on a sample of 50 nonseparation issues decided during the quarter.	75% of issues sampled must pass the review.	*47%*	*58%*	*69%*	*69%*	*54%*

Source: U.S. Department of Labor.
[1] Italicized figures indicate that the performance of Colorado's Unemployment Insurance Program did not meet federal benchmarks.

As shown in the table, with the exception of the first payment timeliness standard for Calendar Years 2006 through 2008, the UI Program did not meet any of these federal standards from Calendar Years 2006 through 2010. In particular, the UI Program has struggled to meet the standards for claims with potential separation issues, issuing only 41 percent of those decisions timely and meeting quality

standards only 45 percent of the time in Calendar Year 2010. This compares to the national average of 59 percent of claims that were decided on time and 69 percent that met federal quality standards.

It is important that the UI Program meet federal timeliness and quality standards, because errors and delays in the claims review and payment processes can result in overpayments or underpayments, denial of due process to claimants and employers, and delayed benefits payments. According to reviews conducted by UI Program staff to estimate the amounts and causes of overpayments, during Calendar Year 2010, about 31 percent of all UI Program overpayments were caused or partially caused by errors made by UI Program staff responsible for reviewing claims. Using this percentage, this would represent an estimated $119 million of $382 million in estimated overpayments for Calendar Years 2006 through 2010, including $52 million of the $169 million in overpayments for Calendar Year 2010.

Overall, we identified three problems that appear to contribute to the errors and delays in the UI Program's processing of claims and review of eligibility issues. First, staff do not always gather sufficient information to support their claims decisions. Second, program rules related to claimants filing weekly claims and staff performance standards can delay the processing of claims. Third, statutory eligibility requirements create additional workload for staff. We discuss these problems in the following sections.

Claims Information Gathering

According to the supporting documentation for the UI Program's quality reviews conducted in Calendar Year 2010, a major reason that the UI Program's claims quality scores have not met federal standards is that staff do not always contact all interested parties and/or make a reasonable attempt to gather all information necessary to support their claims eligibility decisions. Specifically, in Calendar Year 2010, UI Program staff did not collect adequate information from the claimants, employers, and/or other parties to support the eligibility decisions made in 182 (46 percent) of the 400 cases reviewed. It is important to note that the failure to collect sufficient information does not conclusively indicate that staff made an incorrect decision. However, the UI Program's quality reviews also found that staff misapplied the law, made inaccurate eligibility decisions, or issued improper notices of decisions in 71 (18 percent) reviewed cases. These decisions were made in error due to staff miscalculating benefits; improperly allowing, postponing, or denying benefits; or not providing accurate information related to the decisions to the parties. Because these quality reviews use a statistically valid sample, the error rates can be extrapolated to the entire population of claims for Calendar Year 2010.

According to UI Program staff, the large volume of claims that they must review increases the difficulty of collecting all the necessary information on claims and still issuing timely decisions, especially when the claimants and employers provide contradictory information about the reasons why the claimants left employment. As previously mentioned, 94 percent of claims require some manual review. We found that the UI Program may be able to reduce workload, and thereby increase the time staff have to review claims, by further automating the claims review process. Specifically, if claimants file a request for continued benefits payments by phone and indicate that they were not able and available to work or did not look for work during the week, CUBS will automatically deny benefits for that week without UI Program staff also looking at the claims. However, because CUBS is not programmed to automatically deny claims when claimants file for continued benefits online and indicate they were unavailable for work or did not look for work, UI staff must review these online claims manually and issue a decision.

According to UI Program management, staff must also manually review claims, regardless of how they are filed, when claimants indicate that they are not registered at a workforce center, which is a requirement to receive UI benefits. Staff indicated that CUBS could be reprogrammed to process both types of eligibility issues described above, although UI Program management believe this change would require significant resources. We estimate that automating the processing of these claims could eliminate the need for staff to manually process about 9 percent of the eligibility issues identified during Calendar Year 2010 and would save the UI Program the equivalent of about 4.2 FTE and $226,000 in salary and benefits annually.

Program Filing Rules

We also found that UI Program rules for filing claims and performance goals for claims eligibility review staff may increase the number of claims that are not paid on time. As discussed in Chapter 1, after claimants complete the initial application, they must also file a request for benefits before they can be paid. According to statute (Section 8-73-107, C.R.S.) and program rules, claimants must make their first request for payment during a 2-week period, which begins 14 days after they submit their initial application and ends 28 days after the initial application.

We found that these rules can cause the UI Program to make untimely first payments of benefits, as measured by federal standards. As applied to Colorado's UI Program, USDOL standards generally require the UI Program to make the first payment of benefits within 28 days of a claimant submitting the initial application. Thus, if a claimant waits the full 28 days after the initial application to file his or her first request for payment, as allowed by program rules, the UI Program would have to pay the claim on the same day that payment is requested

to meet the federal deadline, which does not allow any time for staff to review the claim for eligibility and process payment. According to UI Program management, at a minimum, review staff must make eligibility decisions 2 days before the federal deadline to ensure timely payment.

According to UI Program management, until February 2009, the program required claimants to file a request for benefits within 7 days of the initial application, which resulted in the UI Program making more timely payments. However, in 2009, the program changed the deadline to 14 days to reduce the number of claimants who miss the deadline and require assistance from UI Program staff. Although this change reduced workload by reducing the number of late filers, management indicated that the change may have increased the number of claims that missed federal timeliness deadlines.

We also found that the UI Program's performance standards established for claims review staff can contribute to untimely payments. Program performance standards allow review staff 10 days to resolve eligibility issues on claims, regardless of whether this deadline could result in the claims not meeting the federal standard. As a result, staff could miss the federal time line but meet the UI Program's performance standard. For example, if a claimant filed his or her first request for payment on the 19th day after submitting his or her initial application, according to program performance standards, review staff would have until the 29th day to complete their review of the claim, which is later than the federal standard of 28 days to pay the claim.

Eligibility Law

As previously mentioned, the UI Program has not met federal standards and has performed below the national average on federally required reviews of its claims review process for separation issues. According to UI Program management, a major reason Colorado's UI Program has difficulty handling claims with separation issues is that Colorado's UI laws require more work to determine eligibility than other states' laws. We were able to identify one particular statutory requirement that appears to drive increased workload for Colorado's UI Program. Specifically, statute (Section 8-73-108, C.R.S.) requires the UI Program to determine claimants' eligibility based on all of the claimants' base period and most recent employers. Thus, claims review staff must consider any separation eligibility issues for each employer for whom the claimants worked for more than a 1-year period. By contrast, at least 30 states' UI programs determine eligibility based solely on the most recent employer. Overall, we found that in Calendar Year 2010, claimants had an average of 1.4 employers during their base period. In Calendar Year 2010, having to review issues associated with multiple employers per claim created approximately 18,600 hours of additional work for UI Program

staff, which equates to about nine FTE at a cost of about $582,000 in salary and benefits annually.

If the UI Program sought legislative change so that claimant eligibility was determined based solely on the most recent employer, it could reallocate the nine FTE and $582,000 mentioned above to better meet the federal requirements. However, before pursuing this change, the program would need to evaluate how this change would affect claimants, employers, and the UI Trust Fund. Based on our review, it appears that basing eligibility on the most recent employer would, in some cases, benefit employers and, in other cases, benefit unemployed workers. For example, changing the current system could benefit employers by allowing them to avoid liability and increased premiums when they lay off an employee who is hired and subsequently fired by a second employer for good cause during the same base period. Because the UI Program would base the claimant's eligibility solely on the last employer, the claimant would be ineligible for benefits due to being fired from his or her most recent job and could not claim benefits based on any previous employer during the base period. In other cases, changing the system would benefit unemployed workers by allowing them to receive benefits payments based on all of their previous employers when they were laid off from their most recent job but were fired or had quit previous jobs during the base period, the reverse of the previous example. Therefore, we believe that the UI Program needs to conduct a comprehensive analysis to determine the net effect that any change to Colorado's multiple employer law would have on employers and employees and, ultimately, the UI Trust Fund (i.e., if basing claimant eligibility on the last employer results in more claimants receiving benefits, the UI Trust Fund could be further depleted). With this information, the UI Program could determine whether the benefits of any change in Colorado's multiple employer law would outweigh the disadvantages.

Recommendation No. 4:

The Department of Labor and Employment (the Department) should improve the efficiency and quality of the Unemployment Insurance Program's (UI Program) review of claims eligibility issues by:

a. Reprogramming the Colorado Unemployment Benefits System (CUBS) to allow for the automated processing of claims with issues related to claimants being able and available for work, looking for work, and registering with a workforce center.

b. Making changes to claims filing rules to require claimants to file earlier and reviewing the procedures used to set deadlines for eligibility review staff to ensure that the deadlines for resolving claims eligibility issues align with federal deadlines, when possible.

c. Analyzing the effect of benefits being determined solely on the last employer, and considering the impact to employers, claimants, and the Unemployment Insurance Trust Fund. If it is determined to be in the best interests of the State, the Department should work with the General Assembly to change this statutory requirement.

Department of Labor and Employment Response:

a. Partially agree. Implementation date: September 2012.

   Due to the complexity of the UI Program's aged IT system, the proposed change is time-consuming and competes with other mandatory changes and upgrades for priority. A cost-benefit analysis of this proposed change should be completed to determine if the efficiency gained would exceed that of other already identified priority initiatives. We will also discuss this issue with the multistate consortium to determine feasibility.

b. Partially agree. Implementation date: July 2013.

   The program has already initiated a time and cost estimate for the completion of the necessary automation changes that would be required to allow claimants to file continued claims weekly instead of biweekly. Due to the expense and concerns with system capacity, telephonic continued claims will continue to be filed on a biweekly basis via the phone system. In April 2011, the Department amended the performance plans and procedures of staff to align deadlines for resolving claim issues to meet both Department and federal timeliness standards.

c. Agree. Implementation date: July 2013.

   We have already begun discussions and are analyzing what the impact of this change would be to both claimants and employers, which should be completed by January 1, 2012. We are also considering the impact of changing statutes and, consequently, business requirements for the new system. If we move forward with legislation, the effective date would be upon implementation of the new technology.

Overpayment Detection and Recovery

Overpayments represent a significant concern for Colorado's UI Program. For example, reviews conducted by the program estimate that there were about $169 million in overpayments of UI benefits in Calendar Year 2010, which represents about 19 percent of the $900 million total state benefits payments made that year. As shown in the following table, total overpayments have increased 285 percent from Calendar Years 2006 through 2010, while the amount of overpayments as a percentage of total payments has remained at or above 15 percent during this period. Most overpayments occur either due to claimants providing inaccurate information when they file for benefits, such as failing to disclose wages that they earned while receiving benefits, or due to claimants not fulfilling all requirements for receiving benefits, such as not completing and documenting required work searches. In addition, overpayments can be caused by employers not providing timely information and by errors made by UI Program staff responsible for reviewing claims.

Unemployment Insurance Program Overpayments
Calendar Years 2006 Through 2010
(Dollars in Millions)

Overpayment Cause	2006	%	2007	%	2008[1]	%	2009[1]	%	2010	%	% Change CY 2006 - 2010
Work Search Issues	$ 6.9	16%	$ 34.2	63%	$ 20.6	70%	$ 36.3	42%	$ 83.0	49	1103%
Earned Wages	8.9	20	2.5	5	4.5	15	13.2	15	23.6	14	165
Separation Issues[2]	13.3	30	6.5	12	1.0	3	12.6	15	24.0	14	80
Not Registered at a Workforce Center	2.5	6	4.2	8	0	0	12.6	15	13.0	8	420
Other Pay Upon Separation	4.1	9	2.5	5	2.1	7	8.4	10	11.7	7	185
Inadequate Base Period Wages	0.8	2	0.8	1	0.2	1	2.5	3	4.8	3	500
Claimant not Able and Available for Work	0.4	1	2.6	5	0	0	0	0	1.6	1	300
Other	7.0	16	0.6	1	1.2	4	0	0	7.5	4	7
Total Overpaid[3]	**$ 43.9**	**100%**	**$ 53.9**	**100%**	**$ 29.6**	**100%**	**$ 85.6**	**100%**	**$169.2**	**100%**	**285%**
Total State Benefits Payments	**$291.3**	**-**	**$308.1**	**-**	**$193.9**	**-**	**$511.4**	**-**	**$907.3**	**-**	**211%**
Percentage Overpaid	**15%**	**-**	**17%**	**-**	**15%**	**-**	**17%**	**-**	**19%**	**-**	**4%**

Source: U.S. Department of Labor and Employment.

[1]Because the Unemployment Insurance Program did not complete the required number of claims reviews in Calendar Years 2008 and 2009, the overpayment figures provided are not statistically valid. Further, total payment figures provided are based on insufficient sampling and do not provide complete totals for the year.

[2]Includes claimants found to be ineligible due to the circumstances of their separation (e.g., quit, laid off, or fired) from employment.

[3]Includes only overpayments of regular state benefits. Federal and state extended benefits payments are not included in estimating the amount overpaid.

Overpayments are a common problem across UI programs nationally, with overpayments composing about 11 percent of all state benefits payments in Calendar Year 2010. However, as the table above shows, Colorado's overpayment rate has consistently been higher than 11 percent over the last 5 years. Further, in September 2011, USDOL identified Colorado as one of seven

states with the highest rates of overpayments for the 3-year period of July 2008 to June 2011.

USDOL requires each state to have procedures in place to (1) estimate the overall amount of benefits overpaid in its system and the reasons for the overpayments and (2) review individual claims to identify actual overpayments that can be recovered. The UI Program relies on two staff units to complete these requirements, as follows:

Benefit Accuracy Measurement (Benefit Accuracy) Unit. Benefit Accuracy unit staff review statistically valid samples of paid claims to determine whether each claimant was eligible to receive benefits and whether the proper amount was paid. Based on the errors found in the samples and a federal extrapolation methodology, the Benefit Accuracy unit calculates an estimate of the total amount of benefits overpaid in Colorado for a given year and the reasons that the overpayments occurred. The Benefit Accuracy unit was responsible for identifying Colorado's $169 million overpayment figure mentioned previously.

Benefit Payment Control (Payment Control) Unit. Payment Control unit staff are responsible for identifying and recovering individual overpayments that compose the overall overpayment figure calculated through Benefit Accuracy unit reviews. Staff can use several methods to detect overpayments, including the following:

- **Wage Cross-Matches—**Records of paid claimants are compared to wage records provided to the UI Program by employers to determine if claimants failed to report wages they were receiving while filing for unemployment.

- **New Hire Directory Cross-Matches—**Records of paid claimants are compared to a federal database that records newly hired workers to determine if claimants became employed while filing for unemployment benefits.

- **Tips and Leads—**UI Program staff follow up on information provided by employers and other parties that claimants are fraudulently claiming unemployment benefits.

Once individual overpayments have been detected, Payment Control unit staff are responsible for recovering the funds from overpaid claimants, which can include offsetting future benefits or creating payment plans for former claimants.

Each year, USDOL evaluates the results of states' previous Benefit Accuracy unit reviews to determine the proportion of overpayments that each state could detect and recover through Payment Control unit activities. Overpayments that are

determined to be detectable and recoverable are known as operational overpayments. Based on the amount of operational overpayments that have occurred during previous years, USDOL sets performance standards for each state's Payment Control unit. Generally, to meet the standard, USDOL requires states to identify, but not necessarily recover, between 50 and 95 percent of operational overpayments, measured over the prior 3 years. The USDOL standard for overpayment identification in Colorado was 53 percent for Federal Fiscal Year 2010. In Calendar Year 2010, the Colorado UI Program's operational overpayments represented an estimated $61 million (36 percent) of Colorado's $169 million in total UI overpayments.

During the audit, we reviewed the Payment Control unit's overpayment detection and recovery data, observed and interviewed Payment Control unit staff, and reviewed Payment Control unit policies and procedures. We also compared the Payment Control unit's 3-year overpayment detection rate to USDOL standards for Colorado's UI Program over the last 5 years. As shown in the following table, the Payment Control unit met federal standards from Federal Fiscal Years 2006 through 2009 but did not meet federal standards in Federal Fiscal Year 2010. The table also shows that the UI Program's detection declined significantly in Federal Fiscal Year 2010.

Unemployment Insurance Program
Benefit Payment Control Unit Performance
Federal Fiscal Years 2006 Through 2010

	2006	2007	2008	2009	2010
USDOL Standard	60%	60%	61%	56%	53%
UI Program's 3-Year Detection Rate	61%	60%	68%	63%	42%

Source: U.S. Department of Labor.

When the Payment Control unit detects fewer overpayments, fewer overpayments will be recovered and, ultimately, more funds will be permanently lost from the UI Trust Fund. For example, in Calendar Year 2010, if the Payment Control unit was meeting the federal performance goal of identifying 53 percent of operational overpayments, it would have identified about $11 million in additional overpayments. Based on the Payment Control unit's average recovery rate for identified overpayments of 43 percent, this would have resulted in about $5 million in additional recoveries in Calendar Year 2010. Further, although the UI Program may be able to identify overpayments from prior years in the future, the likelihood of recovering the overpayments decreases as they age.

As discussed below, we found that a lack of adequate staff and the UI Program's prioritization of overpayment recovery methods have contributed to the UI Program's identifying and recovering fewer overpayments.

Lack of Staff. According to Payment Control unit staff, overpayment detection rates have decreased because of the large increase in overpayments beginning in Calendar Year 2009, which led to a substantial increase in workload for the Payment Control unit. At the same time, the unit did not receive additional staff to accommodate the increase in work. As a result, the Payment Control unit has suspended or significantly reduced staff time dedicated to detecting new overpayments to recover overpayments that have already been identified. For example, interstate cross-matches, which match out-of-state wages with claimants requesting benefits in Colorado, were completely suspended in September 2008. In addition, intrastate cross-matches against wages reported directly to the UI Program are backlogged to 2009. These cross-matches are the Payment Control unit's primary way to identify claimants who were hired and received wages but falsely claimed that they continued to be unemployed.

Although staffing concerns exist across the UI Program, because the Payment Control unit's activities are highly beneficial relative to their costs, we believe that the UI Program should consider reallocating staff to the Payment Control unit to help address the current problems related to a lack of staff. We found that in Fiscal Year 2010, the Payment Control unit recovered $18.9 million in overpaid funds, compared to the $2.8 million the program expended on the unit. This is equivalent to a net gain of about $500,000 for each of the approximately 30 FTE on its staff. Thus, if the UI Program were able to reallocate, for example, 10 FTE to the Payment Control unit, the increased staff could result in an additional $5 million of overpayments being recovered and deposited into the UI Trust Fund annually. As noted at the beginning of this chapter, we identified nearly 40 FTE within the UI Program's claims review functions that we believe could be reallocated to more efficient use.

Recovery Prioritization. We also found that the Payment Control unit could improve the efficiency of its efforts to recover identified overpayments. Specifically, Payment Control unit staff have been attempting to catch up with the current overpayment backlogs for wage cross-matches, which identify claimants who may have failed to report wages when filing for benefits, by working on older claims first. This approach appears to be less efficient, since older claims are likely to be more difficult to recover and may explain why the Payment Control unit's rate of recovery on identified overpayments decreased from 50 percent in Calendar Year 2006 to 43 percent in Calendar Year 2010.

Finally, as noted previously, in September 2011, USDOL identified Colorado as one of the seven states in the country with the highest overpayment rates over the last 3 years. As a result of this identification, USDOL plans to impose a corrective action plan on Colorado's UI Program and increase monitoring and technical assistance in Colorado until the State's overpayment rate dips below 10 percent of all UI payments. At the time of our audit, the UI Program had not received specific information about the corrective action plan that USDOL will require, but

the UI Program should take all steps necessary to comply with this plan and reduce its overpayment rate.

Recommendation No. 5:

The Department of Labor and Employment (the Department) should increase the number of overpayments detected and recovered by:

a. Reviewing the current staffing levels and determining if there are opportunities to reassign additional staff to the Benefit Payment Control unit for the purpose of increasing overpayment detection and recovery activities.

b. Giving priority to detecting and collecting more recent overpayments.

Department of Labor and Employment Response:

a. Agree. Implementation date: November 2011.

From April to August 2011, the Department conducted a comprehensive qualitative and quantitative analysis of staffing and functions within the UI Program to design a more efficient and effective operations structure. The resulting reorganization plan (1) streamlined management and administrative functions, (2) dedicated more resources to customer service and quality control functions, and (3) increased the utilization of permanent part-time staff to balance economic and seasonal demands with fluctuating funding provisions. The UI Program reorganization, which will be complete on November 1, 2011, will allow the program to focus on these issues by moving additional staff from other support areas to direct service, including the customer service center, adjudication, and integrity and fraud units. This should result in decreased administrative overpayments and an increase in detection and recovery of overpayments.

b. Agree. Implementation date: June 2011.

The Department is already intensifying efforts to eliminate overpayments with focus on three main root causes of improper payments: work-search, separation, and benefit-year earnings issues. To tackle these root causes, an Integrity Task Team, composed of staff from all branches, was implemented in July 2011 to focus on prevention, detection, and recovery of improper payments. A robust

Integrity Action Plan has been developed to combat improper payments. This task force will track the improper payment rates, monitor the action plans, and make adjustments, as needed. Communication efforts are being revamped to provide additional methods in which the UI Program can communicate critical information to staff, claimants, and employers beginning in September 2011 and ongoing. As of October 2011, training teams began developing, refining, and testing competency-development tools and techniques for frontline staff in each discipline to improve staff skill and abilities for UI Program delivery that will result in fewer administrative overpayment errors. We anticipate lowering improper payments to meet or be less than the national average of 11 percent by September 2012.

As of June 2011, priority has been given to detect and collect more recent overpayments with emphasis on National Directory of New Hire audits, which allow the overpayment to be detected sooner. The UI Program will begin an aggressive approach for recovery of improper payments by using automated skip-tracing tools that will be made available by October 31, 2011. The UI Program will continue to intercept state tax refunds and will soon intercept federal tax refunds and gaming proceeds for UI overpayments beginning January 2012.

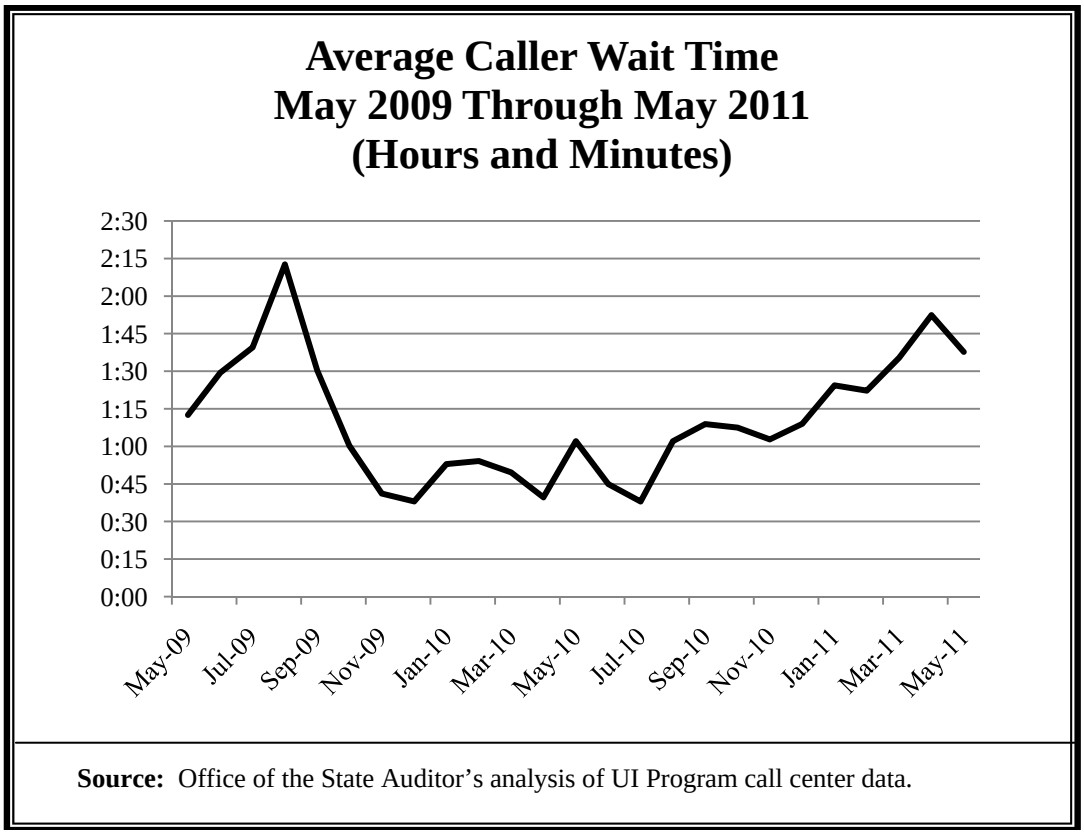
Customer Call Center

The UI Program's customer call center provides claimants with an important resource for obtaining information about their claims and removing holds on claims that could prevent, delay, or reduce payments. The call center is the UI Program's main point of contact with the public and a critical resource to claimants. During the audit, we observed call center staff, reviewed call data, and assessed the UI Program's allocation of call center staff. Overall, we found that due to the large increase in calls, the UI Program has had difficulty providing claimants with adequate access to customer service agents. In addition, we identified several opportunities to increase the number of callers whom the UI Program is able to serve.

Our review of the customer service line indicates that the UI Program has not been able to provide claimants with consistent access to customer service agents. According to our review of call data and testing of the customer service line, since Calendar Year 2009, most claimants calling the UI Program have received either a busy signal or were directed to a self-service menu with no option to speak with an agent because all available lines were full. In addition, during a 9-day period in February 2011, we called the UI Program's customer service line 50 times. For 48

(96 percent) of the calls, we either received a busy signal or were directed to the self-service line, which does not give an option to speak with a call center agent. Further, we reviewed call center data and found that of about 532,000 calls directed to the self-service line in June 2011, about 465,000 (87 percent) calls were abandoned, suggesting that many of the callers needed to speak with a customer service agent but were unable to do so. It is important to note that the 465,000 abandoned calls do not necessarily represent 465,000 individual claimants, as claimants may have made multiple attempts to reach the customer service center.

After callers successfully get through to the main phone line, they typically experience long wait times. As of July 2011, we found that the average wait time for the main general inquiry line was 1 hour and 40 minutes. As shown in the following chart, wait times have varied considerably from May 2009 through May 2011, peaking at 2 hours and 13 minutes in August 2009, falling to 38 minutes in December 2009, then slowly increasing back to current levels. UI Program staff reported that in 2009, caller wait times sometimes exceeded 3 hours.



Source: Office of the State Auditor's analysis of UI Program call center data.

According to UI Program management, the problems we identified are primarily caused by the program not having sufficient staff to answer the volume of claims it has received. Although our review confirmed that lack of staff is a fundamental

problem, we also identified several opportunities to increase the number of callers the UI Program can accommodate, as discussed below.

Eliminating Claimant Call-Back System. To avoid the main customer service line, some claimants attempt to get help with their claims at workforce centers or by randomly calling the UI Program's noncustomer service phone lines. When this occurs, the UI Program staff who are contacted often cannot help the claimants with their issue. To accommodate these claimants, the UI Program established a customer call-back system. This system allows for UI Program staff to collect the claimants' contact information and arrange for a customer service agent to call the customers back in 5 to 7 business days. According to program management, in Calendar Year 2010, the UI Program conducted 40,000 call backs.

Although the customer call-back system provides better service to some claimants, we found that it ultimately reduces the number of calls the UI Program can answer. We examined call-back data and observed staff conducting call backs and found that staff assigned to call backs serve significantly fewer claimants than staff assigned to receive incoming calls. Specifically, from November 2010 through January 2011, we estimate that, on average, full-time call center agents conducting call backs spoke with 78 percent fewer claimants than agents answering incoming calls, because claimants are often not home when they receive the call back. During this time period, the UI Program assigned at least seven FTE to conduct call backs each day. Thus, it appears that the UI Program could increase its staff time available to speak with claimants by the equivalent of about 5.5 FTE and $296,000 in salary and benefits annually by eliminating the call-back system and requiring all claimants to use the customer service line.

Reducing Claims Filing By Phone. As previously discussed, the UI Program gives all UI claimants the option of filing claims over the phone, rather than completing the online application form. During the audit, we found that several other states, including Pennsylvania, Oklahoma, and Utah, limit the ability of most claimants to file claims by phone. If the UI Program required claimants to file for benefits online, it could save a substantial amount of staff time. Specifically, during Calendar Year 2010, about 59,000 claims were filed over the phone. According to UI Program management, it takes staff about 20 minutes per claim to assist claimants who apply for benefits over the phone. Based on this average call time, we estimate that the UI Program could reallocate as much as 9.5 FTE, paid about $512,000 annually in salary and benefits, if most claimants were required to file online.

Although requiring claimants to file for benefits online would reduce call center workload and increase the UI Program's ability to provide other services to claimants, this change could also create a substantial burden for some claimants. For example, UI Program management indicated that some claimants have vision

problems, cannot read, or live in remote areas that do not have Internet access. Thus, before making this change, the UI Program would need to determine whether it could still adequately serve all claimants and develop alternative means of applying for benefits for claimants who cannot file online.

Assigning More Customer Service Staff to Phone Duties. Our review of customer service center staff allocation indicates that the UI Program may be able to increase the number of staff assigned to answer incoming calls. For example, in June 2011, the customer service center had approximately 94 staff but, on average, only assigned 31 (33 percent) staff to answer incoming calls. As a result, customers experienced average wait times of 99 minutes. By comparison, the UI Program was able to reduce caller wait times to 63 minutes in November 2010, when 47 agents were assigned to answering calls. The agents who were not assigned to answer calls were assigned to other duties, such as helping claims review staff, assisting claimants in person, conducting customer call backs, and working on other special projects. In addition, the UI Program gives call center staff the option of having a flex schedule, which allows them to work four 10-hour shifts each week instead of the standard five 8-hour shifts. The UI Program normally experiences its highest caller volumes on Mondays, Tuesdays, and Wednesdays. When we analyzed staffing data for November 2010 through January 2011, we found that, on average, 17 percent of agents were absent on these three days, and call center management indicated that this was primarily because of the UI Program's flex schedule policy. Although the customer service agents work the same number of hours regardless of whether they have a flex schedule, it appears the UI Program could increase its ability to answer calls on the busiest days by restricting flex schedule days off to the least busy days.

Recommendation No. 6:

The Department of Labor and Employment (the Department) should improve the efficiency of its customer service functions in the Unemployment Insurance Program (UI Program) by:

a. Eliminating or restricting the use of customer call backs.

b. Requiring claimants to apply for unemployment insurance benefits online and establishing alternative application procedures for claimants who are not able to file online.

c. Developing and implementing strategies to increase the number of staff answering customer service calls, including evaluating the UI Program's flex schedule policy to determine if it is consistent with optimizing customer service.

Department of Labor and Employment Response:

a. Agree. Implementation date: March 2012.

We have already restricted call backs, and they have been reduced by over half in the past year and will continue to decline as service levels improve in the call center and through outreach efforts. Further restrictions on call backs will be accomplished through internal management procedures and controls. However, recognizing that from time to time the need will arise to respond by telephone to urgent, complex, or unique requests or issues, the program considers it essential that call-back capabilities not be eliminated "completely."

b. Partially agree. Implementation date: May 2012.

The Department believes it would be overly stringent to require all claimants to file over the Internet without regard to service access issues, though this is the preferred method. However, we will research this issue with other states that have moved to an all-online application system to determine if such a system is feasible for Colorado and will take steps, as applicable, based on this research.

c. Agree. Implementation date: July 2012.

The reorganization of the UI Program, which will be complete on November 1, 2011, will allow the UI Program to focus on these issues. Staff will be moved from other support areas to direct service in the call center. The Department has previously evaluated the flex-time policy and staffing needs, making coverage adjustments as needed to best serve the needs and interests of the customers. Our internal analysis demonstrates that the complete elimination of flex-time schedules, however, would result in fewer calls being answered overall due to the reductions in scheduled phone time. We are now going to conduct another analysis based on new staffing levels and days flex time can be offered to maximize customer service.

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

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

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

Report Control Number 2140

Report Control Number 2140

Office of Cyber Security
Governor's Office of Information Technology

Performance Audit
November 2010

PUBLIC REPORT

OFFICE OF THE STATE AUDITOR

LEGISLATIVE AUDIT COMMITTEE
2010 MEMBERS

Senator David Schultheis
Chair

Senator Lois Tochtrop
Vice-Chair

Senator Morgan Carroll
Representative Jim Kerr
Representative Joe Miklosi
Senator Shawn Mitchell
Representative Dianne Primavera
Representative Mark Waller

OFFICE OF THE STATE AUDITOR

Sally Symanski
State Auditor

Dianne Ray
Deputy State Auditor

Jonathan C. Trull
Legislative Audit Manager

Annette Argo
Julie Chickillo
Reed Larsen
Rosa Olveda
Manjula Udeshi
Legislative Auditors

Coalfire Systems
Emagined Security
Contract Auditors

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

STATE OF COLORADO

Sally Symanski, CPA
State Auditor

OFFICE OF THE STATE AUDITOR
303.869.2800
FAX 303.869.3060

Legislative Services Building
200 East 14th Avenue
Denver, Colorado 80203-2211

November 22, 2010

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of the Colorado Office of Cyber Security within the Governor's Office of Information Technology. The 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 penetration test performed as part of this audit was conducted with the permission of the Chief Information Security Officer pursuant to Section 24-37.5-403 (2)(d), C.R.S. The report presents our findings, conclusions, and recommendations, and the responses of the Office of Cyber Security and the Governor's Office of Information Technology.

Sally Symanski

This page intentionally left blank.

TABLE OF CONTENTS

Glossary of Terms and Abbreviations

Application-level Controls - controls incorporated directly into computer applications to help ensure the validity, completeness, accuracy, and confidentiality of data during application processing and reporting.

Attack - attempt to gain unauthorized access to an information system's services, resources, or information, or the attempt to compromise an information system's integrity, availability, or confidentiality.

Colorado Cyber Security Program - an information security framework established by House Bill 06-1157 and overseen by the Governor's Office of Cyber Security.

Computer Application or Application - a computer program or set of programs that perform the processing of records for a specific function. Examples of computer applications include Microsoft Office, Microsoft Excel, COFRS, and SAP.

Defense-in-depth - a commonly accepted "best practice" for implementing computer security controls in today's networked environment. Integrates people, operations, and technology capabilities to protect information systems across multiple layers.

Denial of Service Attack - an assault on a service from a single source that floods the service with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.

Firewall - a router, server, or specialized hardware device designed to restrict access to one network from another network.

FTE - Full-time equivalent. An FTE of 1.0 means that the person is equivalent to a full-time worker, while an FTE of 0.5 signals that the worker is only half-time.

General Computer Controls - controls that relate to the environment within which computer-based applications are developed, maintained, and operated. The objectives of general computer controls are to ensure the proper development and implementation of computer applications and the confidentiality, integrity, and availability of program and data files.

HTTP - Hypertext Transfer Protocol. A networking protocol commonly used to communicate over the Internet or World Wide Web.

IDS - Intrusion Detection System. An automated system that inspects network activity to identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Internet - When capitalized, the term "Internet" refers to the collection of networks and gateways that use the transmission control protocol/Internet protocol suite of protocols.

Intranet - a private network that uses the infrastructure and standards of the Internet and World Wide Web, but is isolated from the public Internet by firewall barriers.

IP Address - Internet Protocol Address. A numerical label assigned to computers and devices participating in a network, such as the Internet.

ISOC - Information Security Operations Center. The group within the Governor's Office of Cyber Security responsible for detecting and responding to threats against the State.

IT - Information technology.

IT Infrastructure - all information technology assets (hardware, software, data), components, systems, applications, and resources.

Modem - short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received.

Network - A group of computers and associated devices that are connected by communications facilities.

OIT - Governor's Office of Information Technology. The state agency within the Governor's Office that is responsible for the administration, management, and oversight of state IT operations and systems.

Patch - additional pieces of code that have been developed to address specific problems or flaws in existing software.

Penetration Test - Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.

PII - Personally Identifiable Information**.** Refers to any information about an individual maintained by an entity, including any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date of birth, or biometric records, and any other information which is linked or linkable to an individual.

Port - an endpoint to a logical network connection.

Public Agency - According to Section 24-37.5-402(9), C.R.S., a public agency means every state office, whether legislative, executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the Department of Higher Education. For our purposes, our audit did not include the Legislative Branch.

Risk - the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact.

Threat - any potential danger to information or systems.

Service - refers to customer or product-related business functions such as file transfer protocol (FTP), hypertext transfer protocol (HTTP), and mainframe supervisor calls.

Social Engineering - a method used by hackers to obtain passwords and other sensitive information. For example, a hacker may call an authorized user of a computer system and pose as a network administrator to gain access.

URL - Uniform Resource Locator**.** The address of a web page on the Internet – e.g., www.state.co.us.

Utilities - Software used to perform system maintenance routines that are frequently required during normal processing operations. Some utilities have powerful features that will allow a user to access and view or modify data or program code.

VPN - Virtual Private Network. A protected information system link that provides the same function as a secured, dedicated line by utilizing tunneling, security controls, and end-point address translation.

Vulnerability - a software, hardware, physical, or procedural weakness that could provide an attacker with unauthorized access to an entity's networks, systems, or data.

War Dialer - software packages that sequentially dial telephone numbers, recording any numbers that answer.

Wide Area Network - a group of computers and other devices dispersed over a wide geographical area that is connected by communications links.

Web Application - an application that is accessed via the web over a network such as the Internet or an intranet.

SALLY SYMANSKI, CPA
State Auditor

Office of Cyber Security
Governor's Office of Information Technology
Performance Audit
November 2010

Purpose and Scope

Our audit reviewed the Governor's Office of Cyber Security's progress in fulfilling the requirements of the Colorado Cyber Security Program (Section 24-37.5-401 through 406, C.R.S.). As part of the audit, we reviewed State Cyber Security Policies, Agency Cyber Security Plans, and Governor's Office of Information Technology (OIT) strategic plans and budget documents; interviewed personnel; surveyed other states' chief information security officers; and analyzed the Office of Cyber Security's processes and procedures related to security incidents. In addition, we contracted with a professional computer security firm to assist our staff in performing a covert penetration test of state networks, applications, and information systems. We performed audit work from February through November 2010.

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 evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Overview

State agencies routinely collect, process, and store personally identifiable information and data, including social security numbers, taxpayer identification numbers, driver's license and ID numbers, personal health information, wage information, and criminal history records. The State, as custodian of the public's data, is responsible for safeguarding the information it receives and for ensuring the confidentiality, integrity, and availability of state systems. In 2006 the General Assembly enacted House Bill 06-1157, creating the Colorado Cyber Security Program, which forms the foundation of the State's security control structure and reflects the General Assembly's commitment to address the security risks facing public agencies.

The Colorado Cyber Security Program is overseen by the Chief Information Security Officer, who is appointed by the Governor. The Colorado Cyber Security Program requires public agencies to annually develop an information security plan utilizing the information security policies, standards, and guidelines developed by the Chief Information Security Officer. In addition to the development of information security plans, the Colorado Cyber Security Program requires the Chief Information Security Officer to direct information security audits and assessments of public agencies, establish and direct a risk management process, conduct information security awareness training, coordinate

budget requests for information security systems, and work with the Colorado Commission on Higher Education related to information security planning and incident reporting. The Office of Cyber Security, administratively located within OIT, is responsible for execution of the Colorado Cyber Security Program. For Fiscal Year 2010, the Office of Cyber Security received spending authority for approximately $2.5 million in reappropriated funds and 17 full-time equivalent positions to carry out its responsibilities.

Key Findings

Colorado Cyber Security Program

According to statute [Section 24-37.5-403, C.R.S.], the Office of Cyber Security is responsible for the implementation of the Colorado Cyber Security Program and for the day-to-day management of the State's information security operations. Overall, we concluded that the Office of Cyber Security has failed to successfully implement the Colorado Cyber Security Program, as required by statute.

- **Agency Cyber Security Plans.** We found that 12 of 20 public agencies, or 60 percent, failed to submit statutorily-required information security plans to the Office of Cyber Security by the July 15, 2010 deadline. We also found that the Commission on Higher Education is not collecting, reviewing, and submitting to the Office of Cyber Security information security plans for institutions of higher education, as required by statute. Additionally, of the eight agency plans reviewed by the Office of Cyber Security as of September 15, 2010, only one was complete. We found that the plans of agencies are often inaccurate and fail to contain detailed and meaningful information.

- **Cyber Security Incidents.** Since 2006 the Office of Cyber Security has only received 43 cyber security incident reports, none of which were reported by institutions of higher education. Additionally, we identified seven data breaches that should have been reported to the Office of Cyber Security but were not. We also found that (1) staff responsible for incident response have generally not received sufficient training, (2) the State Incident Response Plan is outdated and contains inaccurate information, (3) agencies lack sufficiently detailed agency-level procedures for responding to cyber security incidents, and (4) the Office of Cyber Security lacks an electronic incident reporting and tracking system. We also identified one agency that failed to properly respond to a social engineering attack performed as part of our penetration test.

- **Colorado Cyber Security Program Requirements.** The Office of Cyber Security has not implemented significant requirements of the Colorado Cyber Security Program, such as directing information security audits and assessments in public agencies, conducting information security awareness and training programs, and coordinating public agency budget requests related to information security systems.

- **Strategic Planning and Management Oversight.** The Office of Cyber Security lacks a strategic plan for directing its operations, lacks any meaningful measures for assessing its performance, and does not have procedures to collect and analyze meaningful cyber security information. A lack of effective leadership within the Office of Cyber Security and a lack of oversight by the Governor's Office of Information Technology led to many of the problems identified in our audit.

Penetration Test Results

We assessed the State's information security posture or preparedness and exposure to cyber attacks by performing a covert penetration test of state networks and information systems. Overall, we determined that the State is at high risk of a system compromise and/or data breach by malicious individuals, including individuals both internal and external to the State.

- **Exposed Management Interfaces.** We were able, in several cases, to gain access to exposed management interfaces by using vendor default usernames and passwords or by guessing the username and password. The State has a significant number of management interfaces for firewalls, network devices, and web applications exposed directly to the Internet.

- **Default and Easily Guessable Usernames and Passwords.** We gained unauthorized access to systems and administrative interfaces by either guessing the correct username and password or by using vendor default credentials.

- **Unnecessary and Insecure Ports, Services, and Utilities.** We identified numerous IP addresses that appeared to be unused and with ports open that were running unneeded and outdated services. The State has a large Internet presence, including more than 17,600 active Internet Protocol (IP) addresses. Many of the State's servers are running vulnerable services that provide attackers an opportunity for exploitation.

- **Unsecured Web Applications.** We identified hundreds of vulnerabilities in state web applications, including many severe vulnerabilities that led directly to the systems' compromise. In several situations, we were able to take control of the database the application was using to disclose usernames and passwords and citizen data. We also found that application-level logs are not being monitored.

- **Internal Network Security.** We found that public agencies' internal networks are not properly segmented, internal systems are not hardened or patched, insecure network protocols are used for sensitive transactions, and most public agencies lack an internal intrusion detection system.

Our recommendations and the responses from the Governor's Office of Information Technology can be found in the Recommendation Locator and in the body of this report.

This page intentionally left blank.

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
1	31	Re-evaluate and improve the Agency Cyber Security Plan (Plan) development, submission, and review process by (a) establishing additional guidelines and procedures for Plan completion, (b) providing training to agency information security officers on Plan creation and submission, (c) developing and implementing a policy that requires timely written feedback on submitted Plans, (d) reviewing all Plans submitted to the Office of Cyber Security and providing timely feedback, (e) holding agencies accountable for the timely submission of statutorily compliant Plans, (f) ensuring that agencies' risk assessments include specific dates for remediating identified control gaps and that Plans of Actions & Milestones align with the agencies' risk assessments, (g) incorporating the information contained in the Plans into the Office of Cyber Security's strategic planning process, and (h) working with the Colorado Commission on Higher Education to ensure that security plans developed by institutions of higher education are being received annually and reviewed.	Agree	July 2011

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
2	37	Improve the State's incident identification, reporting, analysis, and response processes and procedures by (a) ensuring public agencies, including the Department of Higher Education, are aware of their responsibilities to report cyber security incidents to the Office of Cyber Security; (b) providing training to employees, information security officers, and system administrators in incident awareness, identification, documentation, response, and reporting; (c) updating the State Incident Response Plan; (d) ensuring that each public agency has detailed, written procedures for responding to security incidents and that agency-level procedures align with procedures in the State Incident Response Plan; (e) implementing an automated incident response reporting and tracking system and analyzing and reporting incidents to senior management; (f) performing incident response debriefings; and (g) updating incident response procedures to require that system administrators enforce password changes on accounts that are suspected of being compromised.	Agree	July 2011
3	42	Ensure the Office of Cyber Security has implemented and is complying with all statutory requirements of the Colorado Cyber Security Program by (a) inventorying all statutory requirements that pertain to the Colorado Cyber Security Program, (b) ensuring that the Chief Information Security Officer is aware of his or her duties and responsibilities and is knowledgeable of all statutory requirements of the Colorado Cyber Security Program, and (c) developing and executing a work plan to bring the Office of Cyber Security and public agencies into compliance with Colorado Cyber Security Program requirements.	Agree	July 2011

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
4	45	Work with the Office of Cyber Security to develop a strategic plan for the State's cyber security operations. The strategic plan should establish the Office of Cyber Security's mission, vision, goals, objectives, and short- and long-term priorities, include measurable objectives, and be communicated to information security staff and key stakeholders. Increase oversight of the Office of Cyber Security and ensure that an effective leadership structure is in place.	Agree	January 2011
5	54	Improve the security of the State's network and Internet-facing applications by (a) ensuring that the deficiencies identified in the confidential appendices provided under separate cover are addressed, (b) identifying and inventorying all network devices and applications with management interfaces exposed to the Internet or other publicly accessible or insecure networks, (c) working with agency staff to reconfigure the devices and applications with Internet-exposed management interfaces so that access to the interfaces is only possible from inside the State's network, (d) revising State Cyber Security Policies to require that administrative interfaces not be directly accessible from the Internet, and (e) implementing firewall rules at the State gateway to filter incoming traffic bound for ports running administrative interfaces.	Agree	July 2011

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
6	56	Ensure that all state systems, especially those exposed to the Internet, use strong passwords and non-default usernames by (a) ensuring that the deficiencies identified in the confidential appendices provided under separate cover are addressed, (b) performing routine vulnerability scans of state systems and networks, and (c) requiring that all new systems and network devices undergo the OIT approved hardening, or secure, process using the Center for Internet Security benchmarks.	Agree	July 2011
7	58	Reduce the State's exposure to attacks against unnecessary and insecure ports, services, and utilities by (a) ensuring that the deficiencies identified in the confidential appendices provided under separate cover are addressed, (b) reducing the overall Internet footprint of the State (c) limiting the number of ingress and egress points to the State Wide Area Network and to agency-specific networks, (d) inventorying all systems and applications that require Internet access, (e) defining the appropriate access rules for each inventoried asset, and (f) ensuring that all assets are protected by a monitored firewall.	Agree	July 2011

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
8	60	Ensure that state web applications are appropriately secured by (a) ensuring that the deficiencies identified in the confidential appendices provided under separate cover are immediately addressed, (b) training state application developers on the fundamentals of secure coding and application design, (c) routinely testing all existing web applications and correcting identified deficiencies, (d) ensuring that all newly designed web applications are tested manually and with automated scanners, (e) requiring the Office of Cyber Security to validate that all web applications have been sufficiently tested and properly secured before being moved into production, (f) protecting critical web applications with web application firewalls, and (g) ensuring IT staff are routinely reviewing and monitoring web application logs and reporting suspicious activity to appropriate staff.	Agree	July 2011
9	63	Improve the security of public agencies' internal networks by (a) ensuring that the deficiencies identified in the confidential appendices and provided under separate cover are addressed, (b) architecting internal networks so that they are "segmented" based upon access and security requirements, (c) requiring information security officers to routinely perform automated vulnerability scans of internal networks to identify and remediate vulnerabilities, (d) working with agency IT staff to ensure that proper hardening and patch management practices are being followed, (e) providing guidance to IT staff and agency IT directors on the development and implementation of proper network segmentation, (f) requiring that agencies utilize secure protocols when transmitting sensitive information, and (g) implementing intrusion detection capabilities within internal networks where feasible.	Agree	July 2013

This page intentionally left blank.

Overview of the Colorado Cyber Security Program

Chapter 1

The State of Colorado's information systems and the information they contain and process represent significant assets and are critical to the State's ability to conduct business and achieve its mission of serving Colorado's citizens. State agencies routinely collect, process, and store personally identifiable information and data, including social security numbers, taxpayer identification numbers, driver's license and ID numbers, personal health information, wage information, and criminal history records. Colorado's citizens and those doing business with the State expect that the data they provide will be protected and only used for official purposes. Because of the potential monetary value of these data and their appeal to potential hackers for purposes such as identity theft or other illegal acts, the State is often the target of directed cyber security attacks by both trusted insiders (e.g., government employees and contractors) and groups and individuals external to the State.

The State, as custodian of the public's data, is responsible for safeguarding the information it receives and for ensuring the confidentiality, integrity, and availability of its systems. Understanding the threats facing Colorado's information systems and the State's responsibility to protect the public's data, the General Assembly enacted House Bill 06-1157 during the 2006 Legislative Session. The legislation, better known as the Colorado Cyber Security Program, was signed into law by the Governor in June 2006 and was codified in Part 4 of Article 37.5, Title 24 of the Colorado Revised Statutes. Most of the law's requirements apply only to public agencies. The law defines a "public agency" as "every state office, whether legislative, executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions;" however, the Legislative Branch was not included within the scope of this audit. The law's definition of "public agency" does not include the Colorado Commission on Higher Education, Department of Higher Education, or institutions of higher education. We discuss the provisions of this law in the next section.

Colorado Cyber Security Program

The goal of the Colorado Cyber Security Program is to improve Colorado's information security posture by establishing a statewide information security

framework and governance model. The Colorado Cyber Security Program forms the foundation of the State's security control structure and reflects the General Assembly's commitment to address the security risks facing public agencies using a coordinated and risk-based approach. According to the legislation, the Colorado Cyber Security Program is overseen by the Chief Information Security Officer, who is appointed by the Governor. As specified in House Bill 06-1157, the strategic objectives for the Colorado Cyber Security Program are to:

- Protect the State's communication and information resources against unauthorized access, disclosure, use, and modification or destruction, whether accidental or deliberate, as well as ensure the confidentiality, integrity, and availability of information.

- Ensure that the information the public has entrusted to public agencies is safe, secure, and protected from unauthorized access, unauthorized use, or destruction.

- Secure the State's communication and information resources through a coordinated and shared effort from all departments, agencies, and political subdivisions of the State and a long-term commitment to providing state funding that ensures the success of such efforts.

- Promulgate and implement information security standards, policies, and guidelines throughout public agencies to ensure the development and maintenance of minimum information security controls to protect communication and information resources that support the operations and assets of those agencies.

The law requires public agencies to develop an information security plan utilizing the information security policies, standards, and guidelines developed by the Chief Information Security Officer. The first information security plan for each agency was to be created by July 1, 2007 and submitted to the Chief Information Security Officer on or before July 15, 2007. According to statute, the plans must include:

- Periodic assessments of the risk and magnitude of the harm that could result from a security incident.

- A process for providing adequate information security for the agency's information resources and communications.

- Regular security awareness training for employees and users of agency information resources.

- Periodic testing and evaluation of the effectiveness of information security for the agency, which shall be performed not less than annually.

- A process for detecting, reporting, and responding to security incidents consistent with the information security standards, policies, and guidelines issued by the Chief Information Security Officer.

- Plans and procedures to ensure the continuity of operations for information resources that support the operations and assets of the public agency in the event of a security incident.

The law allowed public agencies to establish a phase-in period to fully comply with the provisions of House Bill 06-1157. Specifically, all public agencies were required to be fully compliant with the provisions of the law, including implementation of all State Cyber Security Policies subsequently issued by the Chief Information Security Officer, by July 1, 2009.

Each year on or before July 15, the executive director or head of each public agency is to report to the Chief Information Security Officer on the development, implementation, and if applicable, compliance with the phase-in schedule of the public agency's information security plan.

Office of Cyber Security

The Office of the Chief Information Security Officer, better known as the Office of Cyber Security, is tasked with statewide information technology-related cyber security functions, including assessment, monitoring, process implementation, and execution of the Colorado Cyber Security Program. The Office of Cyber Security is designated as the single state source for cyber security readiness and awareness. Working closely with federal, state, local, and private sector partners, the Office of Cyber Security actively gathers and analyzes information on cyber threats and vulnerabilities that present risk to the State's information systems, networks, and applications or the critical information managed within them.

The Office of Cyber Security (Office) is located administratively within the Governor's Office of Information Technology (OIT) and led by the governor-appointed Chief Information Security Officer. The Office was formally established in 2006 and is responsible for administering the Colorado Cyber Security Program. For Fiscal Year 2007, the Office's first year of operation, a total of $4.2 million in federal funds and one full-time equivalent (FTE) position, the Chief Information Security Officer, was set aside for the Colorado Cyber Security Program. With the assistance of contractors, the Office of Cyber Security used the funds to upgrade the State's information security infrastructure and establish Colorado's first cyber security policies and standards. These funds

were also used to support security categorization and department-level risk assessments of critical systems, establish a compliance framework, and provide key security control mechanisms. Statewide cyber security training and a multi-agency cyber security incident response program were also developed.

As shown in the table below, for Fiscal Year 2010 the Office of Cyber Security received an appropriation for two FTE, including the Chief Information Security Officer and Deputy Chief Information Security Officer positions, and approximately $2.5 million in reappropriated funds. However, the Office of Cyber Security does not have a dedicated funding source and is required to charge public agencies for its activities in administering the Colorado Cyber Security Program or use other available funds, such as grant funds and federal dollars. Therefore, as seen in the bottom half of the table below, the Office of Cyber Security's annual expenditures are often much less than that year's appropriation.

Colorado Office of Cyber Security
Appropriations, Expenditures, and Full Time Equivalents (FTE)
Fiscal Years 2007 - 2010

	Fiscal Year 2007		Fiscal Year 2008		Fiscal Year 2009		Fiscal Year 2010	
Funding Source	**Approp.**	**FTE**	**Approp.**	**FTE**	**Approp.**	**FTE**	**Approp.**	**FTE**
General Fund	$0	1.0	$0	2.0	$350,000	2.0	$0	2.0
Reappropriated funds[1]	4,200,000		2,450,000		2,455,000		2,459,000	
Total	$4,200,000		$2,450,000		$2,805,000		$2,459,000	

	Fiscal Year 2007	Fiscal Year 2008	Fiscal Year 2009	Fiscal Year 2010
Expenditures	$2,968,000	$1,202,000	$950,000	$429,000
Expenditures as a Percentage of Appropriation	71%	49%	34%	17%

Source: OSA analysis of State of Colorado budget documents and appropriation bills.
[1]Cash exempt funds were reclassified as reappropriated funds as of Fiscal Year 2009.

Senate Bill 08-155 requires that all IT-related functions, systems, and staff within the Executive Branch be consolidated within OIT. As part of the consolidation of state IT, the Office of Cyber Security received management authority for 15 FTE for Fiscal Year 2011 through the transfer of security staff from public agencies. These additional positions will be funded through the Network Services group within the OIT appropriation. The Network Services group plans, coordinates, integrates, and provides telecommunication capabilities and network solutions for state agencies and local governments. Within OIT, IT security staff represent approximately 3 percent of all Executive Branch IT staff.

Organization and Reporting Structure

Prior to July 2010, the Office of Cyber Security implemented the requirements of the Colorado Cyber Security Program through a federated or decentralized model. Agency personnel serving as information security officers did not work for or report to the Chief Information Security Officer. Agency information security officers continued to report to their agencies' management teams and carried out their duties with little oversight from the Office of Cyber Security. With the passage of Senate Bill 08-155, however, that reporting structure has changed significantly. As of July 1, 2010, Executive Branch information security officers and other Executive Branch staff performing security functions within their agencies were transferred to the Office of Cyber Security and now report directly to the Chief Information Security Officer. For Fiscal Year 2011, the Office of Cyber Security is now comprised of 17 FTE, including the vacant Deputy Chief Information Security Officer position. Senate Bill 08-155 also changed the reporting structure for the Chief Information Security Officer. Instead of reporting to the Governor, the Chief Information Security Officer now reports to the State Chief Information Officer (State CIO), the administrative head of OIT.

It also important to point out that the consolidation of state IT only affected Executive Branch agencies. However, the Colorado Cyber Security Program and the Chief Information Security Officer's responsibilities apply to public agencies as defined in Section 24-37.5-402(9), C.R.S., including the Judicial and Legislative Branches, Secretary of State, and Offices of the State Treasurer and Attorney General, and excluding institutions of higher education and the Department of Higher Education. Although these public agencies' systems are not under the Chief Information Security Officer's direct control, the Chief Information Security Officer can remove public agencies' systems from the state network under certain conditions, such as identification of severe vulnerabilities or a compromise that could impact other state systems. Additionally, the Colorado Commission on Higher Education has certain reporting requirements to the Chief Information Security Officer.

The organizational chart on page 17 shows the current structure of the Colorado Office of Cyber Security, including relevant lines of authority. The Office of Cyber Security is divided into three functional groups, each overseen by a supervisory staff person who reports to the Chief Information Security Officer. The three groups, including their responsibilities, are:

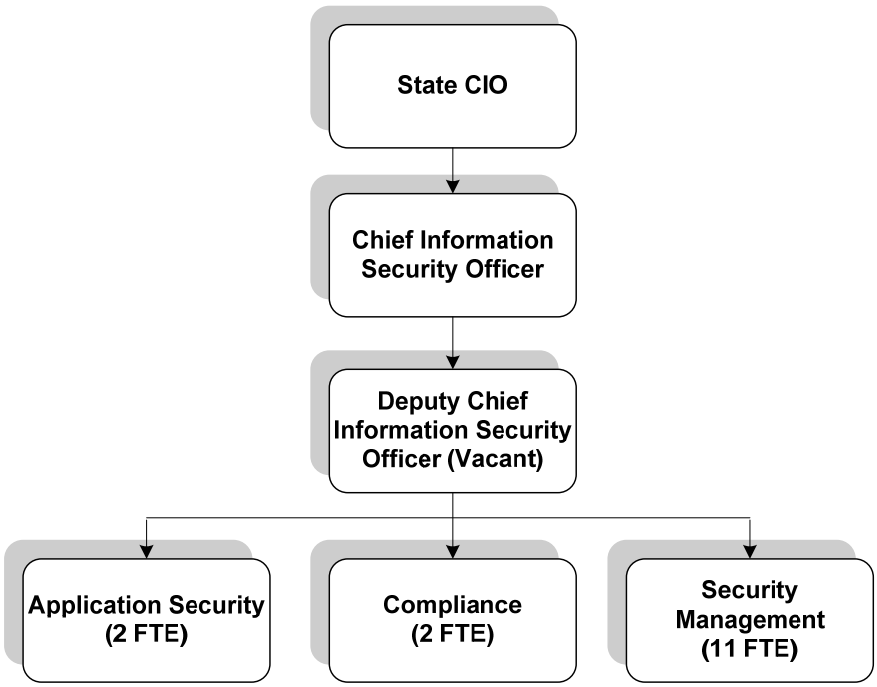
- **Compliance**. The compliance group contains two FTE and is responsible for assisting public agencies in achieving compliance with Colorado Cyber Security Policies and other applicable government and industry regulations, such as the Health Insurance Portability and Accountability Act's Security Policy or the Payment Card Industry's security requirements. The compliance group also tracks all IT audit and

compliance review findings identified by federal auditors and the Office of the State Auditor, and it works with the appropriate staff to ensure that remediation occurs in a timely manner. The compliance group does not perform IT audits or compliance reviews.

- **Security Management.** The security management group is the largest component of the Office of Cyber Security, totaling 11 FTE. The security management group includes the Colorado Information Security Operations Center (ISOC), which is responsible for detecting and responding to threats against the State's wide area network, and the information security officers assigned to handle the security requirements of all Executive Branch agencies. Through the ISOC, the security management group is responsible for network logging and monitoring related to the State's wide area network, uniform resource locator (URL) filtering, virtual private network (VPN) access provisioning, security architecture design and support, and incident identification and response.

- **Application Security.** The application security group is comprised of two staff who are responsible for ensuring that the State's web applications are securely designed. This group trains application developers on the principles of secure coding, reviews the development of state applications for compliance with secure coding principles, and is in the process of mapping and categorizing all state web applications.

Colorado Office of Cyber Security
As of October 2010



Source: Office of Cyber Security.

History and Milestones

Since its creation in 2006, the Office of Cyber Security has undergone significant organizational and leadership changes, including changes related to the consolidation of Executive Branch IT resources and staff. The bullets below identify the major organizational changes impacting the Office of Cyber Security.

- **June 2006**. Colorado Cyber Security Program is established with the enactment of House Bill 06-1157.

- **July 2006**. Office of Cyber Security is created within the Governor's Office. State's first Chief Information Security Officer is appointed by the Governor and reports directly to the Governor.

- **2006—2008**. Contract staff are hired to assist the Chief Information Security Officer in implementing the Colorado Cyber Security Program. The ISOC (including all staff) is transferred from the

Division of Information Technologies within the Department of Personnel & Administration to the Office of Cyber Security.

- **May 2008.** Resignation of the Chief Information Security Officer; duties assigned to contractors.

- **July 2008.** Senate Bill 08-155 moves the Office of Cyber Security under OIT, and the Chief Information Security Officer reports to the State CIO.

- **November 2008.** Appointment of new Chief Information Security Officer by the Governor.

- **June 2010**. Chief Information Security Officer resigns; duties assumed by the Deputy Chief Information Security Officer.

- **July 2010.** Executive Branch IT staff are consolidated under OIT. 15 FTE are transferred from state agencies to the Office of Cyber Security.

Cyber Security Threats and Trends

Research and data collected from information security research institutes and data privacy clearinghouses indicate that the number and sophistication of attacks against state government systems are increasing. According to a recent study conducted by Deloitte & Touche, LLP, on behalf of the National Association of State Chief Information Officers, more than one-fifth of reported data breaches in 2009 occurred in the state and local government sectors. Additionally, a recent study published by HP TippingPoint DVLabs and Qualys, which are computer security organizations that analyze vulnerabilities and develop appropriate countermeasures, showed that the government sector is the most targeted industry for several types of devastating attacks, including malicious Javascript and PHP "file include" attacks. Javascript attacks occur when an attacker induces a user, usually through a link in an email, to launch or run malicious Javascript-computer code on the user's computer. Based on the code run, the attacker may gain control of the user's browser or computer or obtain direct access to the user's login credentials. PHP file include attacks occur when attackers upload malicious PHP code onto a server. The uploaded PHP code is then automatically run by the web server and typically provides the attacker with complete control of the server or with access to databases and sensitive configuration files.

Attackers know that public agencies possess a significant amount of valuable data, and evidence shows that they are focused on obtaining it. The National Governors Association recently issued the following statement regarding the cyber security threat faced by state governments:

> One of our critical infrastructure assets, our state networks, are attacked on a daily basis. The failure to secure these networks has serious implications for national security, including continuity of government, the operations of critical infrastructure and the health, safety, and general welfare of citizens. Cyber attacks have disrupted state government networks, systems and operations, and potentially could impact first-responder communications during an attack on our homeland.

To understand the complexities involved in securing state systems and networks, it is first important to understand the threats that states confront and where those threats originate. A typical data breach originates from more than one type of vulnerability, and several kinds of attacks are used. For example, social tactics, such as eavesdropping on a conversation, may have been used to learn the operating system of a critical server. This valuable information could then be used by the attacker to build custom malware that avoids detection by anti-virus software, latches onto the vulnerable server, and proceeds to collect and transmit thousands of records back to the attacker.

The 2010 Verizon Data Breach Investigations Report provides helpful information for understanding the origination and responsible parties for data breaches. The analysis contained in the 2010 Verizon Data Breach Investigations Report consists of all confirmed data breaches investigated by Verizon and the United States Secret Service during 2009, including cases occurring both in the United States and internationally and both within government and private sector agencies. As the table on the following page indicates, this report found that the most common attack that resulted in a data breach was privilege misuse. Privilege misuse occurs when a trusted insider or former employee improperly uses his or her access to obtain confidential information for personal gain. Several of the data breaches noted in the study occurred when former system administrators or employees used known credentials to log into company systems and steal information they no longer had permission to view or obtain. Privilege misuse was the primary method used by a former Colorado Department of Revenue tax examiner to steal more than $10 million from the State. While employed at the Department, the employee misused the system credentials of other staff to perpetrate the fraud.

After privilege misuse, hacking and malware-based attacks are responsible for a significant number of data breaches and for the largest number of records compromised per breach. These attacks are typically coordinated and carried out by individuals or groups external to the agency attacked. The table below shows the most common types of attacks or threats that led to successful data breaches in 2009, according to investigations conducted throughout the world by Verizon and the United States Secret Service.

Origination of Data Breaches Investigated Throughout the World by Verizon and the United States Secret Service in 2009	
Origin of Breach	**Percentage of Total Breaches[1]**
Privilege Misuse	48
Hacking	40
Malware	38
Social Tactics	28
Physical Attacks	15

Source: Verizon 2010 Data Breach Investigations Report conducted by Verizon in coordination with the United States Secret Service.

[1]Percentages do not total 100 percent because there can be multiple reasons for a data breach.

One of the common misperceptions about information security is that an organization only needs to protect itself from outsiders or individuals external to its business. This concept is wrong for several reasons and could prove disastrous if used to build a perimeter-based security program—a program focused only on securing an organization's external network through firewalls and other networking equipment. First, as the table below demonstrates and as Colorado has experienced, insiders represent a significant threat to information security. In data breaches investigated by Verizon and the United States Secret Service in 2009, 48 percent resulted from actions by an insider, and another 11 percent were due to the actions of a business partner or contractor.

Responsible Parties for Data Breaches Investigated Throughout the World by Verizon and the United States Secret Service in 2009	
Responsible Party	**Percentage of Total Breaches[1]**
External Agents	70
Insiders (Employees)	48
Business Partners/Contractors	11
Multiple Parties	27

Source: Verizon 2010 Data Breach Investigations Report conducted by Verizon in coordination with the United States Secret Service.

[1]Percentages do not total 100 percent because multiple answers could apply to each breach.

Another reason to protect IT resources from both external and internal threats is that many of today's client-based attacks (attacks against client software such as Internet Explorer, Mozilla Firefox, and Adobe Acrobat) allow external parties to

gain access to an agency's internal network. Basically, with these types of attacks, the outsider becomes a trusted insider. All it takes for these client-side attacks to succeed is for an employee to make a poor decision and browse to a malicious website. Once the attacker latches onto or takes control of the employee's web browser, the attacker can then scan and attack the internal network just as if he or she were sitting inside the agency. Perimeter-based defenses such as firewalls are ineffective against these types of attacks.

In addition to these trends, the study published by HP TippingPoint DVLabs and Qualys identified the following common threats to IT systems in 2010:

- Web applications continue to be highly attractive targets and are constantly scanned and persistently attacked.
- Attackers have become more organized, sophisticated, and persistent.
- Increased use of social media and free software by employees has created new avenues for attack.
- Evolving technology and business processes like cloud computing, virtualization, and outsourcing bring new challenges to information security, including many that are not yet known.
- Legacy attacks such as viruses, phishing and pharming, zombie networks, SQL injection, and operating system-level vulnerabilities continue to be exploited quickly if proper security mechanisms are not followed.

Because of the diversity, nature, and source of the threats, information security touches on all aspects of a business or government organization, including not only technological controls but also controls related to personnel, physical security, contracting, and vendor management. To be effective, information security must not only involve technical tools such as firewalls and scanners but also focus on process improvement, training, and awareness. Finally, in today's risk environment, a security program must account for both internal and external threats and implement a layered or defense-in-depth security framework. A defense-in-depth security framework involves hardening (i.e., securing) not only the perimeter of an agency's network but also the internal network, including user computers, client software, intranets, and internal applications.

Audit Scope

This audit reviewed the Governor's Office of Cyber Security's progress in fulfilling the requirements of the Colorado Cyber Security Program (Section 24-37.5-401 through 406, C.R.S.). As part of the audit, we reviewed State Cyber

Security Policies, Agency Cyber Security Plans, and OIT strategic plans and budget documents; interviewed appropriate management, supervisory, and state information security staff; and surveyed other states' chief information security officers. Additionally, we performed a detailed analysis of the Office of Cyber Security's incident identification, reporting, and handling processes and procedures.

In conjunction with our review of the Office of Cyber Security, we contracted with a professional computer security firm to assist our staff in performing a covert penetration test of state networks, applications, and information systems. Penetration testing is a form of security testing in which evaluators attempt to circumvent the security features of systems to gain unauthorized access to data and systems. Our testing was authorized by Colorado's Chief Information Security Officer and management officials within the Governor's Office, Judicial Branch, Secretary of State's Office, Office of the State Treasurer, and Attorney General's Office.

Our testing was focused on Internet protocol (IP) addresses and systems owned and operated by a public agency, defined in Section 24-37.5-402(9), C.R.S. as "every state office, whether legislative, executive, or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions." The Legislative Branch was not included in the scope of this audit. A public agency as defined in this section does not include institutions of higher education or the Department of Higher Education. Some of the specific information systems tested included:

- Colorado Financial Reporting System (COFRS)
- Colorado Personnel and Payroll System (CPPS)
- GenTax (the Department of Revenue's tax system)
- Colorado Unemployment Benefits System (CUBS)
- Colorado Automated Tax System (CATS)
- Colorado Benefits Management System (CBMS)
- County Financial Management System (CFMS)
- Colorado Electronic Benefit Transfer System
- Veteran's Nursing Home Information System

- Medicaid Management Information System (MMIS)
- Colorado Crime Information Center (CCIC)

Because under House Bill 10-1401 the Office of the State Auditor does not have authority until August 2011 to audit the Statewide Internet Portal Authority (Authority), which is responsible for the management of the *colorado.gov* portal, no state applications hosted or housed by the Authority (such as the Colorado Online Tax Payment System) were included within the testing.

The remainder of our report is divided into two chapters. In Chapter 2 we discuss the steps the Office of Cyber Security should take to fully implement the Colorado Cyber Security Program and better secure state systems and data from unauthorized access. In Chapter 3 we provide the high-level, summarized results of the covert penetration test we performed against state systems and networks. That chapter also contains broad findings and recommendations that apply to most public agencies we tested. Due to the sensitive nature of the specific findings identified during testing, only summarized findings and recommendations are included in Chapter 3. The detailed, technical findings and recommendations are included in the appendices to this report that have been provided to the Office of Cyber Security, the Office of Information Technology, and affected public agencies. These appendices are confidential and not available to the public as authorized by the Open Meetings Law in Section 24-6-402(3)(a)(IV), C.R.S., and Public Records Law in Section 24-72-204(2)(a)(VIII), C.R.S. (2010).

This page intentionally left blank.

Colorado Cyber Security Program

Chapter 2

As previously discussed, the Colorado Cyber Security Program was established by the General Assembly in 2006 to ensure the confidentiality, integrity, and availability of state computer systems and protect the public's information entrusted to public agencies. The establishment of a single organization to coordinate and manage information security throughout the state government was key to the effective implementation of the Colorado Cyber Security Program. According to statute [Section 24-37.5-403, C.R.S.], the Office of Cyber Security is responsible for the implementation of the Colorado Cyber Security Program and for the day-to-day management of the State's information security operations.

As discussed in Chapter 3, we conducted a penetration test of public agencies and found significant vulnerabilities throughout state government that allowed the assessment team to compromise thousands of records containing individuals' confidential information, such as social security numbers, birth dates, and income levels. The assessment team also compromised several state networks and systems and identified hundreds of vulnerabilities in state systems. Based on the results of our penetration test, prior information technology audits, and our review of the implementation of the Colorado Cyber Security Program during this audit, we concluded that the Office of Cyber Security has failed to successfully implement the Colorado Cyber Security Program, as specified by statute. As such, the State and the information it receives from the public is at considerable risk of compromise unless significant changes are made.

In the following sections, we discuss specific areas where improvements are necessary to implement the State's Cyber Security Program.

Agency Cyber Security Plans

State statute [Section 24-37.5-404, C.R.S.] requires that all public agencies develop an information security plan, known as an Agency Cyber Security Plan (Plan), based on policies, standards, and guidelines established by the Chief Information Security Officer. The Plans are designed to help public agencies control the risks associated with access, use, storage, and sharing of sensitive information from the public and state electronic information and provide a mechanism for the Office of Cyber Security to use in determining an agency's compliance with the Colorado Cyber Security Program requirements. According to rules promulgated by the Chief Information Security Officer, each public

agency must submit a completed Plan to the Office of Cyber Security by July 15 of each year.

Pursuant to the rules promulgated by the Chief Information Security Officer, each public agency is to submit annually a Plan that contains the following components:

- **Cover letter requesting Plan approval**. An assertion signed by the Executive Director that either states that the agency is compliant with the Colorado Cyber Security Program or that the agency's Plan of Actions and Milestones, a corrective action plan, contains active initiatives that will bring the agency into compliance.

- **Agency Cyber Security Plan**. The agency's detailed Plan for implementing the Colorado Cyber Security Program and complying with State Cyber Security Policies.

- **Agency-Wide Risk Assessment**. An assessment that determines the extent of the potential threats and risks associated with an agency's information technology environment.

- **Agency Disaster Recovery Plan Summary**. An executive-level summary of the agency's detailed disaster recovery plan.

- **Agency Disaster Recovery Plan Test Results**. Results of the most recent disaster recovery tests performed by the agency.

- **Agency Self-Assessment Results**. Results from an annual self-assessment, which is designed to validate the security controls identified in the Agency Cyber Security Plan. The self-assessment should include vulnerability assessments, penetration tests, agency policy gap analysis, and security awareness training statistics.

- **Agency Cyber Security Plan of Action and Milestones**. A high-level plan that describes the cyber security initiatives underway to bring the agency into compliance with the Colorado Cyber Security Program.

The Chief Information Security Officer is responsible for reviewing the Plans to determine if they adhere to State Cyber Security Policies and to assess the agencies' progress in implementing the Colorado Cyber Security Program. Upon completion of his or her review, the Chief Information Security Officer is to issue one of three responses to the public agency:

- The Plan is <u>approved</u> with no changes necessary.

- The Plan is conditionally approved, with the requirement to implement, continue, or complete the initiatives in the Agency Plan of Actions and Milestones. Additionally, the Chief Information Security Officer may add additional requirements to the Plan of Actions and Milestones.

- The Plan is denied approval. If disapproved, the Chief Information Security Officer has the authority pursuant to Section 24-37.5-404(4), C.R.S., to remove the agency's connection to the State's wide area network, thereby removing the agency's ability to conduct business over the Internet.

We reviewed the Plan submission and review process for the July 15, 2010, reporting cycle and analyzed each public agency's Plan, if submitted. As shown in the table below, of the 20 public agencies required to submit plans to the Office of Cyber Security, we found that 12, or about 60 percent, had failed to submit the Plans by July 15, 2010. As of November 1, 2010, eight agencies had still not submitted Plans to the Office of Cyber Security.

Evaluation of Agency Cyber Security Plans
Public Agencies that Failed to Submit Plans by July 15, 2010

Public Agencies	Date Plan Submitted to the Office of Cyber Security
Department of Agriculture	July 27, 2010
Department of Healthcare Policy and Financing	November 9, 2010
Department of Labor and Employment	July 20, 2010
Department of Law	Not submitted
Department of Natural Resources	November 9, 2010
Department of Personnel & Administration	Not submitted
Department of Public Safety	July 23, 2010
Department of Regulatory Agencies	Not submitted
Department of Revenue[1]	September 21, 2010
Department of Treasury	Not submitted
Judicial Branch	Not submitted
Office of the Governor	Not submitted

Source: Office of the State Auditor analysis of information provided by the Office of Cyber Security.

[1] The Department of Revenue's Plan did not include information pertaining to the Colorado Lottery, which is located administratively within the Department.

Additionally, of the eight agencies whose Plans had been reviewed by the Office of Cyber Security as of September 15, 2010, only one agency's Plan, the Department of Human Services, contained all of the required components. Each component of the Plan is important, as one area supports another. For example, an agency should complete a thorough self-assessment to identify areas that need to be included in its annual risk assessment. Both the self-assessment and risk

assessment must be completed to prepare an accurate Plan of Actions and Milestones.

In the following table, for the eight agencies whose Cyber Security Plans were reviewed by the Office of Cyber Security as of September 15, 2010, we identified the number and percentage of the seven required components that were not submitted by each agency. As the table shows, the Departments of Labor and Employment and Local Affairs submitted Plans that were missing five of the seven required components, or were 71 percent incomplete. The Departments of Corrections, State, and Transportation submitted Plans that were missing three of the seven required components, or were 43 percent incomplete. Of the eight plans reviewed by the Office of Cyber Security, all contained the actual security Plan and Plan of Actions and Milestones. However, the majority of submitted plans failed to include a cover letter signed by the agency's Executive Director, a disaster recovery plan summary, and the most recent results from the agency's disaster recovery tests and self-assessments.

Evaluation of Agency Cyber Security Plans
Reviewed for Fiscal Year 2011
As of September 15, 2010

Public Agency	Number of Required Components Not Submitted[1]	Percentage of Required Components Not Submitted
Department of Corrections	3	43%
Department of Education	2	29
Department of Human Services	0	0
Department of Labor and Employment	5	71
Department of Local Affairs	5	71
Department of Public Health and Environment	2	29
Department of State	3	43
Department of Transportation	3	43

Source: Office of the State Auditor analysis of information provided by the Office of Cyber Security.

[1] Plan requirements are based on rules promulgated by the Chief Information Security Officer and include (1) Signed Cover Letter, (2) Updated Security Plan, (3) Updated Risk Assessment, (4) Disaster Recovery Plan Summary, (5) Disaster Recovery Plan Test Results, (6) Updated Self-Assessment Results, and (7) Plan of Actions and Milestones.

In addition to the lack of timely and complete submissions, we found that the Plans of agencies are often incomplete, inaccurate, and lacking in detailed and meaningful information. Specifically, we found that the Plans we reviewed were missing information on critical information systems and were so general as to be

meaningless. Additionally, we found that control gaps agencies noted in the risk assessments lacked specific remediation dates, and items agencies noted in the Plan of Actions and Milestones documents did not appear to have direct correlations to these control gaps. The Plan of Action and Milestones should include all control gaps noted in an agency's risk assessment to ensure that agency management is aware of the deficiencies and that a plan is in place to remediate the problems.

We also found that the Office of Cyber Security has not effectively utilized the information contained in the agency Plans for strategic planning purposes. To obtain greater value from the Plans, it is important that the information be used for strategic planning and budgeting purposes. For example, if most agencies report that they lack an effective intrusion detection system, then it may be appropriate for the Office of Cyber Security to make the procurement of an integrated intrusion detection system a strategic priority. Additionally, the Office of Cyber Security should consider developing a plan for implementing compensating controls until a system can be procured and implemented. We address the lack of strategic planning later in this chapter.

We met with agency information security officers, Office of Cyber Security management staff, and other IT personnel to determine the cause for the problems we identified with agency Plans. Through these discussions, we learned that many agency staff consider the Agency Cyber Security Plan development and submission process to be an unfunded mandate, confusing, and overly time consuming. Others also suggested that the Plan provides very little assurance that an agency is complying with the Colorado Cyber Security Program and takes time that would be better spent actually securing state systems and networks. Agency staff expressed frustration with the fact that the Office of Cyber Security has not established sufficient guidelines for completing each of the Plan's components, fails to provide feedback to agencies once the Plan is submitted, and does not take enforcement action against those agencies that fail to submit complete Plans. As such, many of those we spoke with indicated that the Plan development and submission process is not taken seriously and is simply seen as a "box that needs to be checked."

Our audit confirmed many of the issues identified by agency staff. For example, the Office of Cyber Security has not issued guidance on the completion of Agency Cyber Security Plans, risk assessments, self-assessments, Plans of Actions and Milestones, and disaster recovery planning. Also, until this year, the Office of Cyber Security had not established a process for reviewing and scoring submitted Plans for compliance with Colorado Cyber Security Policies. Additionally, the Office of Cyber Security has not provided formal feedback or responded to agencies on the submission of their Plans since 2007. Finally, the Office of Cyber Security has not taken enforcement action against any of the agencies that have either failed to submit Plans or continue to submit incomplete Plans.

Higher Education

As noted earlier, neither the Department of Higher Education nor institutions of higher education are defined as public agencies by the Colorado Cyber Security Program and are therefore not required to adhere to the policies, standards, and guidelines established by the Chief Information Security Officer. However, statute [Section 24-37.5-404.5, C.R.S.] requires that the Department of Higher Education and each institution of higher education, in coordination with the Colorado Commission on Higher Education (Commission), develop an information security plan. Similar to public agencies, the institutions' plans can contain a phase-in period not to exceed three years. The plans are to be submitted to the Commission by July 1 of each year for review and comment. The Commission is then required to submit the plans to the Chief Information Security Officer and report on the development, implementation, and, if applicable, compliance with the phase-in schedule of the information security plan for each institution.

We found that with the exception of the Colorado Historical Society, the Department of Higher Education has never submitted a Plan. Additionally, we met with officials from the Department of Higher Education and Office of Cyber Security and found that the information security plans for institutions of higher education are not being consistently collected, reviewed, and shared with the Office of Cyber Security. Of the 24 public institutions of higher education in Colorado, the Department of Higher Education had not received any security plans for 2010 as of October 15, 2010. According to Department of Higher Education officials, the Department has never submitted information security plans for these institutions to the Office of Cyber Security, nor has it been contacted by the Office of Cyber Security to do so. Neither the Department nor the Office of Cyber Security has developed the necessary processes and procedures to comply with this component of the Colorado Cyber Security Program.

Improvements

To ensure that Agency Cyber Security Plans are prepared and submitted according to statutory requirements, the Governor's Office of Information Technology needs to work with the Office of Cyber Security to make several improvements. First, the Office of Cyber Security needs to establish additional guidelines and procedures for the completion of the Agency Cyber Security Plan. Once the guidelines and procedures are finalized, the Office of Cyber Security should provide training to information security officers and relevant agency staff on the proper development and submission of the Plan. Second, the Office of Cyber Security needs to develop the necessary processes to ensure that Agency Cyber Security Plans are reviewed in a timely manner. As part of the review process, Office staff need to ensure that all control gaps listed in the agencies' risk

assessments are included in the Plans of Actions and Milestones. If necessary, the Office of Cyber Security should add actions and work steps to agencies' Plans of Actions and Milestones to ensure all control gaps are being addressed.

Third, at the conclusion of the review process, the Office of Cyber Security should provide written feedback on its evaluation of the Plans to state agency executive management. To ensure adjustments to Plans can be made in a timely manner, the Office of Cyber Security should establish a policy that requires written feedback to be delivered to public agencies within a reasonable period of time—e.g., within 45 days. Additionally, the Office of Cyber Security should clearly communicate the changes that are necessary to bring the Plan into compliance with State Cyber Security Policies. Fourth, the Office of Cyber Security should work with the State Chief Information Officer to hold agencies and information security officers accountable for the timely submission of Agency Cyber Security Plans. Fifth, the Office of Cyber Security should use the agencies' Cyber Security Plans as input for its strategic planning process. Finally, the Office of Cyber Security needs to work with the Commission on Higher Education to ensure that the security plans developed by institutions of higher education are received and reviewed annually.

Recommendation No. 1:

The Governor's Office of Information Technology should work with the Office of Cyber Security to reevaluate and improve the Agency Cyber Security Plan development, submission, and review process by:

a. Establishing additional guidelines and procedures for the completion of the Agency Cyber Security Plan, including further guidance related to the performance and documentation of agency risk assessments and self-assessments.

b. Providing training to agency information security officers on the completion and submission of the Agency Cyber Security Plans.

c. Developing and implementing a policy that requires written feedback on submitted Plans to be delivered to public agencies within a reasonable period of time—e.g., within 45 days.

d. Reviewing all Agency Cyber Security Plans submitted to the Office of Cyber Security and providing timely feedback to the agencies, including updating the agencies' Plans of Actions and Milestones to ensure that all control gaps are addressed.

e. Holding agencies accountable for the timely submission of statutorily-compliant Agency Cyber Security Plans by reporting non-compliant agencies to the Governor or appropriate oversight body or executive, such as the Attorney General or the Chief Justice of the Supreme Court.

f. Ensuring that agencies' risk assessments include specific dates for remediating identified control gaps and that Plans of Actions & Milestones align with the agencies' risk assessments.

g. Incorporating the information contained in the Agency Cyber Security Plans into the Office of Cyber Security's strategic planning process.

h. Working with the Colorado Commission on Higher Education to ensure that security plans developed by institutions of higher education are being received annually and reviewed, as required by statute.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

The Agency Cyber Security Plan (ACSP) was never intended to be utilized as a "paper exercise" but as a strategic document to manage the agency cyber security program. The Office of Cyber Security (OCS) is currently revising the management policies, procedures, training, and practices governing the requirements, development, maintenance, evaluation, and enhancement of State of Colorado ACSPs.

For example, OCS recently developed an ACSP Scorecard to provide guidance to non-consolidated agencies, Governor's Office of Information Technology (OIT), and Colorado Commission on Higher Education on areas of improvement to their ACSP. Another example is moving from having individual ACSPs for Executive branch consolidated agencies to having a single consolidated cyber security plan for the State.

To improve the ACSP submission process, OCS will develop an internal policy that requires that the ACSP Scorecard be completed and provided to the reporting agency within 90 days of the Plan's submission. Additionally, OCS will work with OIT senior leadership to hold agencies accountable for the timely submission of statutorily compliant ACSPs. OCS will also be working with the Colorado Commission on Higher Education to develop formal submission procedures for the security plans developed by institutions of higher education.

OCS has also adopted and implemented a statewide tool, called the Colorado Risk, Incident, & Security Compliance (CRISC) system, to document and manage all identified security deficiencies on state systems using a comprehensive and consistent risk management process that meets the Risk Management Framework developed by the National Institute of Standards and Technology. Plans of Action and Milestones (POAM) are automatically generated from the tool allowing state personnel that are responsible for their agency POAM to spend their limited time on other agency mission critical tasks. This information will be used to guide the State on focusing limited resources (people, time, budget) to address the most important risks with the highest level of impact to the State.

Cyber Security Incidents

The timely identification and reporting of cyber security incidents is a critical component of an effective cyber security program. Research shows that the longer an incident goes undetected or unreported, the greater the damage is to information resources and the more significant the loss of data. State statute [Section 24-37.5-405 and Section 24-37.5-404.5(2)(e), C.R.S.] and State Cyber Security Policies require public agencies and institutions of higher education to report all cyber security incidents to the Office of Cyber Security. A cyber security incident is defined as an accidental or deliberate event that results in or constitutes an imminent threat of unauthorized access, loss, disclosure, modification, disruption, or destruction of communications and information resources. Examples of cyber security incidents include malicious code found on agency servers, viruses, missing or stolen computer equipment, and the unintentional disclosure of protected information to unauthorized persons through email, fax, or phone.

The Office of Cyber Security depends on the timely and accurate reporting of incidents for several reasons. First, the Office of Cyber Security is charged by statute with directing and managing appropriate responses to cyber security incidents that affect state information systems. The Office of Cyber Security has access to trained staff and contractors who can be deployed based on the type and severity of the incident. Additionally, the Office of Cyber Security has experience and training for properly handling all phases of an incident. Second, the Office of Cyber Security needs to be aware of all incidents occurring within state systems to determine if a coordinated attack against state government is underway. Although an agency may believe that an incident it identified is isolated, it may actually be the first phase of a more sophisticated attack against other public agencies. Finally, incident reports provide information needed by the Office of Cyber Security to accurately assess the threats facing state government so that proper mitigation strategies can be devised and implemented.

Incident Reporting

To determine if the Office of Cyber Security is receiving reports of all incidents identified, we analyzed the incidents reported to the Office of Cyber Security between October 2006 and September 2010, interviewed state IT staff, and monitored the number of reports generated from our penetration testing activities. Overall, we concluded that the Office of Cyber Security is not receiving reports of all cyber security incidents that are affecting state government and public institutions of higher education. First, as indicated by the table below, the Office of Cyber Security has received reports of 43 incidents in the last four years. The majority of these reports occurred in 2007 and 2008. Based on our knowledge of state operations, industry trends and statistics, and discussions with Office of Cyber Security staff, 43 reported incidents in four years is low and likely does not include all incidents occurring and detected within state information systems.

Cyber Security Incident Reports Reported by Pubic Agencies 2006 -2010[1]

Year[1]	Number of Agencies Reporting	Number of Reported Incidents
2006	1	1
2007	9	9
2008	13	26
2009	3	3
2010	4	4
Total Incidents Reported		43

Source: Office of the State Auditor analysis of Office of Cyber Security incident data.
[1] Data available for October 2006 through September 2010.

Second, of the 43 incidents reported to the Office of Cyber Security, none was reported by institutions of higher education. It is improbable that institutions of higher education have not had a cyber security incident in the last four years; therefore, such incidents are likely occurring but not being reported to the Office of Cyber Security, as required by statute. Third, we estimate that our penetration testing activities should have generated approximately 40 to 60 incident reports over the last six months. The Office of Cyber Security, however, only received four reports unrelated to our penetration testing over the six month period of April through September 2010. Additionally, during testing we became aware of an existing and ongoing incident at one agency that had never been reported to the Office of Cyber Security. Finally, we analyzed the data breaches reported in the media and on the Privacy Rights Clearinghouse website, a clearinghouse for collecting information on known data breaches, and compared those breaches involving public agencies and institutions of higher education to the incidents reported to the Office of Cyber Security. We identified seven data breaches that

should have been reported to the Office of Cyber Security but were not. Some of these breaches resulted in the exposure of personal information.

We identified the following reasons for the low number of security incidents reported to the Office of Cyber Security:

- Some agency staff reported that they do not believe it is necessary or important to report commonly occurring or "routine" incidents, such as viruses and unsuccessful attacks—e.g., multiple failed attempts to log on to a server or network device.

- The Office of Cyber Security has not established the necessary processes, procedures, and working relationships with the Department of Higher Education and public institutions of higher education to obtain incidents occurring within those environments.

- Agencies outside of the Executive Branch are reluctant to submit incidents to the Office of Cyber Security. These agencies believe sharing such information is an infringement on the separation of powers principle of state government.

- The State's intrusion detection capabilities are not sufficient for detecting many types of cyber security incidents. Due to the sensitive nature of these deficiencies, we included the details within the confidential appendices of this report.

Incident Response and Analysis

Once an incident is detected and reported, it is important that a coordinated and professional response occur. Failure to properly respond to an incident can result in increased system damage and downtime, as well as the inability to prosecute the attacker due to inadequate and inadmissible information or evidence. Proper incident response requires knowledgeable and trained staff and updated and detailed procedures and plans. Additionally, cyber security incidents should be tracked and analyzed to determine the most common targets and types of attacks launched against the State.

Statute [Section 24-37.5-405, C.R.S.] provides the Chief Information Security Officer with the authority to coordinate the State's response to cyber security incidents, including, if necessary, entering into contracts with private persons or entities to assist state staff in resolving incidents. The Chief Information Security Officer also has the authority to temporarily discontinue or suspend the operation of a public agency's communication and information resources in order to isolate the source of a security incident. We reviewed the Office of Cyber Security's

incident response processes and procedures, including the State Cyber Security Incident Response Plan, and identified the following specific problems:

- **Inadequate training**. We found that agency staff with responsibilities for incident response have generally not received sufficient training to effectively recognize, respond to, and report cyber security incidents. Although the Office of Cyber Security has provided some informal training to information security officers related to incident response, the training has not been comprehensive or realistic and has not included other key staff, such as system and network administrators. Additionally, the Office of Cyber Security does not routinely conduct debriefings or "lessons-learned meetings" following the investigation and handling of a security incident. Debriefings are an excellent way for staff to learn from their mistakes and improve their skills.

- **Outdated State Incident Response Plan**. In accordance with its duties and responsibilities within Section 24-37.5-405, C.R.S., the Office of Cyber Security developed a State Incident Response Plan for directing the State's response to cyber security incidents. We reviewed the State Incident Response Plan and found that it was outdated and contained inaccurate information. For example, key staff listed as responsible for carrying out portions of the State's Incident Response Plan no longer work for the State. Other staff listed in the plan have been moved into other, unrelated positions.

- **Lack of detailed and cohesive agency-level procedures**. State Cyber Security Policies require that agencies develop agency-level procedures for responding to cyber security incidents. We found that most agencies have not developed procedures in sufficient detail to appropriately direct staff during the handling of an incident. Additionally, we found that agency staff are unclear as to which incident response plan to use, the State Incident Response Plan or the agency-level incident response procedures. We also found that agency level procedures conflict with procedures contained in the State Incident Response Plan.

- **Lack of an electronic incident reporting and tracking system.** The Office of Cyber Security lacks an electronic incident reporting and tracking system. Incidents are reported via phone, email, or fax, and reports are maintained in hardcopy format. The lack of an automated electronic reporting and tracking system makes it difficult for the management staff within the Office of Cyber Security to track and analyze the timing and nature of cyber security incidents.

As part of the penetration test, we also identified a weakness in one agency's response to our social engineering attack (see Chapter 3 for a definition of this

type of attack). Instead of forcing password changes on compromised accounts, the system administrators within this agency left it up to the individual users to change their account passwords. Because individual users did not change their passwords timely, the assessment team was able to retain access to this agency's internal network and information systems for an additional six weeks following the initial identification of the breach.

The Office of Cyber Security has failed to ensure that the State has the processes, procedures, and technology necessary to identify, respond to, and analyze cyber security incidents occurring within computer systems of the State and institutions of higher education. Several changes need to occur to ensure that the State is prepared for cyber security incidents. These changes include communicating with agencies and institutions of higher education about their responsibilities to report security incidents; increasing the training for incident responders, system users, and system administrators; updating and coordinating agency and state incident response procedures; implementing an electronic incident response reporting, tracking, and analysis system; utilizing incident response debriefings; and revising incident response procedures to require that system administrators enforce password changes on user accounts suspected of being compromised.

Recommendation No. 2:

The Governor's Office of Information Technology should improve the State's incident identification, reporting, analysis, and response processes and procedures by:

a. Ensuring that all public agencies, including the Department of Higher Education and institutions of higher education, are aware of their responsibilities to report cyber security incidents to the Office of Cyber Security.

b. Providing training to employees, information security officers, and system administrators in incident awareness, identification, documentation, response, and reporting.

c. Updating the State Incident Response Plan.

d. Ensuring that each public agency has detailed, written procedures for responding to security incidents and that agency-level procedures align with the procedures contained in the State Incident Response Plan.

e. Implementing an automated incident response reporting and tracking system and analyzing and reporting incidents to senior management within the Governor's Office of Information Technology on a periodic basis.

f. Performing incident response debriefings with appropriate staff to further improve the Office's incident response capabilities.

g. Updating incident response procedures to require that system administrators enforce password changes on accounts that are suspected of being compromised.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

The Office of Cyber Security (OCS) Colorado Risk, Incident, & Security Compliance (CRISC) tool has an Incident Response (IR) module that will be used by OCS for a centralized Computer Incident Response Capability (CIRC) that meets all IR criteria as defined by NIST Guidance (SP 800-61: Computer Security Incident Handling Guide) as well as US-CERT reporting requirements. This will aid OCS and state agencies in streamlining and improving incident response processes, provide incident tracking through consistent IR workflows, enhanced incident analysis capabilities, and provide increased statewide incident visibility and IR reporting for state management. The current OCS State IR Plan is being updated to incorporate Governor's Office of Information Technology (OIT) staff within other IT operational bands as part of a State Computer Security Incident Response Team (CSIRT). Training for all roles and responsibilities identified in the IR Plan will be developed and offered through the OCS state online security training system and formal debriefings will be instituted following the resolution of cyber security incidents occurring within consolidated agencies. As part of the ACSP review process, OCS will also work to ensure that agencies have sufficiently detailed incident response procedures that align with the OCS State IR Plan.

A first responder tool has been developed by OCS to be utilized by state incident first responders to collect data on suspected compromised systems that automatically sends IR data back to the Information Security Operations Center (ISOC) for analysis. This tool will increase the state IR response time and analysis throughout the State, especially at remote state offices where any state staff resource can be utilized to collect data from a system for investigation. IR reporting requirements have been incorporated into the State Security Awareness Training, which is presented during monthly OIT staff meetings, updated on the State Chief Information Security Officer (CISO) website, and distributed through security awareness posters.

OCS will also work with the Chief Technology Officer's office and agency Information Security Officers to ensure that system administrators know to enforce password changes on accounts that are suspected of being compromised following an incident. OCS will also ensure that this is a standard procedure included in agency-level IR procedures.

Colorado Cyber Security Program Requirements

In addition to the areas of overseeing agency security plans and responding to security incidents, we reviewed other requirements contained in statutes related to the Office of Cyber Security. Statutes [Sections 24-37.5-403 through 406, C.R.S.] stipulate the requirements of the Colorado Cyber Security Program and specify the duties and responsibilities of the Chief Information Security Officer. The requirements contained in statute are based on information security best practices and represent Colorado's cyber security framework, or philosophy for securing the data and systems maintained by state government. The Chief Information Security Officer and public agencies are required to be knowledgeable of and compliant with these statutory provisions.

We reviewed the statutory requirements of the Colorado Cyber Security Program and evaluated whether the Office of Cyber Security had developed processes and procedures for complying with these provisions. Based on our review, we determined that the Office of Cyber Security has not implemented a significant number of the requirements of the Colorado Cyber Security Program, as specified by statute. We list the specific areas of compliance and non-compliance in the following table.

Evaluation of the Office of Cyber Security's Compliance with the Statutory Requirements of the Colorado Cyber Security Program

Statute	Requirement	Audit Finding
24-37.5-403(2)(a)	Develop and update information security policies, standards, and guidelines for public agencies.	Compliant. In 2006, the Office of Cyber Security developed the Colorado State Cyber Security Policies. Non-compliant. The Office of Cyber Security has not routinely reviewed and updated cyber security policies, standards, and guidelines. Most policies have not been updated since they were first created in 2006.

Evaluation of the Office of Cyber Security's Compliance with the Statutory Requirements of the Colorado Cyber Security Program		
Statute	**Requirement**	**Audit Finding**
24-37.5-403(2)(b)	Promulgate rules pursuant to the Colorado Cyber Security Program containing information security policies, standards, and guidelines for public agencies on or before December 31, 2006.	Compliant. The Office of Cyber Security promulgated rules for public agencies to follow on or before December 31, 2006 (8 CCR 1501-5).
24-37.5-403(2)(c)	Ensure the incorporation of and compliance with information security policies, standards, and guidelines in the information security plans developed by public agencies.	Non-compliant. The Office of Cyber Security has not ensured that public agencies are submitting security plans that comply with State Cyber Security Policies.
24-37.5-403(2)(d)	Direct information security audits and assessments in public agencies in order to ensure program compliance and adjustments.	Non-compliant. The Office of Cyber Security has not conducted or directed security audits and assessments in public agencies to ensure compliance with State Cyber Security Policies.
24-37.5-403(2)(e)	Establish and direct a risk management process to identify information security risks in public agencies and deploy risk mitigation strategies, processes, and procedures.	Non-compliant. Although risk assessments are being completed by some public agencies, the Office of Cyber Security has not used the assessments to deploy risk mitigation strategies, processes, and procedures throughout the State. Additionally, the risk assessments performed by public agencies are oftentimes incomplete and not reflective of the agencies' operating environment.
24-37.5-403(2)(f)	Approve or disapprove and review annually the information security plans of public agencies.	Non-compliant. The Office of Cyber Security has not consistently reviewed the security plans submitted by public agencies and has failed to communicate the results of its reviews to public agencies.
24-37.5-403(2)(g)	Conduct information security awareness and training programs.	Non-Compliant. The Office of Cyber Security has not

Evaluation of the Office of Cyber Security's Compliance with the Statutory Requirements of the Colorado Cyber Security Program		
Statute	**Requirement**	**Audit Finding**
		developed an effective information security awareness and training program. Most state employees have not received cyber security awareness training in the last three years.
24-37.5-403(2)(h)	In coordination and consultation with the Office of State Planning and Budgeting and the Chief Information Officer, review public agency budget requests related to information security systems and approve such budget requests for state agencies other than the Legislative Department.	Non-compliant. The Office of Cyber Security has not established a formal process for reviewing public agency budget requests related to information security systems. Additionally, the Office of Cyber Security has not developed a formal process for identifying the information security needs of public agencies, prioritizing needs based on risk, and developing and submitting consolidated cyber security budget requests to OIT, the Office of State Planning and Budgeting, and the Joint Budget Committee.
24-37.5-403(2)(i)	Coordinate with the Colorado Commission on Higher Education for purposes of reviewing and commenting on information security plans adopted by institutions of higher education that are submitted pursuant to Section 24-37.5-404.5(3), C.R.S.	Non-compliant. The Office of Cyber Security has not developed a process with the Colorado Commission on Higher Education for the annual review of security plans adopted by institutions of higher education. Since established in 2006, the Office of Cyber Security has not received or reviewed the security plans adopted by institutions of higher education.
24-37.5-406	The Chief Information Security Officer is to report to the Governor quarterly on the implementation of the Colorado Cyber Security Program.	Non-compliant. At the time of our review, the Office of Cyber Security had not established performance measures or metrics for assessing the

Evaluation of the Office of Cyber Security's Compliance with the Statutory Requirements of the Colorado Cyber Security Program		
Statute	**Requirement**	**Audit Finding**
		implementation of the Colorado Cyber Security Program. Additionally, the Chief Information Security Officer has not been making quarterly reports to the Governor.
Source: Office of the State Auditor evaluation of the Office of Cyber Security's compliance with the statutory requirements of the Colorado Cyber Security Program.		

The Office of Cyber Security's failure to comply with and enforce the statutory requirements of the Colorado Cyber Security Program puts the State at greater risk of a data breach or system compromise. We found that the Office of Cyber Security has failed to comply with the above-mentioned statutory provisions for numerous reasons, including leadership's lack of knowledge and understanding of all statutory requirements, undefined priorities by the Office of Cyber Security leadership, and poor project management and oversight. To ensure that the Colorado Cyber Security Program is a success, the Governor's Office of Information Technology needs to increase its oversight of the Office of Cyber Security and take the steps outlined in the recommendation below.

Recommendation No. 3:

The Governor's Office of Information Technology should ensure that the Office of Cyber Security has implemented and is complying with all statutory requirements of the Colorado Cyber Security Program by:

a. Inventorying all statutory requirements that pertain to the Colorado Cyber Security Program.

b. Ensuring that the Chief Information Security Officer is aware of his or her duties and responsibilities and is knowledgeable of all statutory requirements of the Colorado Cyber Security Program.

c. Developing and executing a work plan to bring the Office of Cyber Security and public agencies into compliance with Colorado Cyber Security Program requirements.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

It is the responsibility of the Chief Information Security Officer (CISO) to ensure that he fully understands the statutory requirements of the Colorado Cyber Security Program (CCSP), his or her duties and responsibilities to meet these requirements, and provide the leadership and direction for the Office of Cyber Security (OCS) to ensure that these requirements are being met. Steps have already been taken to prioritize all OCS staff and activities to create, improve and consistently follow OCS processes to meet all statutory requirements and CISO strategic initiatives.

Strategic Planning and Management Oversight

The strategic planning process is one of the fundamental ways in which an organization creates its unique sense of identity and purpose. Through defining its mission, goals, and methods of measuring success, an organization develops the foundation for making policy decisions and prioritizing the use of limited resources. The exercise of strategic planning is critical for the Office of Cyber Security because of the numerous and competing demands placed upon its staff and limited budget.

The Office of Cyber Security lacks a strategic plan for directing its operations. This lack of planning has resulted in many of the problems identified throughout our report. Additionally, the information security and agency business staff continually expressed concerns about the Office of Cyber Security's overall lack of vision and direction, including management's failure to establish and communicate priorities to its staff and stakeholders. We also found that the Office of Cyber Security lacks any meaningful metrics or measures for assessing its performance and does not have the processes and procedures in place to collect and analyze meaningful cyber security information. For example, during the audit we requested but were unable to obtain information related to:

- The number of public agencies that have fully implemented the Colorado Cyber Security Program.

- The number of high- and medium-level vulnerabilities identified by information security officers as part of their agencies' annual self-assessments, including the number of vulnerabilities remediated.

- The total number of security assessments and security awareness trainings completed by the Office of Cyber Security and agency information security officers in the last year.

- The number and types of cyber security attacks launched against state systems in the last year, including the Office of Cyber Security's activities to mitigate these threats.

To ensure that the Office of Cyber Security is addressing the right issues, complying with statutory requirements, using its resources and staff wisely, and meeting the intent expressed by the General Assembly in House Bill 06-1157, the Office of Cyber Security should work with the Governor's Office of Information Technology to develop a comprehensive strategic plan. The plan should include the Office of Cyber Security's mission, vision, goals, objectives, and short- and long-term priorities. The Office of Cyber Security should also identify performance targets that, if reached, indicate that the Office is on track to achieving its goals and meeting its mission. The plan should be reviewed and updated regularly and whenever major changes occur in the State's information security environment. The plan should be communicated to the Office of Cyber Security's staff, Governor's Office of Information Technology management, and stakeholders within public agencies and institutions of higher education.

Management Oversight and Leadership

As demonstrated throughout our report, we found that the Governor's Office of Information Technology's oversight of the Office of Cyber Security needs to be improved. During the four years since the enactment of House Bill 06-1157, the Colorado Cyber Security Program has still not been implemented, as required by statute. Statutory requirements have not been met, and as demonstrated in Chapter 3, significant vulnerabilities persist in state information systems and networks. We found that a lack of effective leadership within the Office of Cyber Security and lack of oversight by the Governor's Office of Information Technology led to many of the problems identified in our audit, including the Office of Cyber Security's failure to:

- Implement the Colorado Cyber Security Program and comply with statutory requirements.

- Provide timely feedback to agencies concerning their submission of the statutorily required Agency Cyber Security Plans.

- Communicate the requirements of the Colorado Cyber Security Program to key stakeholders, including public agencies, institutions of higher education, and the Department of Higher Education.

- Hold public agencies and state staff accountable for their responsibilities with regard to implementing the Colorado Cyber Security Program and complying with State Cyber Security Policies.

- Implement an effective compliance program to ensure that State Cyber Security Policies and standards are being uniformly applied.

- Remediate known and existing vulnerabilities in a timely manner.

- Develop and implement a comprehensive information security training program for those tasked with information security responsibilities.

The Governor's Office of Information Technology should take immediate steps to strengthen its oversight of the Office of Cyber Security, including the establishment of effective leadership within the Office of Cyber Security to reduce the State's level of exposure to cyber security attacks.

Recommendation No. 4:

The Governor's Office of Information Technology should work with the Office of Cyber Security to develop a strategic plan for the State's cyber security operations. The strategic plan should establish the Office of Cyber Security's mission, vision, goals, objectives, and short- and long-term priorities and include measurable objectives that can be used to assess the Office's progress in achieving its goals. Once finalized, the Office of Cyber Security should communicate the contents of its strategic plan to information security staff and the key stakeholders within public agencies and institutions of higher education. Finally, the Governor's Office of Information Technology should increase its oversight of the Office of Cyber Security and ensure that an effective leadership structure is in place to carry out the strategic plan and implement the Colorado Cyber Security Program.

Governor's Office of Information Technology Response:

Agree. Implementation Date: January 2011.

The Office of Cyber Security (OCS) has developed a strategic plan for the State's cyber security operations. The strategic plan establishes the OCS's mission, vision, goals, objectives, and short- and long-term priorities and includes measurable objectives that can be used to assess the Office's progress in achieving its goals. Upon review and approval by the State CIO, the strategic plan will be communicated to information security staff

and key stakeholders within public agencies and institutions of higher education. The Governor's Office of Information Technology (OIT) has recently made strategic leadership changes within OCS and has increased its oversight of OCS operations to ensure that the Colorado Cyber Security Program is being effectively carried out. OIT senior leadership will also be closely monitoring OCS' implementation of the audit recommendations to ensure appropriate mitigation strategies are being executed.

Penetration Test Results

Chapter 3

As stated earlier, the State collects and maintains a considerable amount of sensitive data and is responsible for protecting it. As part of our audit, we assessed the State's information security posture or preparedness and exposure to cyber attacks by performing a covert penetration test of state networks and information systems. A penetration test is a method for evaluating the security of networks and computer systems by simulating attacks from malicious sources. The purpose of a penetration test is to both assess an organization's risk of being compromised by a malicious attacker and to identify and recommend steps for preventing such attacks. The scope of our testing included all networks, systems, modems, wireless network devices, and Internet Protocol addresses (IP addresses) owned and operated by public agencies. Our audit did not include tests of any systems hosted or housed on the *colorado.gov* domain, as explained in Chapter 1.

The penetration testing was performed by a team composed of staff from a professional computer security firm under contract with the Office of the State Auditor (OSA), as well as staff from the OSA. Throughout Chapter 3 this team is referred to as the "assessment team" or "team." Team members had expertise in areas associated with malicious computer and system attacks, including social engineering, which involves the act of manipulating people to perform a specific action or divulge confidential information; network and web application security testing; wireless device assessments; and exploit development and execution, which is the process of writing and launching customized computer code to take control of computer systems. To simulate real attacks against state systems, the team was authorized by executive-level staff from the Governor's Office to use all available attack types and techniques to gain unauthorized access to state systems and data, including social engineering and physical-based attacks—i.e., gaining unauthorized physical access to network devices and systems. The team was provided with no advance information about the systems or networks to be tested, just as a real attacker would have no such information. In order to test the State's ability to detect and respond to an attack, state IT staff, including agency information security officers, were not notified in advance of the testing. Active testing was conducted between March 30, 2010, and September 30, 2010.

Test Objectives

The initial scope of the penetration test encompassed more than 67,000 IP addresses (computer systems and network devices), 15 key state agency

applications (e.g., the Colorado Benefits Management System, Colorado Financial Reporting System, Colorado Personnel and Payroll System, GenTax, County Financial Management System, Medicaid Management Information System), 18 physical sites or state buildings, all state-owned wireless network devices identified during testing activities, and 10,760 phone numbers. Due to the size of the State's information technology footprint and the time allotted for testing, we performed preliminary analysis and identified the following areas on which to focus our testing:

- State systems collecting, processing, and storing sensitive and confidential data such as tax records, social security numbers, criminal histories, and personal health information.

- Systems and facilities considered to be the State's most vulnerable in terms of IT security risks.

- Systems where an attacker could make a significant impact, such as high-profile websites at risk for defacement.

Additionally, the Governor's Office of Information Technology provided the names of 15 applications that are critical to state operations and should be tested. Other than the names of the applications, no other information was provided to the team, such as IP address or operating system version.

In cooperation with the Office of Cyber Security, the assessment team identified two objectives that, if achieved, would indicate a successful compromise or data breach:

- Breach the security of the State of Colorado's network and gain access to personally identifiable, sensitive, and/or confidential information.

- Identify security weaknesses in systems or web applications that, if exploited, would provide an attacker with significant visibility, confidential data, or the ability to attack the site's users—Colorado's citizens and businesses.

To ensure adequate coverage of state systems, testing was discontinued on a network or system if both objectives were achieved. As such, not all vulnerabilities that exist within an application or network may have been discovered or validated as part of this engagement.

Penetration Test Results

Overall, the results of the penetration test demonstrate that the State is at high risk of a system compromise and/or data breach by malicious individuals, including individuals both internal and external to the State. We identified a significant number of serious vulnerabilities in the State's networks and applications that would likely provide a malicious attacker with unauthorized access to the public's data or with the ability to directly target Colorado's citizens. In the following sections, we provide summarized information about the number and types of vulnerabilities identified by the assessment team for each component of the State's information resources or architecture. This information provides a high-level overview of the State's current information security posture, including the risk of being compromised by a malicious individual.

We were able to compromise several state government networks and systems and gain unauthorized access to thousands of individuals' records, including state employees' records, containing confidential data such as social security numbers, income levels, birth dates, and contact information—i.e., phone numbers and physical addresses. We also compromised or gained access to usernames and passwords belonging to state employees and other individuals. Based on national averages, a data breach of this magnitude by a malicious individual would have cost the State between $7 and $15 million to remediate. This estimate does not include the cost to individual citizens whose data would have been stolen.

In assessing the threat to State systems, the assessment team utilized the U.S. Department of Homeland Security's National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) to rate the vulnerabilities identified during preliminary testing. Vulnerabilities are weaknesses in information systems, system security procedures, internal controls, or implementation that could be exploited or triggered by an attacker. Vulnerabilities listed in the NVD receive a CVSS score between 0 and 10, with 0 indicating a low-risk vulnerability and 10 indicating a high-risk vulnerability. For our purposes, we utilized the following scale to rate the vulnerabilities identified:

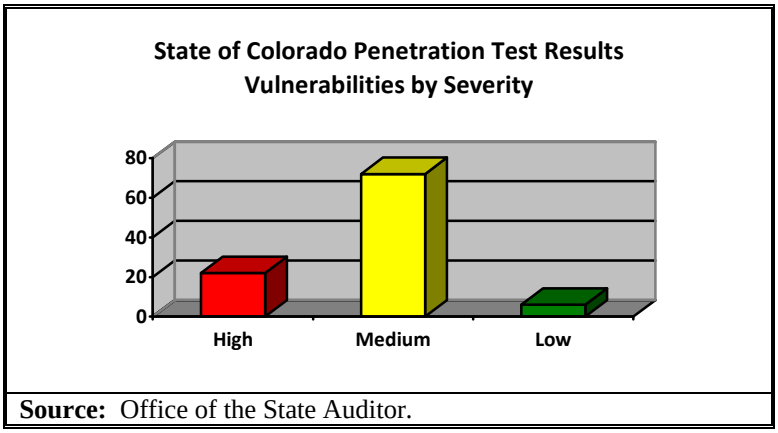
- **High.** High-risk vulnerabilities are considered to be severe security issues that can easily be exploited to immediately impact a system or network. Vulnerabilities with a CVSS base score of 7.0–10.0 are rated as "High." Additionally, regardless of the CVSS base score, the vulnerability was rated as "High" if it directly contributed to the assessment team's success in compromising confidential data.

- **Medium.** Medium-risk vulnerabilities are moderate security issues that require some effort to exploit to successfully impact a system or network. Vulnerabilities rated as "Medium" have a base CVSS score of 4.0–6.9.

- **Low.** Low-risk vulnerabilities have limited or marginal impact to systems and networks. Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0–3.9.

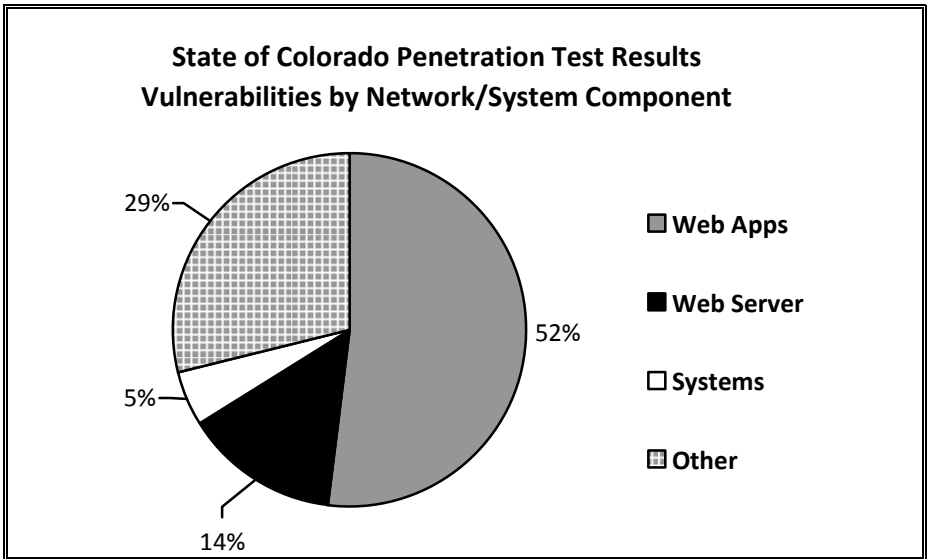
The NVD's listing of known vulnerabilities, including their CVSS base scores, can be found at http://web.nvd.nist.gov/view/vuln/search.

In total, we identified hundreds of vulnerabilities in state systems and networks. As shown in the following chart, of the total vulnerabilities identified 22 percent were high-risk, 72 percent were medium-risk, and 6 percent were low-risk vulnerabilities.



Source: Office of the State Auditor.

In addition to total vulnerabilities, we also analyzed which components of the State's information technology infrastructure contained the greatest percentage and severity of vulnerabilities. As seen in the following chart, 52 percent of all vulnerabilities were identified in web applications, with another 14 percent found in the servers hosting the web applications. This is important information because, as discussed in Chapter 1, most attackers are focused on exploiting web applications and servers, the areas of the State with the greatest number of vulnerabilities.



Source: Office of the State Auditor.

In the following table, we provide the risk ranking related to the specific components of the State's networks and systems tested. The risk ranking represents the likelihood that the confidentiality, integrity, and availability of State networks, systems, and information will be impacted based on known threats, identified vulnerabilities, and the effectiveness of the State's information system controls. As such, a risk ranking of "HIGH" means that it is extremely likely, based on current threats and system controls, that the confidentiality, integrity, and availability of the specified system component could be impacted. To protect the State, the details that led us to each risk ranking are provided to OIT, the Office of Cyber Security, and appropriate agencies in confidential appendices under separate cover.

State of Colorado Penetration Test Results Risk Ranking by Network/System Component		
Network/System Component Tested	**Description of Testing**	**Risk Ranking**
External Network Testing	Scanning the State's wide area network and publicly accessible IP addresses, or IP addresses associated with computers and other devices that are connected to and accessible through the Internet. Scanning results were then used to attempt to bypass security controls and gain unauthorized and privileged access to agency systems and internal networks.	HIGH
Physical Security Testing	Identifying and attempting to bypass physical security barriers or controls to gain access to the agency's internal network, computer hardware, or documents containing confidential information.	HIGH
Internal Network Testing	For those agencies at which the assessment team was able to bypass perimeter security controls—meaning controls within computer systems, such as firewalls, that are accessible through the Internet—or physical security controls, testing to identify and attempting to exploit systems located on the agencies' internal networks.	HIGH
Web Application Testing	Identifying all web applications exposed to the Internet, scanning identified web applications for vulnerabilities, and attempting to exploit those vulnerabilities, whether part of the web server or the application itself.	HIGH
Social Engineering	Attempting to obtain confidential information directly or to obtain information that can be used to further an attack. Testing included launching a directed "phishing" attack against state employees and other social engineering tactics.	HIGH
Modem Testing	A modem is a device that allows digital signals to be transmitted and received over analog telephone lines. Testing included "war dialing," which involves automatically dialing large blocks of phone numbers, in an attempt to find and exploit misconfigured dial-up modems.	LOW
Wireless Network Testing	A wireless network is a network that uses a wireless access point and radio waves for the transmission of data instead of network cables. Testing included identifying state-owned wireless networks and attempting to exploit the wireless access point and break the security encryption used to secure the radio transmissions.	LOW
Source: Office of the State Auditor penetration test results.		

Findings and Recommendations

In the next sections, we provide our high-level findings and recommendations that generally apply to all agencies and require a concerted and coordinated effort by the Office of Cyber Security. As stated earlier, the detailed technical findings and recommendations are being provided to OIT, the Office of Cyber Security, and appropriate agencies in confidential appendices under separate cover. The Office of the State Auditor will track OIT's, the Office of Cyber Security's, and agencies' implementation of the recommendations contained both in the public and confidential sections of this report.

The most significant vulnerabilities that allowed the assessment team to compromise state systems and networks and gain access to state data were:

- Management interfaces exposed to the Internet with default or easily guessable usernames and passwords enabled.
- Web applications, servers, and network devices accessible through the Internet with default or easily guessable usernames and passwords enabled. Many of these accounts provided the assessment team with privileged or administrative-level access to the system.
- Unnecessary ports, services, and utilities exposed to the Internet, including services with known and exploitable vulnerabilities.
- Unsecured or misconfigured web applications susceptible to SQL injection, remote file inclusion—an attack in which the attacker uploads inappropriate files onto a web server—and other well-known attacks.
- Poorly secured internal networks.
- Poor physical security that allowed testers to gain unlimited access to public agencies' internal networks and information assets.
- Lack of security awareness by employees, resulting in the successful execution of phishing attacks that allowed testers to harvest system credentials and access state systems and data.

Exposed Management Interfaces

Management or administrative interfaces to applications and network devices allow system administrators to perform privileged operations, such as adding or removing routes to other networks; reading, adding, or deleting databases; and

adding, removing, or modifying users. Oftentimes, the only barrier between an attacker and full access to an administrative interface is a username and password. Industry best practices recommend that access to administrative interfaces be limited to computers located on an entity's internal network. Access to management or administrative interfaces should not be directly accessible from the Internet because of the higher exposure to potential attacks.

During our testing, we found that the State has a significant number of administrative interfaces for firewalls, network devices, and web applications exposed directly to the Internet. This means that anyone with access to the Internet can attempt to gain access to these interfaces. In several cases, the assessment team was able to gain access to these interfaces by using vendor default usernames and passwords or by guessing the username and password. These techniques would have been impossible if the State followed industry best practices and limited access to management interfaces to only internal IP addresses. We make several recommendations to the Governor's Office of Information Technology below, including requiring the Office of Cyber Security to update State Cyber Security Policies to match industry best practices.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 5:

The Governor's Office of Information Technology should improve the security of the State's network and Internet-facing applications by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.

b. Identifying and inventorying all network devices and applications with management interfaces exposed to the Internet or other publicly accessible or insecure networks.

c. Working with agency staff to reconfigure the devices and applications with Internet-exposed management interfaces so that access to the interfaces can only be gained from inside the State's network. If this is not technically possible, then IP filtering should be added to the interface to limit those systems that can reach the service.

d. Revising State Cyber Security Policies to require that administrative interfaces not be directly accessible from the Internet.

e. Implementing firewall rules at the State gateway to filter incoming traffic bound for ports running administrative interfaces.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

Due to budget and resource constraints the exercise of reconfiguring devices and reprogramming software has not been as robust as the Office of Cyber Security (OCS) originally envisioned. In 2007, OCS initiated a project called the Web Application Scanning Project. The purpose of the project was to work with state agencies to reduce any unnecessary exposure of state systems on the Internet. OCS is planning a similar effort to begin in January 2011. Using the recent Office of the State Auditor (OSA) penetration test results with additional OCS activities, OCS will identify all state system exposures on the Internet and work with agency staff for business justification. Any exposure that does not have a legitimate agency business purpose will be removed either at the system, agency firewall, or state network level.

Once the State Internet footprint has been reduced to a baseline, the OCS Threat and Vulnerability Management Program (TVMP) will be utilized for the identification and management of new system exposures, vulnerabilities, and configuration weaknesses. It is an industry best practice to not expose system administrative interfaces on the Internet and this will be incorporated in the State Cyber Security Policies during the next OCS policy review and change process.

Default and Easily Guessable Usernames and Passwords

State Cyber Security Policies and industry best practices recommend the use of strong passwords. Specifically, State Cyber Security Policies require that passwords be at least eight characters in length and be complex, which means passwords should include a combination of lower and uppercase letters, numbers, and special characters. In addition to strong passwords, State Cyber Security Policies and industry best practices recommend changing vendor default usernames and passwords. These default usernames and passwords are well known by attackers and are readily available on the Internet.

Throughout our testing, we gained unauthorized access to systems and administrative interfaces by either guessing the correct username and password or by using vendor default credentials. Failure to use strong passwords or change vendor default passwords, especially for systems and applications accessible through the Internet, places the State at extreme risk of compromise. Several of the specific vulnerabilities we identified would have been discovered by the Office of Cyber Security or agency staff through routine vulnerability scans. However, we learned that the Office of Cyber Security and public agencies are not routinely performing vulnerability scans of state systems. Additionally, in one instance, a firewall we compromised had recently been moved into production without undergoing the OIT-approved hardening, or securing, process. If the state agency would have followed the hardening process required by State Cyber Security Policies, the default username and password the assessment team used to gain control of the firewall would have been disabled, removed, or changed. In the following recommendation, we provide several steps the Governor's Office of Information Technology should take to guard against the use of default and easily guessable usernames and passwords.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 6:

The Governor's Office of Information Technology should ensure that all state systems, especially those exposed to the Internet, use strong passwords and non-default usernames by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.

b. Performing routine vulnerability scans of state systems and networks.

c. Requiring that all new state systems and network devices undergo the OIT approved hardening, or securing, process using the Center for Internet Security benchmarks, which include the removal of default credentials from all hardware and software prior to being placed into production.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

Beginning in 2011, the Office of Cyber Security (OCS) will expand the Threat and Vulnerability Management Program (TVMP) by requiring

agency Information Security Officers (ISOs) to perform monthly vulnerability scans within each agency environment. Pending budget approval, OCS will procure vulnerability scanning software for each of the consolidated Executive Branch agencies. OCS will provide training, standardized scanning policies, vulnerability tracking tools, and monthly reporting requirements for ISO's dedicated to each agency. Phase I of this effort will focus on mitigating high-rated vulnerabilities within each agency. Phase II of this effort will focus on the continuous management of high-rated vulnerabilities and the initiation of mitigating medium-rated vulnerabilities. Phase III will focus on the continuous monitoring and management of all vulnerabilities within each agency environment. Management of the identified vulnerabilities from the Office of the State Auditor (OSA) penetration test effort will be managed through this process.

OCS has been working with the Chief Technology Officer's office with adopting, implementing, and socializing the use of the Center for Internet Security (CIS) hardening practices as the state security standard for all state systems, applications, and network devices. OCS will utilize the TVMP efforts as an assurance program to validate that the CIS standards are being met and maintained throughout the system development life cycle of each state system.

Unnecessary and Insecure Ports, Services, and Utilities

Ports provide a gateway to services and utilities that are running on a server. State Cyber Security Policies, industry best practices, and the Center for Internet Security hardening standards specify that only those ports, services, and utilities necessary to conduct business should be open and running. Unneeded ports, services, and utilities provide an unnecessary avenue for attackers to exploit and should be closed or disabled. Additionally, some ports and services are known to be insecure. Whenever possible, insecure services and utilities should be discontinued and replaced with secure ones.

From our testing, we found that the State has a large Internet presence, including more than 17,600 active IP addresses. Of these, we identified numerous IP addresses that appeared to be unused and that had ports open that were running unneeded and outdated services. Additionally, we identified a file upload utility on one agency's web server that allowed us to upload malicious code and take full control of the server. It was later determined that the file upload utility was unnecessary and should have been removed. As part of our assessment, we also found that many of the State's servers are running vulnerable services that provide

attackers an opportunity for exploitation. During our assessment, it also became clear that the Office of Cyber Security did not have an accurate inventory of all state systems requiring public Internet access, including a list of the ports, services, utilities, and access rules required for each system. Without an accurate inventory, the Office of Cyber Security cannot take the appropriate steps necessary to limit the State's exposure to Internet-based attacks. Additionally, many of the systems and applications we exploited either did not have a functioning firewall in place or had a firewall that was not being monitored by agency staff. The lack of a monitored firewall allowed the assessment team to continuously attack and exploit Internet-facing systems without being detected.

We have provided the specific details of the vulnerabilities we identified to the Office of Cyber Security in the confidential appendices. The Governor's Office of Information Technology should take immediate steps to reduce the State's exposure to attack, including reducing the State's overall Internet footprint. We provide additional recommendations below.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 7:

The Governor's Office of Information Technology should reduce the State's exposure to attacks against unnecessary and insecure ports, services, and utilities by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.

b. Reducing the overall Internet footprint of the State through the consolidation of servers and identification and removal of unneeded IP addresses and systems.

c. Limiting the number of ingress and egress points to the State Wide Area Network and to agency-specific networks.

d. Inventorying all systems and applications (assets) that require public Internet access.

e. Defining the appropriate access rules for each inventoried asset.

f. Ensuring that all assets are protected by a monitored firewall.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

Reducing the overall Internet footprint by reducing servers and consolidating applications is the primary goal of consolidation and is complex and will take resources and some time to complete. The State's wide area network was re-bid this summer and is now known as the Colorado State Network (CSN). This new network will enable the Office of Cyber Security (OCS) to provide more secure ingress and egress points as well as improve monitoring. Additionally, through consolidation, OCS is working with the Governor's Office of Information Technology (OIT) to develop a comprehensive list of all state systems and applications, including those exposed to the Internet. OCS will ensure that proper access rules protect these systems through the vulnerability scans and remediation activities discussed next. Beginning in 2011, OCS will expand the Threat and Vulnerability Management Program (TVMP) by requiring agency Information Security Officers (ISOs) to perform monthly vulnerability scans within each agency environment. Pending budget approval, OCS will procure vulnerability scanning software for each of the consolidated Executive Branch agencies. OCS will provide training, standardized scanning policies, vulnerability tracking tools, and monthly reporting requirements for ISOs dedicated to each agency. Phase I of this effort will focus on mitigating high-rated vulnerabilities within each agency. Phase II of this effort will focus on the continuous management of high-rated vulnerabilities and the initiation of mitigating medium-rated vulnerabilities. Phase III will focus on the continuous monitoring and management of all vulnerabilities within each agency environment. Data collected through this effort will be consolidated for a root cause analysis (i.e., configuration management, patch management, access controls, etc.) and used to target agencies' limited resources (people, time, budget) and future OIT strategic planning. Where budget and resources permit, OCS will also work with agencies to ensure that all critical state systems are protected with a firewall that includes appropriately defined ingress and egress rules.

Unsecured Web Applications

As previously discussed, web applications are becoming the primary target of malicious individuals. To ensure that web applications are attack-resilient, security controls must be implemented throughout each tier or layer of the

application's architecture, including the network within which the application resides, the server the application is running on, the application itself, and the database the application uses. Vulnerabilities or misconfigurations in any component of the application's architecture can result in a successful attack. Industry best practices recommend that web applications be secured by incorporating security within the design and initial build of the application, routinely testing applications for vulnerabilities, and using web application firewalls for the most critical applications.

As part of the penetration test, we identified hundreds of vulnerabilities in state web applications, including many severe vulnerabilities that led directly to the systems' compromise. In several situations, we were able to take control of the database the application was using to disclose usernames and passwords and citizen data. In many instances, we were also able to abuse the application's functionality to disclose usernames and bypass application controls to gain access to portions of the website normally restricted from the public. In one instance where we identified a state intranet application that was exposed to the Internet, we were able to exploit the site's poorly designed authentication mechanism to gain access to the site and download information that provided useful information for further attacks against the State. Finally, we found that system administrators do not appear to be routinely monitoring application-level logs. As part of our testing, we launched thousands of attacks against state web applications; many of these attacks would have generated tens of thousands of anomalous or suspicious log entries. Except for one agency, none of our attacks was reported to the Office of Cyber Security.

Securing the State's websites will be a large undertaking and will require, at times, the Office of Cyber Security to work with the vendors that originally developed the applications. We have provided the details of the specific deficiencies we identified to the Office of Cyber Security for remediation in the confidential appendices. Additionally, as discussed in the recommendation below, we recommend that the Governor's Office of Information Technology implement a web application security program that includes routine and pre-deployment testing, training, log monitoring, and the deployment of web application firewalls where appropriate.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 8:

The Governor's Office of Information Technology should ensure that state web applications are appropriately secured by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.

b. Training state application developers on the fundamentals of secure coding and application design.

c. Routinely testing all existing web applications both manually and with automated application security scanners and correcting the identified deficiencies.

d. Ensuring that all newly designed web applications, whether created by the state or a vendor, are tested manually and with automated scanners.

e. Requiring the Office of Cyber Security to validate that all web applications have been sufficiently tested and properly secured before being moved into production.

f. Protecting critical web applications with web application firewalls.

g. Ensuring IT staff are routinely reviewing and monitoring web application logs and reporting suspicious activity to appropriate staff.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2011.

The Office of Cyber Security (OCS) initiated an Application Security (AppSec) program in March 2010 to begin to handling the issues of weak web applications within the State of Colorado. Due to budgetary and human resource constraints (the AppSec program currently consists of one highly skilled security application expert), the AppSec has had limited but effective success through the offering of several application security classes to state developers, reviewing and providing guidance on application security requirements for several key state projects, creating a communication mechanism to assist developers with mitigation strategies to close security holes in state web applications, aiding in the implementation of several web application firewalls for critical state applications, and developing application security checklists to be used by developers to check the security of their applications. Testing of applications will be performed through the OCS Threat & Vulnerability Management Program (TVMP) and all identified issues will be mitigated through the AppSec program and tracked to resolution using the OCS Colorado Risk, Incident, & Security Compliance tool. Where budget and

resources permit, OCS will assist agencies in testing all new critical and major rated web applications prior to moving the applications into production and will continue providing assistance in the implementation and configuration of web application firewalls.

Guidance on the detection of anomalous and malicious activity against state web applications will be created by the AppSec program and will be integrated into the OCS detection and monitoring program where budget allows for the expansion of the centralized OCS centralized logging system.

Internal Network Security

An agency's internal network is the portion of its network that is considered private and not accessible to the general public. The internal network typically includes user computers and applications, internal network shares, and the servers and databases that support the agency's operations. State Cyber Security Policies and industry best practices recommend a layered or defense-in-depth approach to security. A layered defensive approach means that security controls will be included or built in each layer of the agency's infrastructure, including the internal network. Common security controls include network segmentation, internal system hardening, use of secure network protocols, and intrusion detection.

Once the assessment team gained access to an agency's internal network, the team identified problems in each of these areas, including:

- **Network segmentation.** Network segmentation is the process of dividing a network into different segments or zones based upon access and security requirements of the systems in those zones. Agency internal networks were generally flat, meaning all computers and servers were included within the same network. This made it easy for the assessment team to directly reach all internal computer assets, including sensitive servers and databases. Furthermore, the assessment team found that access to administrative interfaces and utilities on internal servers was not filtered. As such, the team was able to gain administrative access to firewalls and databases as a common user.

- **System hardening.** System hardening includes removing or changing all guest accounts and default passwords, disabling nonessential services, setting system parameters to mitigate potential attacks, and patching systems from known vulnerabilities. We identified numerous systems that were not properly hardened and patched. For example, we gained

administrative access to one system within an agency's internal network by exploiting a well-known operating system vulnerability that has had an available patch since 2008. This specific vulnerability is targeted by one of the most damaging Internet worms in history.

- **Insecure network protocols.** Many common network protocols transmit information between computers in cleartext, such as the Hypertext Transfer Protocol (HTTP). Although appropriate for some uses, these types of protocols should not be used to transmit sensitive information, such as usernames and passwords. The assessment team was able to sniff, or monitor network traffic, once internal access was gained. Through network monitoring, the assessment team was able to capture usernames and passwords and default strings for network devices and internal applications, many of which contained sensitive information about state employees.

- **Intrusion detection.** With the exception of one agency, our internal testing was not detected by system administrators. From prior audit engagements and our interviews with information security officers, we determined that most public agencies lack an internal intrusion detection capability.

Failure to properly secure the internal network makes it more likely that attackers will gain access to confidential or sensitive data if external controls are bypassed or fail. We recommend that the Governor's Office of Information Technology work with public agencies to further harden or secure their internal networks by taking the steps listed below.

(Classification of Finding: Material Weakness – See Appendix A)

Recommendation No. 9:

The Governor's Office of Information Technology should improve the security of public agencies' internal networks by:

a. Ensuring that the specific deficiencies identified in the confidential appendices provided under separate cover are immediately addressed.

b. Architecting internal networks so that they are "segmented," or broken into different zones based upon the access and security requirements of the systems in those zones. In particular, OIT and agencies should isolate servers and databases where sensitive data may be stored and limit the

systems which can access them and the protocols that are allowed based on business needs.

c. Requiring information security officers to routinely perform automated vulnerability scans of internal networks to identify and remediate vulnerabilities.

d. Working with agency IT staff to ensure that proper hardening and patch management practices are being followed.

e. Providing guidance to IT staff and agency IT directors on the development and implementation of proper network segmentation.

f. Requiring that agencies utilize secure protocols when transmitting sensitive information to prevent someone who gains access to the internal network from being able to "sniff," or capture usernames and passwords.

g. Implementing intrusion detection capabilities within internal networks where feasible.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2013.

Many of the state internal networks were created before the Office of Cyber Security (OCS) policy requirements stating that "all sensitive data is to be stored and processed on a LAN segment that is separated from end users through the use of a firewall or other access control mechanism" as well as that "security protocols are [to be] used to protect user login information to State systems." Through consolidation, the Office of Information Technology (OIT) has inherited these State networks that do not comply with these security requirements. Mitigating these problems will require significant budget and human resources. Through the data center consolidation effort, agency server systems will be segmented from the agency end user workstation environments and provide some of the compliance mechanisms for this policy requirement. OCS will also be working with the Chief Technology Officer's office to develop guidance for agencies on proper network segmentation practices.

OCS will be requiring monthly vulnerability scanning in agencies which will assist in the identification of all unsecure protocol issues. These issues will be managed through the OCS Colorado Risk, Incident, & Security Compliance (CRISC) tool. OCS will ensure that proper patching

and hardening practices are implemented within each agency through the Information Security Officers (ISO) annual self-assessments and through monthly scanning. Where budget and resources permit, OCS will assist agencies in the implementation and monitoring of internal intrusion detection systems.

Poor Physical Security Over Information Systems

Due to the sensitive nature of the information contained within this finding, it is reported in the confidential appendices provided under separate cover.

(Classification of Finding: Material Weakness – See Appendix A)

Lack of Employee Security Awareness

Due to the sensitive nature of the information contained within this finding, it is reported in the confidential appendices provided under separate cover.

(Classification of Finding: Material Weakness – See Appendix A)

This page intentionally left blank.

Appendix

This page intentionally left blank.

Public Appendix A

Report Findings by Classification of Finding

Definition of Finding Classifications	
Classification	**Description**
Material Weakness	A material weakness produces an immediate risk directly impacting the confidentiality, integrity, and availability of information systems and data. For IT projects, a material weakness represents an immediate threat to the overall success of the project. This would be considered a high risk finding.
Significant Deficiency	Significant deficiencies do not alone produce an immediate risk, but could affect the confidentiality, integrity, or availability of systems in conjunction with other factors. For IT projects, significant deficiencies do not represent an immediate threat to the overall success of the project but could result in project delays, cost overruns, or incomplete deliverables. This would be considered a moderate risk finding.
Control Deficiency	Control deficiencies do not present an immediate risk but could be indicative of operating deficiencies and/or have the potential to adversely affect the confidentiality, integrity, or availability of systems over an extended period of time. For IT projects, control deficiencies may not represent an immediate threat to the overall success of the project but could, over an extended period of time and in conjunction with other deficiencies, result in project delays, cost overruns, or incomplete deliverables. This would be considered a low risk finding.

Rec. No.	Page No.	Audit Finding	Classification of Findings		
			Material Weakness	Sig. Deficiency	Control Deficiency
1	31	Re-evaluate and improve the Agency Cyber Security Plan development, submission, and review process.	X		
2	37	Improve the State's cyber security incident identification, reporting, and response processes and procedures.	X		
3	42	Implement and comply with all statutory requirements of the Colorado Cyber Security Program.	X		
4	45	Develop a strategic plan for the Office of Cyber Security, hold cyber security leadership accountable, and increase the Governor's Office of Information Technology's oversight of the Colorado Cyber Security Program.	X		
5	54	Secure exposed management interfaces.	X		
6	56	Ensure that all state systems are using strong passwords and that vendor default usernames and passwords are changed.	X		
7	58	Inventory all Internet-facing systems and close and/or disable all unnecessary and insecure ports, services, and utilities.	X		
8	60	Secure state web applications.	X		
9	63	Improve the security of public agencies' internal networks.	X		
CONFIDENTIAL RECOMMENDATIONS					
1	N/A	Poor Physical Security Over Information Systems	X		
2	N/A	Lack of Employee Security Awareness	X		

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

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

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

Report Control Number 2068A

Report Control Number 2068A

ATTACHMENT D

An audit of questionable spending by a state agency, along with resulting recommendations, is an example of good government.

By The Denver Post Editorial Board The Denver Post
Posted:

DenverPost.com

Oh, those zany boys and girls over at the Statewide Internet Portal Authority — whatever will they think of next in terms of breaking the mold for footloose expense controls?

You hadn't heard of SIPE? You're forgiven, although it happens that this obscure subdivision of the state does important work — including managing the Colorado.gov internet portal and providing e-government services to scores of entities. Not only is the work highly skilled, it grows more vital all the time because of society's reliance on the Internet for all types of transactions.

But SIPE is also a small outfit — only three full-time employees and a part-time contract accountant — and maybe its intimate size cultivated a bit of an "on-your-honor" system in terms of some procedures. Or at least that's what it sounds like based upon a report released recently by the state auditor.

The auditor found, for example, that "between July 2010 and April 2012, the executive director made about 480 credit card expenses totaling about $69,400" — that would appear to be nearly one per day after subtracting for weekends and time off — and yet that individual "approves his own credit card statements for payment."

Now that's convenient. Any bets on how easily those expenses sailed through approval?

The auditor, who has this green-eyeshades-type belief that solid financial controls are a key to good management, also took a dim view of SIPE's cavalier attitude toward record-keeping involving these sorts of expenses — and not just by the executive director.

Indeed, "during our review of ... 176 expenses we became aware that SIPA does not require staff to retain receipts to support credit card expenses." The auditor nevertheless was able to identify "272 SIPA expenses totaling about $13,700 ... including meals, travel and miscellaneous expenses for which we question either the reasonableness or necessity of the expense or both."

Why? "First, we question the business purpose of frequent, small purchases at places like Starbucks or 7-Eleven. Second, we question the high cost and business purpose of meals at restaurants such as Earl's, Panzano and The Broker, for which SIPA did not maintain documentation of the individuals attending the meal or the business purpose of the meal."

The audit also highlighted security issues involving the protection of data and and lack of a risk-management plan. And it offered a number of recommendations, most of which SIPE has accepted for implementation throughout 2013. So this is a story with a happy ending.

The office of state auditor is not always appreciated as the bulwark to good government that it clearly is. Yet its performance audits routinely uncover questionable practices that might otherwise have gone on for years — such as the "on-your-honor" system at SIPE.

ATTACHMENT E

Colorado Office of the State Auditor
Audit-Related Legislation
2009-2012 Legislative Sessions

The following bills were enacted by the Colorado General Assembly and signed into law related to recommendations made or studies conducted by the OSA.

2012

SB 12-012 Department of Revenue Audits of Auto Emission Test Centers
SB 12-034 Repeal Rapid Screen for High-Emitting Vehicles
HB 12-1074 Judicial Oversight of Guardians and Conservators

2011

SB 11-002 Low-Income Telephone Assistance Program
SB 11-082 OSA Security Audits IT Systems

2010

SB 10-087 Secretary of State Authority to Regulate Lobbyists
SB 10-118 Child Care Assistance Program Fingerprint-Based Criminal History Checks
SB 10-186 State Warrants for Tax Refunds
HB 10-1003 State Personnel Board Appeal Deadline
HB 10-1011 Department of Revenue Fingerprint-Based Criminal History Checks
HB 10-1060 Penalty for Failing to Withhold Severance Tax

2009

SB 09-048 Elimination of Office of Child's Representative Audit
SB 09-065 Elimination of Public Safety Communications Trust Fund Audit
SB 09-066 Consolidation of Public Employee Retirement Plans
SB 09-111 Enforcement of the Notaries Public Act
SB 09-135 Requirements for Parole Decision Reporting and Statistics
HB 09-1002 Changes in State Lottery Operations
HB 09-1024 Modifications to the Local Government Audit Law
HB 09-1053 Repeal of the Colorado Foreign Capital Depository Act
HB 09-1066 Changes in Duties of the Division of Aeronautics
HB 09-1103 Authority to Seek Federal Authorization for Presumptive Eligibility for Medicaid Long-Term Care
HB 09-1229 Changes in Requirements for Higher Education Enterprise Designations

ATTACHMENT F

Responses to Performance Audit Recommendations Calendar Years 2009–2012				
Department/Agency	**Number of Recommendations**			
	Agree	**Partially Agree**	**Disagree**	**Total**
Agriculture	18			18
Corrections	1			1
Governor's Office	112	3		115
Health Care Policy & Financing	43	2		45
Higher Education	63	22	2	87
Human Services	108	5		113
Independent Ethics Commission	2	1		3
Judicial	31	1		32
Labor & Employment	53	7		60
Law	4		1	5
Local Affairs	19			19
Natural Resources	42			42
Office of the Colorado State Public Defender	3			3
Office of the Child's Representative	2			2
Personnel & Administration	121			121
Pinnacol Assurance (Workers' Compensation Fund)	24	4		28
Public Health & Environment	28	2	1	31
Public Safety	15	2		17
Regional Transportation District	39	1	1	41
Regulatory Agencies	51	4		55
Revenue	32	4		36
State	2		1	3
Statewide Internet Portal Authority	25	1	1	27
Transportation	106	12		118
Treasury	8	1		9
Total	**952**	**72**	**7**	**1,031**
Percent of Total	**92%**	**7%**	**1%**	**100%**
Source: Office of the State Auditor's recommendation database.				

Recommendations from Performance Audits Released During Calendar Years 2009–2012 Implementation Status as of June 30, 2012		
Implementation Status	**Count**	**Percent of Total**
Implemented	704	68%
Partially Implemented	106	10%
Not Implemented	197	19%
Not Applicable[1]	24	3%
Total	**1,031**	**100%**

Source: Office of the State Auditor's recommendation database.

[1]Not applicable is used when the agency either disagreed with the original audit recommendation, or the program or other factors have changed such that implementation of the recommendation as it was originally written is no longer applicable.

Recommendations Not Implemented by Audit Report Release Date		
Release Date	**Count**	**Percent of Total**
Calendar Year 2009	10	5%
Calendar Year 2010	9	5%
Calendar Year 2011	5	2%
Calendar Year 2012	173	88%
Total	**197**	**100%**

Source: Office of the State Auditor's recommendation database.

ATTACHMENT G

Colorado Office of the State Auditor
External Presentations
2009-2012

2012

- NCSL Legislative Summit (Chicago, IL)
  "Fielding Audit Requests"
  Greg Fugate, Audit Manager

- NLPES Fall Professional Development Seminar (Atlanta, GA)
  "Audit Planning for Lean Government"
  Greg Fugate, Audit Manager

- NLPES Fall Professional Development Seminar (Atlanta, GA)
  "QC Practices: Perspectives from a Yellow Book State"
  Greg Fugate, Audit Manager

- NLPES Fall Professional Development Seminar (Atlanta, GA)
  "Dealing With Difficult Auditees Suspected of Fraud"
  Jenny Page, Audit Manager

- Mountain & Plains Intergovernmental Audit Forum (Atlanta, GA)
  "From Audit to Audience: Publicizing Your Audit Results"
  Monica Bowers, Deputy State Auditor
  Jenny Atchley, Communication Analyst

- Institute of Internal Auditors, Denver Chapter (Denver, CO)
  "Adding Value Through Performance Audit Techniques"
  Dianne Ray, State Auditor
  Monica Bowers, Deputy State Auditor

- Institute of Internal Auditors, Denver Chapter (Denver, CO)
  "Government Auditors Roundtable Panel"
  Monica Bowers, Deputy State Auditor

2011

- NLPES Fall Professional Development Seminar (Denver, CO)
  Plenary Session
  "Report Messaging: Telling the Story Behind the Numbers"
  Jenny Atchley, Communication Analyst
  Greg Fugate, Audit Manager

- NLPES Fall Professional Development Seminar (Denver, CO)
  "Higher Education Student Fees"
  Eric Johnson, Audit Manager

- NLPES Fall Professional Development Seminar (Denver, CO)
  "Problem Drivers and Traffic Fatalities"
  Trey Standley, Audit Supervisor

- NLPES Fall Professional Development Seminar (Denver, CO)
  "Weatherization Assistance Program"
  Sarah Aurich, Audit Manager

- NLPES Fall Professional Development Seminar (Denver, CO)
  "Low-Income Telephone Assistance Program"
  Jacob Wager, Audit Supervisor

- American Association of State Highway and Transportation Officials Audit Conference (Denver, CO)
  "Developing a Focused Audit Scope"
  Monica Bowers, Audit Manager
  Sarah Aurich, Audit Manager
  Jenny Page, Audit Manager

2010

- NLPES Fall Professional Development Seminar (Baton Rouge, LA)
  "Performance Audits of the Colorado Lottery"
  Greg Fugate, Audit Manager

- NLPES Fall Professional Development Seminar (Baton Rouge, LA)
  "Auditing American Recovery and Reinvestment Act (ARRA) Programs"
  Sarah Aurich, Audit Manager

- Mountain & Plains Intergovernmental Audit Forum (Denver CO)
  "A Strategic Vision for Smaller, More Focused Performance Audits"
  Cindi Stetson, Deputy State Auditor
  Sarah Aurich, Audit Manager
  Michelle Colin, Audit Manager
  Greg Fugate, Audit Manager
  Eric Johnson, Audit Manager

2009

- NCSL Legislative Summit, Legislative Health Staff Network Preconference (Philadelphia, PA)
  "Medicaid Oversight: Colorado's Approach"
  Cindi Stetson, Deputy State Auditor

Thank you for attending the 2011 NLPES Professional Development Seminar!

Please complete an evaluation form and leave it at the registration table.

2011-2012 NLPES Executive Committee

Dale Carlson, California

Greg Fugate, Colorado

Patrick Goldsmith, Louisiana

Wayne Kidd, Utah

Lisa Kieffer, Georgia
Secretary

Marcia Lindsay, South Carolina

Angus Maciver, Montana

Kathy McGuire, Florida
Immediate Past Chair

Tricia Oftana, Hawaii

Carol Ripple, North Carolina

Scott Sager, Wisconsin
Chair

Karl Spock, Texas
Vice-Chair

Bob Boerner
NLPES Staff Liaison
National Conference of State Legislatures

Colorado 2011

NLPES Professional Development Seminar

September 19-21, 2011

Magnolia Hotel
Denver, Colorado

Sponsored by the National Legislative Program Evaluation Society
Hosted by the Colorado Office of the State Auditor

NATIONAL CONFERENCE *of* STATE LEGISLATURES
The Forum for America's Ideas

Monday, September 19

Registration 8:00 a.m.—5:00 p.m.
Magnolia Hotel, Lower Level

Plenary Session 8:00 a.m.—Noon
Pew's Results First Project
Magnolia Ballroom
(across 17th Street from main hotel building)

Moderator:
- **Gary VanLandingham**, Director, Results First, Pew Center on the States

Speakers:
- **Gary VanLandingham**, Director, Results First, Pew Center on the States
- **Michael Wilson**, Economist/Statistical Analysis Center Director, Oregon Criminal Justice Commission
- **Elizabeth Drake**, Senior Research Associate, Washington State Institute for Public Policy

Support for the Results First Project was provided in part by The Pew Charitable Trusts.

Lunch (on your own) Noon—1:00 p.m.

Breakout Sessions 1:15 p.m.—3:00 p.m.
Higher Education: Cracking the Ivory Tower
Magnolia Ballroom
(across 17th Street from main hotel building)

Moderator:
- **Patrick Goldsmith**, Assistant Legislative Auditor and Director of Performance Audit and Actuarial Services, Louisiana Office of the Legislative Auditor

Speakers:
- **Dale Carlson**, Senior Auditor/Evaluator III, California Bureau of State Audits
- **Eric Johnson**, Audit Manager, Colorado Office of the State Auditor
- **Charles Sallee**, Deputy Director, New Mexico Legislative Finance Committee

Motor Vehicles: $trategies to Improve $afety
Larimer/Champa Rooms

Moderator:
- **Lisa Kieffer**, Deputy Director, Performance Audit Operations, Georgia Department of Audits and Accounts

Speakers:
- **Trey Standley**, Audit Supervisor, Colorado Office of the State Auditor
- **Nneka Norman-Gordon**, Legislative Research Analyst II, Tennessee Offices of Research and Education Accountability
- **Dot Reinhard**, Performance Audit Manager, Arizona Office of the Auditor General
- **Shunti Taylor**, Audit Supervisor, Georgia Department of Audits and Accounts

Wednesday, September 21

Registration 8:00 a.m.—11:30 a.m.
Magnolia Hotel, Lower Level

Breakout Sessions 8:00 a.m.—10:00 a.m.
Medicaid: Auditing the Elephant in the Room
Magnolia Ballroom
(across 17th Street from main hotel building)

Moderator:
- **Tim Osterstock**, Audit Manager, Utah Office of the Legislative Auditor General

Speakers:
- **Karen LeBlanc**, Audit Manager, Louisiana Office of the Legislative Auditor
- **Maria Griego**, Program Evaluator, New Mexico Legislative Finance Committee
- **Eric Douglass**, Auditor, South Carolina Legislative Audit Council
- **John Bowden**, Research Analyst, Washington Joint Legislative Audit and Review Committee
- **Tim Osterstock**, Audit Manager, Utah Office of the Legislative Auditor General

State Employee Benefits: From Health Programs to Retirement
Larimer/Champa Rooms

Moderator:
- **Wayne Kidd**, Audit Supervisor, Utah Office of the Legislative Auditor General

Speakers:
- **Wayne Kidd**, Audit Supervisor, Utah Office of the Legislative Auditor General
- **Ross Johnson**, Performance Auditor, Montana Office of the Legislative Auditor
- **Kiernan McGorty**, Senior Program Evaluator, Performance Evaluation Division, North Carolina General Assembly
- **Matthew Holmes**, Evaluator, Mississippi Performance Evaluation and Expenditure Review Committee

Roundtable Session 10:15 a.m.—11:30 a.m.
Evaluating Evaluators
Larimer/Champa Rooms

Moderators:
- **Tricia Oftana**, Senior Analyst, Hawaii Office of the Auditor
- **Kiernan McGorty**, Senior Program Evaluator, Program Evaluation Division, North Carolina General Assembly

Optional Networking Activities 11:30 a.m. until . . .
(see registration table for details)

Monday, September 19

Breakout Sessions 3:15 p.m.—5:00 p.m.

Taxation: There's No Escaping It!
Magnolia Ballroom
(across 17th Street from main hotel building)

Moderator:
- **Kathy McGuire**, Deputy Coordinator, Florida Office of Program Policy Analysis and Government Accountability

Speakers:
- **John Sylvia**, Director, Performance Evaluation and Research Division, West Virginia Legislative Auditor's Office
- **Nathalie Molliet-Ribet**, Division Chief, Virginia Joint Legislative Audit and Review Commission
- **Kathy McGuire**, Deputy Coordinator, Florida Office of Program Policy Analysis and Government Accountability
- **Maryann Nardone**, Project Manager, Pennsylvania Legislative Budget and Finance Committee

Under and Over the Land: Familiar and Emerging Natural Resource Issues in the States
Larimer/Champa Rooms

Moderator:
- **Angus Maciver**, Performance Audit Manager, Montana Office of the Legislative Auditor

Speakers:
- **Sean Hamel**, Program Evaluator, Program Evaluation Division, North Carolina General Assembly
- **Will Soller**, Senior Performance Auditor, Montana Office of the Legislative Auditor
- **Gerald Hoppmann**, Program Evaluation Section Manager, Wyoming Legislative Service Office
- **Darin Underwood**, Audit Manager, Utah Office of the Legislative Auditor General

Evening Reception 5:00 p.m.—6:00 p.m.

Magnolia Ballroom
(across 17th Street from main hotel building)

Reception Co-sponsored by:

National Legislative Program Evaluation Society (NLPES)
and
National Legislative Services and Security Association (NLSSA)

Tuesday, September 20

Breakout Sessions 3:15 p.m.—5:00 p.m.

Housing Assistance Programs: Administration, Eligibility, and Unintended Consequences
Stout Room

Moderator:
- **Patrick Goldsmith**, Assistant Legislative Auditor and Director of Performance Audit and Actuarial Services, Louisiana Office of the Legislative Auditor

Speakers:
- **Sarah Aurich**, Audit Manager, Colorado Office of the State Auditor
- **Jacob Wager**, Audit Supervisor, Colorado Office of the State Auditor
- **Michelle Downie**, Policy Analyst, Texas Sunset Commission

Corrections: Improvements Needed From Coast to Coast
Larimer/Champa Rooms

Moderator:
- **Dale Carlson**, Senior Auditor/Evaluator III, California Bureau of State Audits

Speakers:
- **Scott Farwell**, Legislative Analyst, Maine Office of Program Evaluation and Government Accountability
- **Jan Yamane**, Deputy Auditor and General Counsel, Hawaii Office of the Auditor
- **Tammy Lozano**, Senior Auditor/Evaluator III, California Bureau of State Audits
- **Amy Lorenzo**, Principal Evaluator, Idaho Office of Performance Evaluations

Optional Networking Activities 5:00 p.m. until . . .

(see registration table for details)

Fall Colors in Colorado's High Country
Independence Pass

Tuesday, September 20

Registration 8:00 a.m.—5:00 p.m.
Magnolia Hotel, Lower Level

Plenary Session 8:00 a.m.—9:45 a.m.
Magnolia Ballroom
(across 17th Street from main hotel building)

Welcome and NLPES Chair's Update

Speaker:
- **Scott Sager**, Program Evaluation Supervisor, Wisconsin Legislative Audit Bureau

Report Messaging: Telling the Story Behind the Numbers

Moderator:
- **Greg Fugate**, Audit Manager, Colorado Office of the State Auditor

Speaker:
- **Jenny Atchley**, Communication Analyst, Colorado Office of the State Auditor

Breakout Sessions 10:00 a.m.—11:30 a.m.
Strategic Planning in Audit and Evaluation Offices: the How and Why of Contrasting Strategies
Stout Room

Moderator:
- **Karl Spock**, Senior Manager, Texas Sunset Commission

Speakers:
- **Wendy Cherubini**, Senior Analyst, Maine Office of Program Evaluation and Government Accountability
- **Kelly Kennedy**, Policy Analyst, Texas Sunset Commission

Making the Grade: Evaluating Education Programs
Larimer/Champa Rooms

Moderator:
- **Tricia Oftana**, Senior Analyst, Hawaii Office of the Auditor

Speakers:
- **Katja Vermehren**, Associate Program Evaluator, Wyoming Legislative Service Office
- **Allison LaTarte**, Senior Legislative Analyst, Wisconsin Legislative Audit Bureau
- **Nicole Edmonson**, Performance Audit Manager, Louisiana Office of the Legislative Auditor

Tuesday, September 20

NLPES Luncheon 11:30 a.m.—1:00 p.m.
Magnolia Ballroom
(across 17th Street from main hotel building)

Speakers:
- **Dianne Ray**, Colorado State Auditor
- **William T. Pound**, Executive Director, National Conference of State Legislatures
- **Michael Adams**, Staff Chair, National Conference of State Legislatures

Awards:
- Certificates of Impact
- Excellence in Research Methods
- Excellence in Evaluation
- Outstanding Achievement

Breakout Sessions 1:15 p.m.—3:00 p.m.
Oversight of Social Services: Balancing Independence and Accountability
Stout Room

Moderator:
- **Scott Sager**, Program Evaluation Supervisor, Wisconsin Legislative Audit Bureau

Speakers:
- **Amy Lorenzo**, Principal Evaluator, Idaho Office of Performance Evaluations
- **Pam Galbraith**, Program Evaluator, New Mexico Legislative Finance Committee
- **Kathy McGuire**, Deputy Coordinator, Florida Office of Program Policy Analysis and Government Accountability
- **Scott Sager**, Program Evaluation Supervisor, Wisconsin Legislative Audit Bureau

Workforce Investment, Unemployment Insurance, and Workers' Compensation: Getting America Back to Work
Larimer/Champa Rooms

Moderator:
- **Marcia Lindsay**, Audit Manager, South Carolina Legislative Audit Council

Speakers:
- **Linda Triplett**, Quality Assurance Manager, Mississippi Performance Evaluation and Expenditure Review Committee
- **Emily Wilson**, Performance Audit Manager, Louisiana Office of the Legislative Auditor
- **Michelle Garcia**, Associate Program Evaluator, Wyoming Legislative Service Office
- **Marcia Lindsay**, Audit Manager, South Carolina Legislative Audit Council