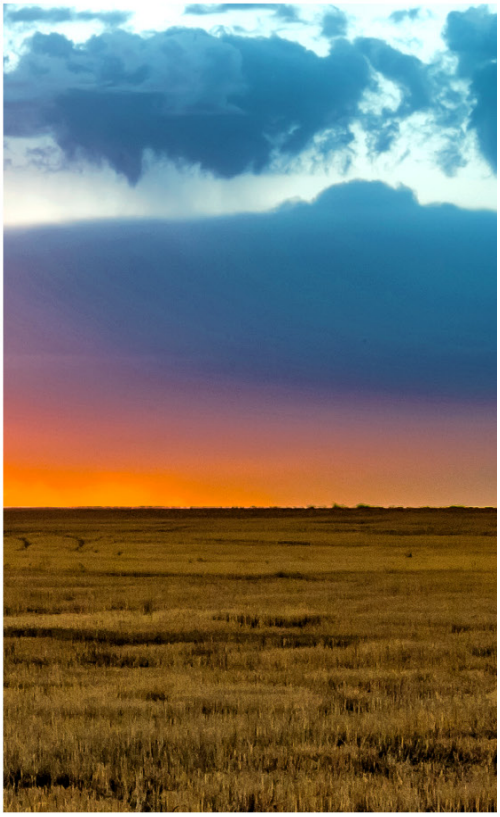
COLORADO
OFFICE OF THE
STATE AUDITOR

We Set the Standard for Good Government

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

SYSTEMS BACKUP AND RECOVERY





OCTOBER 2014

IT PERFORMANCE AUDIT

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

LEGISLATIVE AUDIT COMMITTEE

Senator Lucia Guzman - Chair

Senator David Balmer
Senator Kevin Grantham
Representative Dan Nordberg
Representative Dianne Primavera
Representative Su Ryden
Representative Jerry Sonnenberg
Senator Lois Tochtrop

OFFICE OF THE STATE AUDITOR

Dianne E. Ray	State Auditor
Matt Devlin	Deputy State Auditor
Bryan Becker	Team Leader
Reed Larsen	Staff Auditors
Larry Ciacio	
Kiran Keshav	

AN ELECTRONIC VERSION OF THIS REPORT IS AVAILABLE AT
WWW.STATE.CO.US/AUDITOR

A BOUND REPORT MAY BE OBTAINED BY CALLING THE
OFFICE OF THE STATE AUDITOR
303.869.2800

PLEASE REFER TO REPORT NUMBER 1403P WHEN REQUESTING THIS REPORT

OFFICE
OF THE STATE AUDITOR

DIANNE E. RAY, CPA
STATE AUDITOR

October 15, 2014

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of system backup and recovery processes 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 report presents our findings, conclusions, and recommendations, and the responses of the Governor's Office of Information Technology.

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

303 869 2800

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

CONTENTS

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

REPORT HIGHLIGHTS

BACKUP AND RECOVERY
PERFORMANCE AUDIT, OCTOBER 2014

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

CONCERN
The Governor's Office of Information Technology needs to improve governance over system backup and recovery processes within the Executive Branch.

KEY FACTS AND FINDINGS

- The Governor's Office of Technology (OIT) is responsible for oversight and governance of backup and recovery processes for seventeen Executive Branch agencies.
- The Colorado Information Security Policies (P-CISPs) were established in 2006, prior to consolidation of IT services under OIT in 2008, and were subsequently updated in 2011 by OIT. OIT is currently revising the P-CISPs and plans to publish and communicate the policies once they have been updated and approved.
- We found inconsistency between management's expectations of backup and recovery requirements identified in the Colorado Information Security Policies (P-CISPs) and OIT personnel's understanding of the policies.
- OIT and agency personnel were not aware of backup and recovery policy requirements, including various roles and responsibilities over backup and recovery processes.
- Five of five systems tested had control failures across multiple backup and recovery controls. Two of five systems tested had failures in every control category.
- System restoration and recovery testing is not consistently performed per policy requirements.
- Physical and logical access controls to facilities, systems, and data are not being performed consistently according to OIT policy requirements.
- Agency Cyber Security Plans and agency Disaster Recovery Plans have not been updated and approved by OIT since 2012.
- An Enterprise Cyber Security Plan (ECSP) was introduced through a rule change [C.C.R. 8 1501-5] in December 2013 and will replace the Agency Cyber Security Plans as of July 15, 2014. However, as of early October 2014, the ECSP has not been formally submitted to the CIO for approval.

BACKGROUND

Governor's Office of Information Technology:

- Was established in 2008.
- Centralized the management of Executive Branch information technology resources, including IT staff.
- Is responsible for documenting policies, procedures, and guidelines for IT services.
- Provides IT services, including backup and recovery, for systems across Executive Branch agencies.
- Oversees the backup and recovery processes for approximately 149 applications or systems classified to be essential or critical.

OUR RECOMMENDATIONS

The Governor's Office of Information Technology should:

- Review, update, and communicate system backup and recovery policies and establish a mechanism to hold IT staff accountable for implementing the policies.
- Document and implement backup and recovery roles and responsibilities per requirements.
- Work with agencies to develop system backup and recovery procedures that meet agency needs.
- Categorize data on systems and apply encryption policy requirements when applicable.

OIT agreed and partially agreed with all of the recommendations.

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

RECOMMENDATION LOCATOR

AGENCY ADDRESSED: GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

REC. NO.	PAGE NO.	RECOMMENDATION SUMMARY	AGENCY RESPONSE	IMPLEMENTATION DATE
1	23	Ensure that backup and recovery procedures for OIT-managed systems are in place and appropriate by (a) communicating the relevant backup and recovery policies to OIT personnel responsible for establishing, implementing, performing, and managing backup and recovery procedures and establishing a mechanism to hold IT staff accountable for implementing backup and recovery policies and procedures and (b) ensuring that backup and recovery procedures are developed and implemented in accordance with agency Disaster Recovery Plans. This would include coordinating with agency personnel to identify system backup and recovery requirements in agency Disaster Recovery Plans.	A AGREE B AGREE	A JULY 2015 B DECEMBER 2016

AGENCY ADDRESSED: GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

REC. NO.	PAGE NO.	RECOMMENDATION SUMMARY	AGENCY RESPONSE	IMPLEMENTATION DATE
2	29	Ensure that backup and recovery monitoring processes are effective by (a) updating policies by adding monitoring requirements and standards that ensure the availability of information systems and data through backup and recovery, (b) establishing processes to communicate updated OIT backup and recovery policies to personnel responsible for managing monitoring processes and holding personnel accountable for implementing the policies, (c) correcting configurations on systems that can support automated backup and recovery notifications to notify appropriate personnel of backup status in a timely manner, and (d) ensuring that appropriate resources are cross-trained and allocated to perform manual backup monitoring processes.	A AGREE B AGREE C AGREE D AGREE	A DECEMBER 2016 B JULY 2015 C DECEMBER 2016 D DECEMBER 2016
3	35	Ensure that backup and recovery offsite storage requirements are met by (a) establishing processes to communicate OIT and agency backup and recovery policies to personnel responsible for managing offsite backup storage procedures and hold personnel accountable for implementing the procedures, (b) ensuring that personnel responsible for managing backup and recovery processes have the facilities to comply with offsite storage policy requirements, and (c) developing and following a formal process to coordinate backup and recovery process changes with agency system owners.	A AGREE B AGREE C AGREE	A JULY 2015 B DECEMBER 2016 C DECEMBER 2015

AGENCY ADDRESSED: GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

REC. NO.	PAGE NO.	RECOMMENDATION SUMMARY	AGENCY RESPONSE	IMPLEMENTATION DATE
4	42	Ensure that encryption is applied to backup and recovery media and systems appropriately by (a) establishing a process to communicate relevant OIT policies to personnel responsible for categorizing data according to policy requirements and (b) developing and implementing a process to categorize all backed up data based on the OIT policies and establishing a mechanism to hold IT staff accountable for implementing data backup encryption processes, as appropriate.	A AGREE B AGREE	A JULY 2015 B DECEMBER 2016
5	47	Ensure that system recovery policy requirements are met by (a) establishing processes to communicate OIT system recovery policies to personnel responsible for managing system recovery processes and holding personnel accountable for implementing the policies and (b) evaluating hardware needs and resources to adequately perform system recovery testing and providing the necessary hardware, based on availability of resources.	A AGREE B AGREE	A JULY 2015 B DECEMBER 2017
6	55	Ensure that OIT backup and recovery access management processes are effective by (a) updating policies to include access management requirements and standards to address the risks associated with lost or stolen access cards or tokens and to ensure that access to backup and recovery facilities is restricted appropriately and (b) establishing a process to communicate access management policies to personnel responsible for managing these procedures and holding personnel accountable for implementing the policies.	A PARTIALLY AGREE B AGREE	A DECEMBER 2016 B JULY 2015

AGENCY ADDRESSED: GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

REC. NO.	PAGE NO.	RECOMMENDATION SUMMARY	AGENCY RESPONSE	IMPLEMENTATION DATE
7	63	Improve governance over backup and recovery processes by (a) creating a process for reviewing, updating, and communicating OIT backup and recovery policies to personnel responsible for managing IT backup and recovery processes and establishing a mechanism to hold IT staff accountable for implementing backup and recovery policies and procedures and (b) finalize the ECSP that was due July 15, 2014, including backup and recovery roles and responsibilities within OIT.	A AGREE B PARTIALLY AGREE	A JULY 2015 B JULY 2015

CHAPTER 1
OVERVIEW OF BACKUP AND RECOVERY

In May 2007, the Governor issued Executive Order D 016 067 to centralize the management of Executive Branch information technology resources under the Governor's Office of Information Technology (OIT). The purpose was to address infrastructure, purchasing, project planning and delivery, asset management, and strategic leadership needs. OIT was created on July 1, 2008 through Senate Bill SB08-155 and codified in Section 24-37.5-101, C.R.S. Senate Bill SB08-155 was designed to consolidate management of Executive Branch agencies' information

technology functions, systems, and actions under the oversight of the Governor's Office of Information Technology.

Exhibit 1.1 identifies the agencies that are within and outside of OIT's oversight.

EXHIBIT 1.1. GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY OVERSIGHT

AGENCIES WITHIN OIT'S OVERSIGHT	
Department of Agriculture	Department of Natural Resources
Department of Corrections	Department of Personnel & Administration
Department of Education	Department of Public Health and Environment
Department of Health Care Policy and Financing	Department of Public Safety
Department of Higher Education	Department of Regulatory Agencies
Department of Human Services	Department of Revenue
Department of Labor and Employment	Department of Transportation
Department of Local Affairs	Governor's Office
Department of Military and Veteran Affairs	
AGENCIES OUTSIDE OIT'S OVERSIGHT	
Department of Law (Attorney General)	Institutions of Higher Education
Department of State (Secretary of State)	Judicial Branch
Department of Treasury (State Treasurer)	Legislative Branch

SOURCE: Office of the State Auditor's analysis of Sections 24-37.5-102 through 105, C.R.S.

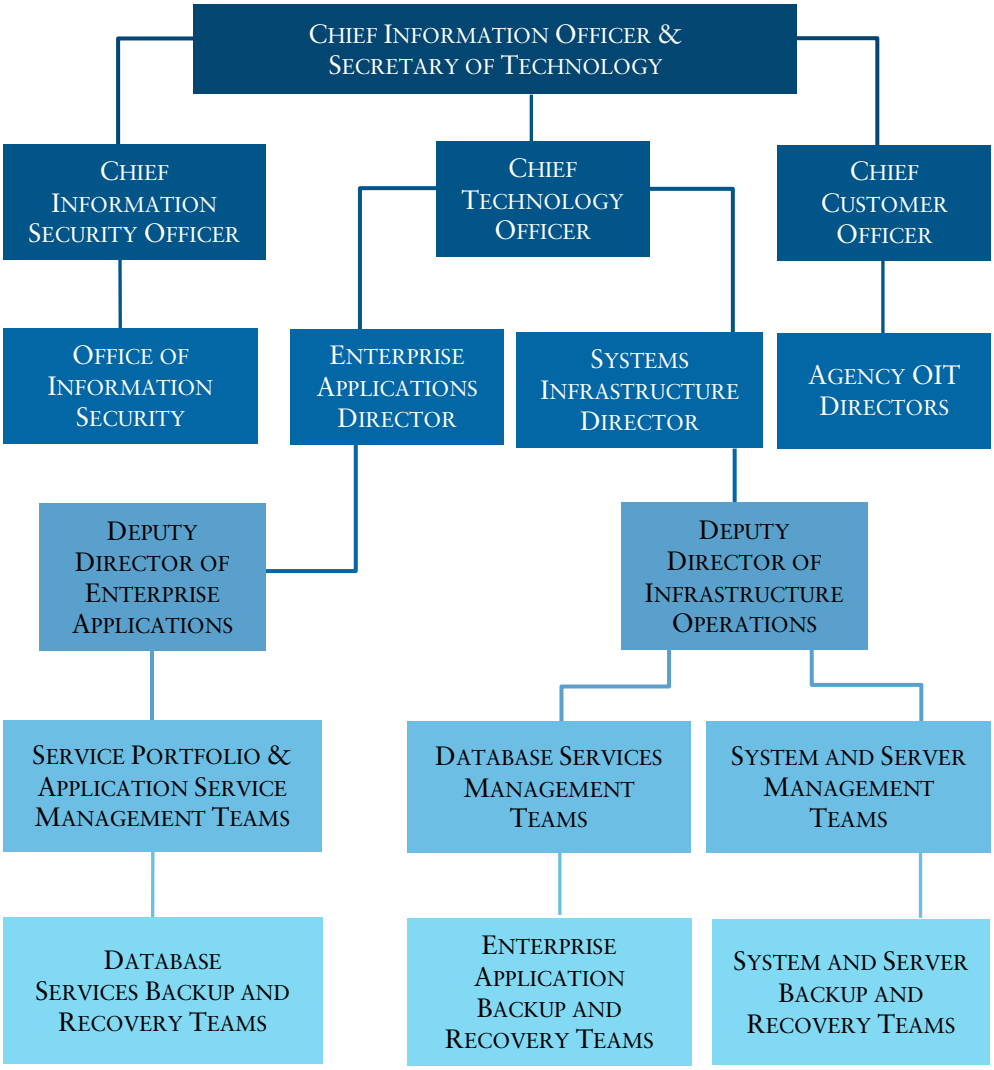
BACKUP AND RECOVERY ORGANIZATIONAL STRUCTURE

As a result of the consolidation, OIT is responsible for overseeing and providing backup and recovery services, in accordance with agency business requirements, to ensure that data and systems are available in the event that systems fail or have disruptions in service. OIT oversees the backup and recovery processes for approximately 149 applications or systems classified to be essential or critical. Systems are classified as essential or critical based on the importance of the system or the types of service the system provides to the agency. An essential system is defined by OIT as a system that affects life-safety and where loss or unavailability of the system is unacceptable. A critical system is defined by OIT as a system that provides critical data to the public, serves a vital function to government, but does not affect life-safety.

Currently, OIT backup and recovery personnel are required to follow the Colorado Information Security Policies (P-CISPs), agency data backup procedures, and agency Disaster Recovery Plans to perform backup and recovery processes.

Exhibit 1.2 outlines the structure of OIT as it relates to backup and recovery processes. Detailed descriptions of the responsibilities for items in the exhibit follow. The descriptions of responsibilities are limited to accountabilities as they relate to backup and recovery processes.

EXHIBIT 1.2. GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY BACKUP AND RECOVERY ORGANIZATIONAL STRUCTURE



SOURCE: Office of the State Auditor's analysis of the Governor's Office of Information Technology Organizational Chart as of 9/2/2014.

THE CHIEF INFORMATION OFFICER (CIO) & SECRETARY OF TECHNOLOGY is responsible for the overall administration of OIT as well as supervising the Chief Information Security Officer (CISO). Statute requires the CIO to coordinate and direct the development, communication, and enforcement of policies, standards, specifications, and guidelines for information technology in public agencies, including those related to backup and recovery. The CIO is responsible for reviewing and approving the Cyber Security Plan on an annual basis.

THE CHIEF INFORMATION SECURITY OFFICER (CISO) reports to the CIO and is responsible for overseeing the Office of Information Security and Colorado Information Security Program which includes governance, risk, compliance, and risk management. Statute requires the CISO to develop, update, communicate, and ensure the incorporation of and compliance with information security policies, standards, and guidelines, including those related to backup and recovery for state agencies. Further, the CISO is responsible for conducting information security awareness and training programs for OIT staff. Finally, the CISO is responsible for annually submitting the Enterprise Disaster Recovery Plan Summary (DRP) as well as submitting the Enterprise Cyber Security Plan to the CIO on or before July 15 of each year.

THE OFFICE OF INFORMATION SECURITY (OIS) is responsible for cyber security readiness and awareness. The OIS works with federal, state, local, and private sector partners to gather and analyze information on cyber threats and vulnerabilities that present risks to the state's critical information systems and data. The Security Management team within OIS manages the Colorado Information Security Policies (P-CISPs) and security standards, including those associated with backup and recovery.

THE ENTERPRISE APPLICATION DIRECTOR AND DEPUTY DIRECTOR OF ENTERPRISE APPLICATIONS are responsible for overseeing application services. This includes supervising the operations teams that manage executive branch agencies' applications and systems used to collect,

store, and manage data. As part of the management of these applications and systems, the operations teams perform application backup and recovery processes.

THE SYSTEMS INFRASTRUCTURE DIRECTOR AND DEPUTY DIRECTOR OF INFRASTRUCTURE OPERATIONS are responsible for overseeing system, server, and database services. This includes supervising the managers and the individuals on the operations teams that perform system, server, and database backup and recovery processes.

DATABASE SERVICES, ENTERPRISE APPLICATION, AND SYSTEM AND SERVER BACKUP AND RECOVERY TEAMS are responsible for day-to-day backup and recovery operations and processes for agency systems, which include applications, operating systems, and databases.

THE CHIEF CUSTOMER OFFICER (CCO) manages relationships with agency partners, supervises agency IT directors, works to communicate OIT services, and oversees agency system and data classification processes which are relevant in developing backup and recovery objectives and requirements.

AGENCY OIT DIRECTORS are responsible for working with agencies to identify agency backup and recovery objectives and requirements, required by policy (Disaster Recovery, P-CISP-004) to lead the development of agency Disaster Recovery Plans and develop data backup procedures for performing backup and recovery services on Executive Branch agencies' systems and data.

FUNDING

The Information Technology Revolving Fund (Fund) was established in statute (Section 24.37.5-112, C.R.S.) in 2008 for OIT to deposit fees from agencies for their share of information technology costs provided by OIT. Annually, OIT receives an appropriation from the Fund to cover OIT direct and indirect costs. The annual appropriations of funds are identified in the General Appropriations Act Long Bill. In Exhibit 1.3, we provide the total appropriations and

full time equivalents (FTE) for Fiscal Year 2012 through Fiscal Year 2015.

EXHIBIT 1.3. OFFICE OF INFORMATION TECHNOLOGY APPROPRIATIONS AND FULL TIME EQUIVALENTS FOR FISCAL YEARS 2012 THROUGH 2015

	FY2012	FY2013	FY2014	FY2015	PERCENT CHANGE FROM FY2012-FY2015
APPROPRIATION (MILLIONS)	$125.7	$136.3	$151.4	$186.4	48.3%
FTE	902.8	897.5	920	925.9	2.6%

SOURCE: HB14-1336 Long Appropriations Bill

PREVIOUS OSA BACKUP AND RECOVERY RECOMMENDATIONS

Over the past several years, the Office of the State Auditor (OSA) has made recommendations related to backup and recovery process improvements for individual applications and systems. These recommendations were made as a result of IT audit work in support of the annual statewide financial audits as well as IT work in support of various performance audits that were not directly related to backup and recovery topics.

Since 2008, the OSA made 23 recommendations related to data backups and secured storage of backups. Exhibit 1.4 contains a summary of audit recommendations and implementation statuses related to backup and recovery since 2008, for which OIT has responsibility:

EXHIBIT 1.4. BACKUP AND RECOVERY RECOMMENDATIONS MADE BY THE OSA 2008–2014

	RECS SINCE 2008	FULLY IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED
DRIVER'S LICENSE & ID CARD SECURITY AUDIT, 2008				
Driver's License Information System – Department of Revenue	4	3	1	0
SAP INFORMATION SYSTEM AUDIT, 2010				
SAP – Department of Transportation	2	1	1	0
STATEWIDE FINANCIAL AUDIT, FY2010				
LEAP – Department of Human Services	1	1	0	0
Columbia Ultimate Business Solutions (CUBS) – Department of Personnel & Administration and OIT	2	2	0	0
GenTax – Department of Revenue	1	0	1	0
STATEWIDE FINANCIAL AUDIT, FY2011				
County Financial Management System - Department of Human Services and OIT	1	1	0	0
STATEWIDE FINANCIAL AUDIT, FY2012				
AVATAR – Department of Human Services and OIT	3	3	0	0
CFMS – Department of Human Services and OIT	1	1	0	0
KRONOS – OIT	1	1	0	0
COMPASS – Department of Public Health and Environment & OIT	1	0	0	1
STATEWIDE FINANCIAL AUDIT, FY2013				
CPPS – Department of Personnel & Administration and OIT	3	0	0	3[1]
KRONOS – OIT	1	0	0	1[2]
MEDICAL MARIJUANA REGULATORY PART II, 2013				
Medical Marijuana Registry – Department of Public Health and Environment	2	1	1	0
TOTAL RECOMMENDATIONS	23	14	4	5
PERCENTAGES	100%	61%	17%	22%

SOURCE: Office of the State Auditors Recommendations Database

[1]Two of the three recommendations have implementation dates of December 2014.

[2] This recommendation has an implementation date of September 2015.

AUDIT PURPOSE, SCOPE, AND METHODOLOGY

We conducted this 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 February 2014 through August 2014. We acknowledge the cooperation and assistance by staff and management at the Governor's Office of Information Technology, as well as the agencies that own the applications we reviewed.

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 and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The primary objectives of this audit were to evaluate the design and operating effectiveness of backup and recovery governance, management, and operational processes around a sample of critical and essential IT systems within the Executive Branch agencies under the authority and management of OIT.

We judgmentally sampled two essential systems and three critical systems (five total systems) within Executive Branch agencies overseen by OIT and performed test procedures to accomplish our audit objectives. For the purpose of this audit, we defined a "system" as having three components – the application, the application's operating system, and the application's database. The backup and recovery processes for each of these components is performed by separate OIT teams and thus we performed independent backup and recovery testing for each component. Therefore, we tested five systems with a total of 15 separate components for this audit. We specifically selected systems that had not been tested in OSA IT engagements in the last five years. Additionally, we selected systems across multiple Executive Branch departments and across multiple IT platforms. The purpose of this selection methodology was to gain a broad understanding of

backup and recovery processes across critical or essential systems that have not been assessed in recent years as part of OSA audits.

We did not include the names of the systems or the agencies that own the systems in this report to protect the security of the agencies, systems, and data associated with this audit. Below are high-level descriptions of the systems and the data on the systems as well as recovery requirements.

SYSTEM 1: A system used by the state to communicate with public safety organizations. There are approximately 150 users of the system at 6 regional centers. OIT and the system business owners coordinated and classified this as an essential system, and according to OIT's requirements for essential systems, the system must be recovered within 2 to 24 hours after an outage.

SYSTEM 2: A system that enables a variety of organizations to electronically track health records in real time. The system contains approximately 4 million records. There are approximately 2,000 users of the system. OIT and the system business owners coordinated and classified this a critical system, and according to OIT's requirements for critical systems, the system must be recovered within 72 hours after an outage.

SYSTEM 3: A system that contains citizens' information and processes payments to the state. The system contains approximately 55 million records. There are approximately 34 system users. OIT and the system business owners coordinated and classified this as a critical system, and according to OIT's requirements for critical systems, the system must be recovered within 72 hours to one week after an outage.

SYSTEM 4: This system is a collection of 45 applications within an interface and is used by state personnel. The system has 8,746 active users and stores information on more than 130,000 individuals. OIT and the system business owners coordinated and classified this as an essential system, and according to OIT's requirements for essential systems, the system must be recovered within 2 to 24 hours after an outage.

SYSTEM 5: This system contains claimant information, is used by approximately 120 state personnel, processes approximately $1.3 million in claims, and an additional $5 million in payments. OIT and

the system business owners coordinated and classified this as a critical system, and according to OIT's requirements for critical systems, the system must be recovered within 72 hours to one week after an outage.

We performed the following procedures to accomplish our audit objectives:

- Reviewed relevant state statutes, rules, OIT and agency policies and procedures, and other guidance relative to the governance and operations of system backup and recovery processes.
- Interviewed OIT and agency management and staff.
- Gathered and analyzed documentation and data on OIT's governance and performance of system backup and recovery processes.
- Evaluated system backup and recovery processes and documentation against policy requirements.

We planned our audit work to assess the design and effectiveness of governance over, and operation of, system backup and recovery processes and controls that were significant to our audit objectives. Our conclusions on the effectiveness of those controls, as well as details about the audit work supporting our findings, conclusions, and recommendations, are described in CHAPTER 2 of this report.

CHAPTER 2

BACKUP AND RECOVERY PROCESSES

Backup and recovery processes for Executive Branch agencies are managed by the Governor's Office of Information Technology (OIT). OIT's officers and employees are responsible for developing backup and recovery processes in accordance with agency requirements to ensure the reliability, availability, and effective management of Executive Branch systems and data. Colorado statute coupled with OIT and agency policies and procedures define the requirements and guidelines that OIT is required to apply to system backup and recovery processes.

EVALUATIONS OF OIT BACKUP AND RECOVERY ENVIRONMENTS

OIT hired two different consultants over the past two years to assess areas that included disaster recovery and backup and recovery. The following summarizes the work and findings contained in the two reports:

REPORT 1

OPERATIONS, DISASTER RECOVERY, BUSINESS CONTINUITY ASSESSMENT: In March 2012, OIT contracted a consulting firm to perform an evaluation of the State's essential and critical applications to determine if these important applications have Disaster Recovery Plans in place. Overall, the consulting firm found that most of the essential and critical systems they assessed (192 of the 220 applications reviewed, or 87 percent) did not have formalized Disaster Recovery Plans in place. The report recommended:

- Develop Disaster Recovery Plans.
- Update existing Disaster Recovery Plans.
- Test Disaster Recovery Plans.
- Update the essential and critical applications/systems list.

OIT is in process of implementing these recommendations.

REPORT 2

STATE OF COLORADO BACKUP AND RECOVERY ASSESSMENT: OIT hired a consulting firm to perform a data protection assessment for the State of Colorado across 17 agencies in June 2014. The goals of the assessment were to evaluate the current backup and recovery infrastructure, identify backup and recovery challenges, propose tactical solutions, begin planning for a long-term backup and recovery strategy, and align business requirements with appropriate technologies. The assessment was performed on day to day backup and recovery operations and did not include an assessment of disaster

recovery processes. As of the time this report was written, a finalized report of the assessment had not been completed.

IMPACT OF BACKUP AND RECOVERY FAILURES

In April 2013, one Executive Branch Department experienced a backup and recovery failure for a key IT system that stored applicant data submitted by the public. OIT maintains the servers that store the IT system and applicant data; however, those servers failed. This resulted in a loss of all the applicant data submitted by the public. OIT performed backups of most of the data stored on the servers and used the backups to restore the data to new servers. However, the applicant data collected during the initial application process was not backed up. Therefore, OIT was able to restore the IT system because it was backed up; however, some of the data stored on the servers, including applicant data, could not be restored because this data was not backed up. The Department had to replace the lost data and subsequently divisions within the department changed the application processes and required applicants to resubmit information that they had previously provided.

BACKUP AND RECOVERY AUDIT

Our audit work reviewed operational and information security processes for backup and recovery systems managed by OIT as well as OIT's governance of those backup and recovery processes, including policies and procedures, resource management, and communication. This chapter presents our findings related to backup and recovery and information security processes performed by OIT. Overall, we identified areas in which OIT needs to improve operational, information security, and governance processes related to backup and recovery.

AGENCY DATA BACKUP AND RECOVERY PROCEDURES

OIT developed backup and recovery policies to provide structure and guidance for implementing backup and recovery processes. The current published Colorado Information Security Policies (P-CISPs) require agency IT Directors (OIT staff) to work with the agencies to develop Disaster Recovery Plans, including agency backup and recovery objectives and requirements. OIT and agency personnel are responsible for developing data backup and recovery procedures based on the objectives and requirements for each system identified in agency Disaster Recovery Plans. The procedures are to be applied to agency systems and data by OIT backup and recovery personnel. Each agency has independent requirements that should be identified and documented to ensure that each agency's backup and recovery requirements are met. Agency data backup and recovery procedures are intended to provide a link between the agency's backup and recovery needs and requirements, and the processes that OIT backup and recovery teams perform.

Data backup procedures can include, but are not limited to, details such as system information, the criticality of systems and data, backup scheduling requirements, the type of backups to be performed, recovery time objectives, recovery point objectives, backup storage requirements, restoration testing requirements, backup logging and monitoring requirements, backup memory requirements, backup paths, and the steps to perform backup and recovery functions.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of our audit work was to evaluate whether the State's backup and recovery processes that are managed by OIT are sufficient and comply with applicable backup and recovery policy and procedure requirements. As part of our audit work, we reviewed backup and recovery processes and controls for a sample of four OIT-managed systems by performing test procedures on the application, operating system, and database within each system. We determined that System 1 was not applicable for this testing. We interviewed OIT personnel and reviewed OIT policies to identify backup and recovery procedure requirements. We also reviewed whether OIT has adequate processes to verify that OIT personnel and agencies follow backup and recovery requirements and that backup and recovery procedures are designed appropriately and operating effectively.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We applied the following criterion when evaluating the sufficiency of backup and recovery procedures for OIT-managed systems:

BACKUP AND RECOVERY PROCEDURES MUST BE ESTABLISHED. According to OIT's Systems and Applications Security policy (P-CISP-007, 7.2.3), "The Agency IT Director shall establish data back-up procedures to recover information according to recovery objectives established in the agency Disaster Recovery Plans and in accordance with the Disaster Recovery Policy, P-CISP-004."

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

We identified the following problem regarding backup and recovery procedures for OIT-managed systems:

FORMAL BACKUP AND RECOVERY PROCEDURES HAVE NOT BEEN ESTABLISHED. For four out of the four systems we tested (System 2, System 3, System 4, and System 5), OIT backup and recovery personnel stated that formal backup and recovery procedures have not been established.

WHY DID THE PROBLEMS OCCUR?

LACK OF AWARENESS OF BACKUP AND RECOVERY POLICIES. OIT backup and recovery personnel stated they were not aware of OIT's Disaster Recovery policy (P-CISP-004) requiring backup procedures to be established based on requirements identified in agency Disaster Recovery Plans. OIT personnel may not be aware of the policy since OIT does not have consistent procedures in place to ensure that OIT personnel follow policies related to system recovery testing, such as requiring personnel to periodically review current policies.

WHY DOES THIS FINDING MATTER?

When backup and recovery procedures have not been formalized, backup and recovery procedures may be inadequate to support system backup and recovery needs and increases the possibility that systems and information will be unavailable in the event of a system outage or failure.

RECOMMENDATION 1

The Governor's Office of Information Technology (OIT) should ensure that backup and recovery procedures for OIT-managed systems are in place and appropriate by:

A Communicating the relevant backup and recovery policies to OIT personnel responsible for establishing, implementing, performing, and managing backup and recovery procedures and establishing a mechanism to hold IT staff accountable for implementing backup and recovery policies and procedures.

B Ensuring that backup and recovery procedures are developed and implemented in accordance with agency Disaster Recovery Plans. This would include coordinating with agency personnel to identify system backup and recovery requirements in agency Disaster Recovery Plans.

RESPONSE

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

A AGREE. IMPLEMENTATION DATE: JULY 2015.

The Governor's Office of Information Technology (OIT) agrees that a process for reviewing, updating, and communicating policies is critical to the business. The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification, are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all OIT personnel and state agencies. Currently any new policies that are approved by the executive leadership team are communicated to all OIT staff through email and also published on OIT's internal website. OIT will enhance its policy communication effort by creating a quarterly update with

OIT staff. OIT will implement a biannual operational review for all relevant OIT staff to strengthen accountability and ensure compliance with established policies and procedures. Also OIT will partner with management teams at state agencies to ensure that agencies' personnel are aware of relevant policies.

B AGREE. IMPLEMENTATION DATE: DECEMBER 2016.

The Governor's Office of Information Technology (OIT) agrees that a process for developing, updating, and communicating policies is critical. The Colorado Information Security Policies and procedures which include backup and recovery policies and associated activities, are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all OIT employees and state agencies. OIT also agrees that backup and recovery procedures should be aligned to disaster recovery plans. However, the development of a disaster recovery plan is a joint responsibility between state agencies and OIT. The availability of funding and resources is necessary to document and operationalize the disaster recovery plans, including procurement and configuration of required infrastructure, and testing of the plan both at state agencies and OIT. OIT will work with management teams at state agencies to identify resource and budget needs and initiate or assist the agency in funding request. The complete implementation of this recommendation is subject to timely availability of funding and resources.

AUDITOR'S ADDENDUM

It is unclear why implementation of this recommendation will take two years.

MONITORING OF BACKUP AND RECOVERY PROCESSES

OIT backup and recovery personnel are responsible for backing up data up in an effort to ensure that applications, operating systems and data can be restored or recovered in the event of a system failure or outage. OIT backup and recovery personnel are responsible for monitoring backup and recovery processes to ensure backups of agency systems and data are available. OIT backup and recovery personnel monitor system and data backup sessions, by manual or automated processes, to validate that backups are completed. The monitoring process allows backup and recovery teams to identify problems such as failed backups or partially completed backups, and take corrective action. Agencies should establish requirements that restrict how much data can be lost and the length of time systems can be inoperable before they need to be restored. Monitoring has an impact on the availability of backups and is directly related to OIT's success in meeting agency backup and recovery requirements.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of our audit work was to evaluate whether the State's backup and recovery processes on systems that are managed by OIT have sufficient monitoring controls and comply with the monitoring requirements established by OIT. As part of our audit work, we reviewed the backup and recovery processes and controls for a sample of five OIT-managed systems by performing test procedures on the application, operating system, and database within each system. We interviewed OIT personnel and reviewed OIT policies and procedures to identify monitoring requirements. We also reviewed whether OIT has adequate processes to verify that OIT personnel and agencies

follow monitoring requirements and that system controls are designed appropriately, and operating effectively.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We applied the following criteria when evaluating the sufficiency of monitoring controls for backup and recovery systems that are managed by OIT:

INFORMATION MUST BE AVAILABLE. According to statute (Section 24-37.5-401 (1)(a)), the General Assembly determined a need for coordinated efforts to protect IT assets and, in part, to assure the availability of information. Statute (C.R.S. 24-37.5-402 (1)) defines "availability" as "the timely and reliable access to and use of information created, generated, collected, or maintained by a public agency." The ability to backup and restore a system, in the event of a network, hardware, software, or database incident that renders a system unreachable or unusable is critical for meeting the availability requirement outlined in the statute.

We compared OIT's backup and recovery processes with industry best practices as specified by the Information Systems Audit and Control Association (ISACA). Specifically, the availability of data depends on successful backup and recovery processes that meet requirements defined in an organization's disaster recovery plan. By proactively monitoring backup processes through the use of appropriate tools and methods, this enables backup and recovery personnel to address backup failures.

In addition, according to ISACA, complete and accurate processing of data requires effective management of personnel, data processing procedures, job scheduling and monitoring. This process includes defining operating policies and procedures for effective management of scheduled processing and monitoring.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

We identified the following problems regarding the backup monitoring process of systems and media:

- **BACKUP AND RECOVERY CONTROLS DO NOT EXIST TO VALIDATE THAT THE BACKUP PROCESS IS WORKING.** For one of the five systems we tested (System 3), we were unable to determine whether successful backups of one component within the system (the database) had occurred. There were no backup logs and no monitoring or notification processes in place.

- **BACKUP FAILURE NOTIFICATIONS ARE NOT PROVIDING ADEQUATE NOTICE.** Of the five systems we tested, four of the OIT teams that provide backup and recovery services on the systems noted that they rely on automated backup status notifications. For one of the four systems we tested (System 3), components within the systems that were relied upon to send notifications to personnel were not configured appropriately, therefore backup status notifications were not being sent to backup and recovery personnel.

  For one of the four systems we tested (System 4), only one user receives automated backup status notifications for components within the system. This would not be adequate if the single user is not available to act on notifications.

WHY DID THE PROBLEMS OCCUR?

The backup and recovery system monitoring problems identified above occurred due to the following reasons:

LACK OF REQUIREMENTS WITHIN POLICIES. There are no requirements identified in OIT policies to address backup and recovery monitoring processes or controls.

INADEQUATE SYSTEM CONFIGURATION. The systems were not configured to generate timely notifications to appropriate backup and

recovery personnel for the components of two of the four systems (System 2 and System 3) that rely on automated backup status notifications.

Lack of an Appropriate Number of Individuals to Perform the Manual Backup Monitoring Process. Only one individual is trained to perform the manual backup monitoring process for the database component of System 2. No one else is trained or has access to monitor the status of database backups.

WHY DOES THIS FINDING MATTER?

When backup and recovery monitoring controls are not established to validate that backup and recovery processes are working, this creates the potential for backup failures to go unnoticed or unresolved for extended periods of time potentially leading to a loss of data and availability.

RECOMMENDATION 2

The Governor's Office of Information Technology (OIT) should ensure that backup and recovery monitoring processes are effective by:

A Updating policies by adding monitoring requirements and standards that ensure the availability of information systems and data through backup and recovery.

B Establishing processes to communicate updated OIT backup and recovery policies to personnel responsible for managing monitoring processes and holding personnel accountable for implementing the policies.

C Correcting configurations on systems that can support automated backup and recovery notifications to notify appropriate personnel of backup status in a timely manner.

D Ensuring that appropriate resources are cross-trained and allocated to perform manual backup monitoring processes.

RESPONSE

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

A AGREE. IMPLEMENTATION DATE: DECEMBER 2016.

The Governor's Office of Information Technology (OIT) agrees that a process for developing, updating, and communicating policies is critical. The Colorado Information Security Policies and procedures which include backup and recovery policies and associated activities, including monitoring backup processes, are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all OIT employees and state agencies. OIT also agrees that backup and

recovery procedures should be aligned to disaster recovery plans. However, the development of a disaster recovery plan is a joint responsibility between state agencies and OIT. The availability of funding and resources is necessary to document and operationalize the disaster recovery plans, including procurement and configuration of the required infrastructure, and testing of the plan both at state agencies and OIT. OIT will work with management team at state agencies to identify resource and budget needs and initiate or assist the agency in funding request. The complete implementation of this recommendation is subject to timely availability of funding and resources.

AUDITOR'S ADDENDUM

It is unclear why implementation of this recommendation will take two years and require additional funding since the recommendation is only to update policies.

B AGREE. IMPLEMENTATION DATE: JULY 2015.

The Governor's Office of Information Technology (OIT) agrees that a process for reviewing, updating, and communicating policies is critical to the business. The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification, are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all OIT personnel and state agencies. Currently any new policies that are approved by the executive leadership team are communicated to all OIT staff through email and also published on OIT's internal website. OIT will enhance its policy communication effort by creating a quarterly update with OIT staff. OIT will implement a biannual operational review for all relevant OIT staff to strengthen accountability and ensure compliance with established policies and procedures. Also OIT will partner with management teams at state agencies to ensure that agencies' personnel are aware of relevant policies.

C AGREE. IMPLEMENTATION DATE: DECEMBER 2016.

OIT agrees that backups should be monitored to ensure successful completion, however we do not require that all backup notifications be delivered automatically. State applications span over different technologies and platforms and all of them do not support automated notifications. Currently, OIT staff responsible for backups manually confirm that backup tasks were completed. OIT will evaluate the existing systems for capability of automated notification and will request funding to implement an enterprise wide notification system.

AUDITOR'S ADDENDUM

It is unclear why implementation of this recommendation will take two years and require additional funding since the recommendation is only to correct the configuration of existing systems with automatic notification capabilities.

D AGREE. IMPLEMENTATION DATE: DECEMBER 2016.

OIT agrees that appropriate resources are needed to monitor manual backups. State applications span over different technologies and platforms. Systems that have the capability of implementing automated notifications will be evaluated and automated notification systems will be implemented subject to availability of funding. Systems that do not support automated notification capability would be monitored manually. Once it is determined how many systems need to be monitored manually OIT will perform a resources review, perform cross training where needed and allocate resources as needed.

AUDITOR'S ADDENDUM

It is unclear why implementation of this recommendation will take two years and require additional funding since the recommendation is only to cross-train other personnel to monitor manual backup processes.

OFFSITE BACKUP STORAGE MANAGEMENT

OIT backup and recovery personnel are responsible for ensuring that backup data is protected and stored offsite in an effort to safeguard application, operating system, and data backups so they are available and can be used to recover systems and data in the event of a system failure or outage. OIT backup and recovery personnel are responsible for ensuring physical backup media is sent offsite to a storage facility periodically based on agency requirements, and that virtual system and data backups are stored in a separate facility than the systems and data they backup.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of our audit work was to evaluate whether the State's offsite backup storage processes for systems managed by OIT comply with requirements established by OIT policy and business requirements outlined by the agencies. As part of our audit work, we reviewed offsite backup storage processes and controls for five OIT-managed systems by performing test procedures on the application, operating system, and database within each system. We interviewed OIT personnel and reviewed OIT and agency policies and procedures to identify offsite backup storage requirements. We also reviewed whether OIT has adequate processes to verify that OIT personnel and agencies follow offsite backup storage requirements and that system controls are designed appropriately and operating effectively.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We applied the following criteria when evaluating the sufficiency of offsite backup storage processes that are managed by OIT:

BACKUP MEDIA MUST BE ROTATED TO AN OFFSITE STORAGE FACILITY. According to OIT's Disaster Recovery policy (P-CISP-004, 7.1.7.1) regarding agency requirements that should be addressed in the Disaster Recovery Plan, "All backup media, documentation, and other IT resources necessary to recover or resume IT processing must be offsite. Backup procedures and rotation schemes must be adequate to provide the necessary data for recovery while minimizing data loss."

Additionally, for one of the five agencies that owned systems that we tested as a part of this audit, an agency-specific cyber security policy was available and was last updated in 2008. This policy included a requirement for backup media to be rotated to an offsite location weekly for all line-of-business systems, which included one of the systems (System 3) that we tested as a part of this audit.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

We identified the following problems regarding offsite backup storage processes:

OFFSITE BACKUP STORAGE POLICIES ARE NOT BEING FOLLOWED. For two of the five systems we tested (System 2, System 3), offsite backup storage policies are not being followed. Backup media is not sent to a separate, offsite facility for one of the two systems identified (System 2). For this system, OIT backup and recovery personnel noted that they do not perform backups using physical media but perform virtual backups/replications of the application, operating system, and database to virtual machines. However the virtual machines are housed on physical servers in the same facility as the production system's physical servers, and therefore, the backups on the virtual machines are not stored at a separate offsite facility. For the second system (System 3), OIT backup and recovery personnel were not following the agency-specific disaster recovery policy that had been established. Specifically, for this system (System 3), backup media is sent offsite less frequently than the weekly requirement identified in the agency-specific policy. The backup tapes for this system were

residing in this same physical location as the production system for at least four weeks before being sent to the offsite location.

WHY DID THE PROBLEMS OCCUR?

Lack of Awareness and Communication Regarding Offsite Storage Policies. OIT backup and recovery personnel stated that they were not aware of OIT's Disaster Recovery policy (P-CISP-004) requiring Disaster Recovery Plans to be established at each agency to incorporate agency-specific offsite backup and recovery requirements. OIT backup and recovery personnel may not be aware of the policy since OIT does not have a consistent procedure in place to ensure that personnel follow Disaster Recovery Policies, such as requiring personnel to periodically review current policies. In addition, OIT could not provide evidence of policy training or regular communications regarding current or changed policies.

Lack of Offsite Backup Storage Facility. OIT backup and recovery personnel indicated that they currently do not have an offsite storage facility to which they can send backups.

Lack of Coordination With Agency. OIT backup and recovery personnel indicated that the offsite backup media transport schedule was changed from weekly transports to monthly offsite transports by the server administration team. This was done without the knowledge or approval of the agency system owner. OIT personnel noted that the schedule change was made because they work at multiple locations and were not always at the agency during the scheduled weekly backup tape pickup times and there was a cost-savings benefit by changing the schedule from weekly to monthly.

WHY DOES THIS FINDING MATTER?

If backups are not stored at an offsite storage facility, or are not sent offsite as frequently as required, in the event of a disaster, both backups and systems could be damaged or destroyed, resulting in systems and data not being restored, recovered, or available as needed.

RECOMMENDATION 3

The Governor's Office of Information Technology (OIT) should ensure that backup and recovery offsite storage requirements are met by:

A Establishing processes to communicate OIT and agency backup and recovery policies to personnel responsible for managing offsite backup storage procedures and hold personnel accountable for implementing the procedures.

B Ensuring that personnel responsible for managing backup and recovery processes have the facilities to comply with offsite storage policy requirements.

C Developing and following a formal process to coordinate backup and recovery process changes with agency system owners.

RESPONSE

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

A AGREE. IMPLEMENTATION DATE: JULY 2015.

The Governor's Office of Information Technology (OIT) agrees that a process for reviewing, updating, and communicating policies is critical to the business. The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification, are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all OIT personnel and state agencies. Currently any new policies that are approved by the executive leadership team are communicated to all OIT staff through email and also published on OIT's internal website. OIT will enhance

its policy communication effort by creating a quarterly update with OIT staff. OIT will implement a biannual operational review for all relevant OIT staff to strengthen accountability and ensure compliance with established policies and procedures. Also OIT will partner with management teams at state agencies to ensure that agencies' personnel are aware of relevant policies.

B AGREE. IMPLEMENTATION DATE: DECEMBER 2016.

OIT agrees that adequate off-site storage is important to the backup and recovery process. As such in the fall of 2013 OIT requested supplemental funding to perform a study analyzing the size of the State's backup needs and advise on the information technology architecture needed to provide proper data storage and recovery capabilities. The study is currently underway and upon completion OIT will work with the Office of State Planning and Budgeting to identify budget needs and request the necessary funding to secure an off-site facility where needed. The complete implementation of this recommendation is subjected to timely availability of funding and resources.

AUDITOR'S ADDENDUM

It is unclear why implementation of this recommendation will take two years.

C AGREE. IMPLEMENTATION DATE: DECEMBER 2015.

OIT agrees that a process needs to be in place to communicate and coordinate changes to backup and recovery processes and components to the agency system owner. OIT will implement change management process around backup and recovery related changes and communicate the new process.

ENCRYPTION REQUIREMENTS FOR SYSTEMS AND MEDIA

OIT is responsible for working with agencies to identify and categorize agency data based on the data categories outlined in OIT's policies. This includes reviewing the sensitivity of the data that resides on systems and the privacy and compliance rules that the systems and data may be subject to. Once the data has been categorized, OIT is responsible for encrypting the systems and/or media that the data resides on, based on the P-CISPs.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of our audit work was to evaluate whether the State's backup and recovery systems and media that are managed by OIT have sufficient encryption controls and comply with the encryption requirements established by OIT. As part of our audit work, we reviewed encryption processes related to backup and recovery controls for a sample of five OIT-managed systems by performing test procedures on the application, operating system, and database within each system. We interviewed OIT personnel and reviewed OIT policies and procedures and agency documentation to identify encryption requirements. We also reviewed whether OIT has adequate processes to verify that OIT personnel and agencies follow encryption requirements and that system controls are designed appropriately and operating effectively.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

Offsite backup data does not reside in the same physical location as the production data. Therefore, data can be misplaced, lost, or stolen. Data backed up by OIT personnel may contain sensitive information, such as names, identification numbers, like Social Security numbers, or other unique identifying numbers, as well as addresses, or health-related information. In the event that sensitive data on portable or mobile media is compromised, an individual with malicious intent could gain access to the information if the data is not properly encrypted. Therefore, we looked at encryption surrounding data backups.

We applied the following criteria when evaluating the sufficiency of encryption requirements for backup and recovery systems and media that are managed by OIT:

Sensitive Information is Required to be Encrypted on State Systems. According to OIT's Data Handling and Disposal policy (P-CISP-011, 7.2, 8.2, and 8.3), the agency IT Director is to work with agency system owners to identify data contained in systems and categorize the data into one of four categories; the Agency Information Security Officer is to maintain an inventory of systems and their associated data classifications. In addition, OIT's Data Handling and Disposal policy (P-CISP-011, 7.4 and 7.5) states that Unrestricted and Level 1 data does not require encryption while Level 2 and Level 3 data requires encryption. The four data categories as well as the encryption requirements for Level 2 and Level 3 data are noted below:

Unrestricted Data Category. According to OIT's Data Handling and Disposal policy (P-CISP-011, 7.2), unrestricted data is defined as information that would have no measurable impact on the agency in the event of a breach of confidentiality, loss of integrity, or lack of availability.

LEVEL 1 DATA CATEGORY. According to OIT's Data Handling and Disposal policy (P-CISP-011, 7.2), Level 1 data is defined as information that would have little impact on the agency in the event of a breach of confidentiality, loss of integrity, or lack of availability.

LEVEL 2 DATA CATEGORY (HAVING ENCRYPTION REQUIREMENTS). According to OIT's Data Handling and Disposal policy (P-CISP-011, 7.2), Level 2 data is defined as information that would have a significant financial or operational burden on an agency in the event of a breach of confidentiality, loss of integrity, or lack of availability. Additionally, OIT's Data Handling and Disposal policy (P-CISP-011, 7.4 and 7.5) requires that Level 2 data be encrypted when stored on removable media, portable systems, and when transported or transmitted.

LEVEL 3 DATA CATEGORY (HAVING ENCRYPTION REQUIREMENTS). According to OIT's Data Handling and Disposal policy (P-CISP-011, 7.2), Level 3 data is defined as information that is required by federal, state, or local law to be protected, or, in the event of a breach of confidentiality, loss of integrity, or lack of availability would have serious impact to the agency up to and including physical harm to individuals, or that which would cause significant hardship to the agency, state, or commercial entities that have entrusted this data to the agency. Additionally, OIT's Data Handling and Disposal policy (P-CISP-011, 7.4 and 7.5) requires that Level 3 data be encrypted when stored on state systems, removable media, portable systems, and when transmitted or transported.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

We identified the following problems regarding encryption of backup and recovery systems and media:

DATA IS NOT CATEGORIZED AND MAY NOT BE ENCRYPTED APPROPRIATELY. For all five systems we tested, IT Directors had not worked with agencies to categorize data types and inventories of

agency systems, and their associated data classifications had not been formally documented and maintained as required by policy. Because of this, we could not conclude whether agency data required encryption and was encrypted according to OIT policy requirements.

For example, for two of the five systems we tested (System 3 and System 4), although the agency system owners (i.e., senior agency management) had not been through a process to formally categorize the data on their systems, during the audit the system owners stated that the data on their systems fits into the Level 2 data category. Both systems are backed up to portable media that is sent offsite periodically and should be encrypted according policy requirements for Level 2 data. However, we determined that the portable backup media for these systems was not being encrypted.

For a third system (System 1), senior agency management indicated that it was difficult to determine if System 1 contained Level 2 or Level 3 data, despite the system having many different interfaces with other sensitive systems that may contain Level 2 or Level 3 data. However, the transmission of data from the System 1 production site to the offsite backup location was not being encrypted. Some of the OIT personnel that managed the systems were aware that the OIT policies existed (i.e., the Systems and Applications Security Operations and Data Classification, Handling, and Disposal policies), but neither OIT nor agency management and personnel were aware of the contents and the encryption requirements within the policies.

WHY DID THE PROBLEMS OCCUR?

LACK OF POLICY AWARENESS. Neither agency personnel nor OIT personnel were aware that all system data must be defined and categorized according to OIT's Data Handling and Disposal policy. Additionally, neither agency personnel nor OIT personnel were aware that sensitive data stored on backup media is required to be encrypted if it contains Level 2 or Level 3 data. This lack of policy awareness may be due to OIT not having a consistent procedure in place to ensure that personnel follow policies, such as requiring personnel to periodically review current policies. In addition, OIT did not provide

evidence of policy training or regular communications regarding current or changed policies, and this was corroborated by agency and OIT personnel.

WHY DOES THIS FINDING MATTER?

If sensitive data is not encrypted, it may not be secured appropriately and could lead to sensitive information being compromised. If sensitive information is compromised, this could further constitute a security incident, which in turn, could be very costly and time consuming to remediate and address with impacted parties.

RECOMMENDATION 4

The Governor's Office of Information Technology (OIT) should ensure that encryption is applied to backup and recovery media and systems appropriately by:

A Establishing a process to communicate relevant OIT policies to personnel responsible for categorizing data according to policy requirements.

B Developing and implementing a process to categorize all backed up data based on the OIT policies and establishing a mechanism to hold IT staff accountable for implementing data backup encryption processes, as appropriate.

RESPONSE

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

A AGREE. IMPLEMENTATION DATE: JULY 2015.

The Governor's Office of Information Technology (OIT) agrees that a process for reviewing, updating, and communicating policies is critical to the business. The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification, are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all OIT personnel and state agencies. Currently any new policies that are approved by the executive leadership team are communicated to all OIT staff through email and also published on OIT's internal website. OIT will enhance its policy communication effort by creating a quarterly update with OIT staff. OIT will implement a biannual operational review for all relevant OIT staff to strengthen accountability and ensure compliance

with established policies and procedures. Also OIT will partner with management teams at state agencies to ensure that agencies' personnel are aware of relevant policies.

B AGREE. IMPLEMENTATION DATE: DECEMBER 2016.

The Governor's Office of Information Technology (OIT) agrees that accurate data classification is critical to ensure that adequate controls are built around the data. In the fall of 2013 OIT initiated a multi-year project to identify all critical and essential applications under its authority. In the fall of 2014 OIT initiated the process of identifying appropriate data classification for each of these applications. Relevant data encryption requirements can be established once data is classified per Colorado Information Security Policies. OIT will then identify whether or not the functional technology exists to activate "encryption". If the technology is not present within the infrastructure requiring encryption, OIT will identify budget needs for the work and request the necessary funding. The complete implementation of this recommendation is subjected to timely availability of funding and resources.

AUDITOR'S ADDENDUM

It is unclear why implementation of this recommendation will take two years.

SYSTEM RECOVERY TESTING

OIT backup and recovery personnel are responsible for performing system and data backup and recovery testing based on the requirements identified in backup and recovery policies and procedures. This includes performing restoration and recovery testing on a regular basis as prescribed by backup and recovery policy and procedures. OIT backup and recovery personnel are responsible for assessing the results of the recovery testing to verify that systems and data can be restored successfully in the event of loss, disruption, or disaster. Recovery processes are to be modified as necessary based on testing results to ensure that recovery processes will work effectively to meet agency recovery requirements.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of our audit work was to evaluate whether the State's system backup and recovery processes for systems that are managed by OIT have sufficient system recovery processes and comply with the system recovery requirements established by OIT. As part of our audit work, we reviewed the system recovery processes and controls for a sample of five OIT managed systems by performing test procedures on the application, operating system, and database within each system. We interviewed OIT personnel and reviewed OIT and agency policies and procedures to identify system recovery process requirements. We also reviewed whether OIT has adequate processes to verify that OIT personnel and agencies follow system recovery process requirements and that system recovery controls are designed appropriately and operating effectively.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We applied the following criterion when evaluating the sufficiency of system recovery processes for systems managed by OIT:

SYSTEM RECOVERY TESTING MUST BE PERFORMED REGULARLY. OIT's Disaster Recovery policy (P-CISP-004, 7.1.7.2) requires that backup and recovery processes for systems be tested at least on an annual basis.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

We identified the following problem regarding system recovery processes:

SYSTEM RECOVERY TESTING IS NOT PERFORMED ON A REGULAR BASIS. For three of the five systems we tested (System 2, System 3, and System 4), OIT backup and recovery personnel noted that they do not perform regular system restoration testing for the application, operating system, or database. For four of the five systems we tested (System 1, System 2, System 3, System 4), OIT backup and recovery personnel noted that they do not perform regular system recovery testing on backup media and hardware.

WHY DID THE PROBLEMS OCCUR?

LACK OF AWARENESS OF RESTORATION POLICIES. OIT backup and recovery personnel stated they were not aware of OIT's Disaster Recovery policy (P-CISP-004) requiring Disaster Recovery Plans to be tested on a regular basis to test backup media and hardware, and to ensure that IT systems can be effectively recovered and shortcomings can be addressed. OIT backup and recovery personnel may be unaware of the policies due to OIT not having consistent procedures

in place to ensure that personnel follow policies related to system recovery testing.

LACK OF SYSTEM RESOURCES. For two of the five systems we tested (System 3 and System 4), OIT backup and recovery personnel noted that they do not have adequate hardware to perform system recovery testing.

WHY DOES THIS FINDING MATTER?

If system recovery testing policy requirements and procedures are not established or followed, system and data backups may not be restored appropriately to meet the needs of the business, or systems and data may be rendered unavailable in the event of a disaster or system failure.

RECOMMENDATION 5

The Governor's Office of Information Technology (OIT) should ensure that system recovery policy requirements are met by:

A Establishing processes to communicate OIT system recovery policies to personnel responsible for managing system recovery processes and holding personnel accountable for implementing the policies.

B Evaluating hardware needs and resources to adequately perform system recovery testing and providing the necessary hardware, based on availability of resources.

RESPONSE

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

A AGREE. IMPLEMENTATION DATE: JULY 2015.

The Governor's Office of Information Technology (OIT) agrees that a process for reviewing, updating, and communicating policies is critical to the business. The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification, are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all OIT personnel and state agencies. Currently any new policies that are approved by the executive leadership team are communicated to all OIT staff through email and also published on OIT's internal website. OIT will enhance its policy communication effort by creating a quarterly update with OIT staff. OIT will implement a biannual operational review for all relevant OIT staff to strengthen accountability and ensure compliance with established policies and procedures. Also OIT will partner with

management teams at state agencies to ensure that agencies' personnel are aware of relevant policies.

B AGREE. IMPLEMENTATION DATE: DECEMBER 2017.

The Governor's Office of Information Technology (OIT) agrees that adequate hardware and resources needs to be in place both at agency and at OIT to perform system recovery testing. OIT has already initiated a multi-stage project to identify the hardware and resources required. OIT will need funding and resources to design and architect an infrastructure that will be necessary to ensure that system recovery testing can be performed at an enterprise level.

AUDITOR'S ADDENDUM

It is unclear why implementation of this recommendation will take three years since the recommendation is to evaluate the hardware needs and provide the hardware as resources are available.

ACCESS MANAGEMENT TO BACKUP AND RECOVERY FACILITIES, SYSTEMS, AND DATA

OIT is responsible for following and implementing physical and logical access management processes to backup and recovery facilities, systems, and data. This includes the completion of access forms and processes for adding, changing, or removing access to backup and recovery facilities, systems, and data, and following access documentation retention requirements, account use guidelines, and termination and approval process guidelines identified in policies and procedures.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of our audit work was to evaluate whether the State's backup and recovery facilities and systems that are managed by OIT have sufficient access management processes and comply with applicable access management policy requirements. As part of our audit work, we reviewed the access management processes and controls for a sample of five OIT-managed facilities and systems by performing test procedures on the application, operating system, and database within each system. We interviewed OIT personnel and reviewed OIT policies and procedures to identify the access management requirements. We also reviewed whether OIT has adequate processes to verify that OIT personnel and agencies follow access management requirements and that system controls are designed appropriately and operating effectively.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We applied the following criteria when evaluating the sufficiency of access management processes for backup and recovery facilities and systems that are managed by OIT:

LOGICAL ACCESS RECORDS SHALL BE RETAINED. According to OIT's Access Control policy (P-CISP-008, 7.2.4.2), written records of new access requests, changes, terminations, and transfers shall be retained for all IT systems, including those that perform backup and recovery. The policy requires these written records to be retained for one full year after the term of employment of every individual that has access to the backup and recovery system. Furthermore, the Access Control policy (P-CISP-008, 7.2.4.3) requires the system business owner at the agency to approve or disapprove access requests for each given system. The system owner must grant access to requestors using a "least privilege" methodology. Least privilege means that a user is granted only the minimum access required to perform their job functions.

SYSTEM ACCOUNTS MUST NOT BE SHARED. According to OIT's System and Applications Security Operations policy (P-CISP-007, 7.1.2.5), agencies are to ensure that system individual administration credentials (e.g., username and password, token, and pass phrase) to all IT systems, including systems that perform backup and recovery, are not to be shared between system administrators. Additionally, OIT's Access Control policy (P-CISP-008, 7.2.5.3), requires that use of administrative accounts, such as a "root" or "super-user" accounts are traced back to an individual user. In the event that a "super-user" account cannot be directly traced back to a system administrator, the system administrators must use utilities that allow for individual accountability to perform administration actions. Finally, OIT's Access Control policy (P-CISP-008, 7.2.7.2), requires users to utilize their own individual, unique User IDs when logging in to the agency networks and applications.

PHYSICAL AND LOGICAL ACCESS RIGHTS MUST BE REMOVED FOR TERMINATED OR TRANSFERRED INDIVIDUALS. According to OIT's Access Control policy (P-CISP-008, 7.2.1.1), "Agencies are to develop procedures that ensure staff supervisors immediately notify the Agency's IT group responsible for granting and revoking access upon receipt of a subordinates resignation." In addition, OIT's Access Control policy (P-CISP-008, 7.2.2.2) requires OIT personnel to implement procedures to immediately terminate all facility and system access rights upon notice of termination of personnel.

PHYSICAL ACCESS MUST BE LIMITED BASED ON POLICY REQUIREMENTS. According to OIT's Physical Security policy (P-CISP-010, 3.0), physical access to areas that contain sensitive data such as computer rooms and backup media storage facilities are to be limited to only those authorized personnel who require access to perform assigned duties. Additionally, according to OIT's Physical Security policy (P-CISP-010, 7.4.2.3), "When employment is terminated, all physical access to State of Colorado facilities must be revoked immediately and all physical access tokens (i.e., IDs, keys, magnetic strip cards, etc.) must be recovered." Finally, according to OIT's Physical Security policy (P-CISP-010, 7.4.4.8), card key access is required to gain entry into rooms storing sensitive systems and data. Key code entry is an alternative only if the key code access is combined with video monitoring.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

We identified the following problems regarding access management processes for backup and recovery facilities and systems:

LACK OF SYSTEM ACCESS REQUEST AND APPROVAL. For one of the five systems we tested (System 3), we found one user who did not have proper documentation for access to the backup system. A user access request form was provided for the user in question. However, the form did not indicate that the user should have access to the backup

system and was not signed or formally approved by the user's supervisor.

SHARED SYSTEM ACCOUNTS ARE USED. For two of the five systems we tested (System 1 and System 3), shared administrative accounts are being used to access backup systems.

LOGICAL ACCESS RIGHTS WERE NOT REMOVED FOR TERMINATED EMPLOYEES. For two of the five systems we tested (System 3 and System 5), found three terminated employees had active accounts in the system that is used to manage offsite storage of backup media.

PHYSICAL ACCESS IS NOT RESTRICTED TO AUTHORIZED INDIVIDUALS. For two of the five systems we tested (System 1 and System 3), we determined that former personnel had active access cards to computer rooms that house backup and recovery systems and media. For System 1, three terminated personnel had active access to the computer room that house backup and recovery systems and data. For System 3, eight former personnel (3 terminated and 5 transferred) had active access cards to the computer room that houses backup and recovery systems and data.

For System 3, we also found that the PIN pad code on the door that restricts access to the on-site backup media storage room has not been changed in 8 years. We were unable to determine who has knowledge of the PIN pad code. However, backup and recovery personnel stated that former OIT and agency employees have knowledge of the current PIN pad code since it has not been changed in 8 years.

LOST ACCESS CARDS TO THE COMPUTER ROOM ARE NOT DISABLED. For one of the five systems we tested (System 4), three individuals had two access cards each assigned to them. One of the three individuals had lost an access card, the lost access card was not deactivated, and a second active access card had been issued. In this instance, the access card administrator was notified of the lost access card prior to provisioning the second access card. We were not able to establish reasons why the other two individuals each had two active access cards.

WHY DID THE PROBLEMS OCCUR?

The backup and recovery system access management problems identified above occurred due to the following reasons:

LACK OF AWARENESS OF ACCESS MANAGEMENT POLICIES. Backup and recovery personnel stated that they were not aware of the OIT policies containing access management requirements for OIT-managed facilities and systems, including those related to system access records, shared accounts, and access termination. OIT personnel may not be aware of the policies due to the fact that OIT does not have a consistent procedure in place to ensure that personnel follow access management. In the case of System 1, OIT personnel managing the system did not believe that sharing an account was a problem since only two users knew the administrative login credentials. Additionally, OIT personnel managing System 1 informed us that the system does not allow individual accounts to log into the system administrative account. In the case of the System 3, OIT personnel reported that it was easier to manage the operating system by sharing an administrative account. In addition, no policy training or regular communications regarding current or changed policies was evident.

OIT backup and recovery personnel for System 1, System 3, and System 4 reported that they have been following access management processes that were in place prior to the consolidation of IT services in 2008, and therefore were not following current OIT access management policies.

LOGICAL AND PHYSICAL ACCESS TERMINATION NOTIFICATIONS DID NOT OCCUR. For two of the five systems we tested (System 1 and System 3), the security administrators did not receive termination notifications that terminated physical access to the on-site computer rooms, or, for System 3, change notifications for the PIN pad code for the onsite backup media storage closet. In addition, for System 3, the security administrator responsible for controlling access to the system that is used to manage offsite storage of backup media did not receive the termination notification.

LACK OF REQUIREMENTS WITHIN POLICIES. There are no requirements identified in OIT policies to address processes or controls for lost or stolen access cards or to restrict users from having multiple access cards.

WHY DOES THIS FINDING MATTER?

If access management policy requirements are not followed, or current policies do not identify control requirements to address specific risks—such as those regarding lost or stolen access tokens, access to backup and recovery facilities and systems may not be controlled appropriately. This could result in inappropriate or unauthorized access to backup and recovery systems and data, which in turn, could result in a lack of system and data integrity and availability, a loss of data, or compromised or stolen data.

RECOMMENDATION 6

The Governor's Office of Information Technology (OIT) should ensure that OIT backup and recovery access management processes are effective by:

A Updating policies to include access management requirements and standards to address the risks associated with lost or stolen access cards or tokens and to ensure that access to backup and recovery facilities is restricted appropriately.

B Establishing a process to communicate access management policies to personnel responsible for managing these procedures and holding personnel accountable for implementing the policies.

RESPONSE

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

A PARTIALLY AGREE. IMPLEMENTATION DATE: DECEMBER 2016.

The Colorado Information Security Policies and procedures which include access management policies and associated activities are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all employees. Once the policies are established OIT will review the backup and recovery facilities and ensure access is restricted for the facilities controlled by OIT. There are certain facilities where the access control management lies with agency or third party and they own the execution of access controls. OIT cannot enforce access management controls for the facilities that are not under OIT's authority.

AUDITOR'S ADDENDUM

OIT has oversight of the agencies listed in CHAPTER 1; therefore, the Access Control policies previously mentioned would apply to all agencies on the list. Additionally, it is unclear why implementation of this recommendation will take two years since the recommendation is just to update policies.

B AGREE. IMPLEMENTATION DATE: JULY 2015.

The Governor's Office of Information Technology (OIT) agrees that a process for reviewing, updating, and communicating policies is critical to the business. The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification, are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all OIT personnel and state agencies. Currently any new policies that are approved by the executive leadership team are communicated to all OIT staff through email and also published on OIT's internal website. OIT will enhance its policy communication effort by creating a quarterly update with OIT staff. OIT will implement a biannual operational review for all relevant OIT staff to strengthen accountability and ensure compliance with established policies and procedures. Also OIT will partner with management teams at state agencies to ensure that agencies' personnel are aware of relevant policies.

GOVERNANCE OF IT BACKUP AND RECOVERY PROCESSES

OIT is currently responsible for the operations and delivery of all information technology services, including backup and recovery services, for systems across seventeen Executive Branch agencies. Statute requires OIT and its officers to develop and update policies, procedures, guidelines as well as ensure that policies, procedures and guidelines are communicated and followed when backup and recovery processes are performed. Additionally, OIT is responsible for identifying backup and recovery roles and responsibilities and communicating those roles to OIT personnel. Roles and responsibilities are required to be documented and approved by the appropriate officers on a regular basis.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

The purpose of our audit work was to evaluate whether OIT's governance of backup and recovery processes are sufficient based on governance-related requirements established in statute and policies. As part of our audit work, we reviewed governance processes over backup and recovery operations, which included policy definition, implementation, communication, monitoring, and organizational structure definition and alignment with backup and recovery needs. We interviewed OIT and agency personnel and reviewed state statutes, Code of Colorado Regulations, and OIT and agency policies and procedures to identify governance requirements.

HOW WERE THE RESULTS OF THE AUDIT WORK MEASURED?

We applied the following criteria when evaluating the sufficiency of governance over backup and recovery processes that are managed by OIT:

OIT MUST CREATE POLICIES, STANDARDS, SPECIFICATIONS, AND GUIDELINES FOR BACKUP AND RECOVERY. As part of the Chief Information Officer's duties and responsibilities in overseeing OIT, statute [Section 24-37.5-106, C.R.S.] requires OIT to develop policies, standards, specifications, and guidelines for information technology and related procedures to effectively manage IT. This includes all aspects of system backup and recovery.

THE CHIEF INFORMATION SECURITY OFFICER (CISO) is required to develop and update policies that address system backup and recovery and ensure compliance. Statute requires the CISO to develop and update information security policies, standards, and guidelines (Section 24-37.5-403, C.R.S.). This includes the development of policies related to system backup and recovery. Statute further requires the CISO to ensure compliance with these policies.

Additionally, as established in revised rule C.C.R. 8 1501-5, effective December 2013, the CISO is required to submit a Disaster Recovery Plan Summary as part of an Enterprise Cyber Security Plan (ECSP) by July 15 each year to the Chief Information Officer. Prior to revision of C.C.R. 8 1501-5 in December 2013, according to the rule and OIT's Disaster Recovery policy (P-CISP-004, 8.1), the CISO was required to review and approve agency Disaster Recovery Plans as part of the Cyber Security Plan approval process.

AGENCY IT DIRECTORS ARE REQUIRED TO ESTABLISH BACKUP AND RECOVERY PROCEDURES AND ROLES AND RESPONSIBILITIES. The CISO's Systems and Applications Security Operations policy (P-CISP-007, 7.2.3) requires agency IT Directors, employed by OIT, to

establish backup and recovery procedures, consistent with the CISO's Disaster Recovery policy (P-CISP-004). Additionally, rules (C.C.R. 8 1501-5) require that the ECSP identify roles and responsibilities to carry out the Enterprise Cyber Security Plan, including backup and recovery. Prior to December 2013, each agency was required to annually submit its Agency Cyber Security Plan, including the roles and responsibilities for a Disaster Recovery Plan.

WHAT PROBLEMS DID THE AUDIT WORK IDENTIFY?

Throughout the audit we identified problems related to OIT governance, management, and operations of system backup and recovery processes. These include the following problems:

BACKUP AND RECOVERY CONTROL FAILURES OCCURRED ACROSS FIVE OF THE FIVE SYSTEMS TESTED. As outlined in Exhibit 2.1, and described throughout the other findings in this report, we found failures across six backup and recovery control activities across five of the five systems that we tested. In three control areas, data backup procedures, encryption, and access management, we found control activity failures across all systems tested.

EXHIBIT 2.1. GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY BACKUP & RECOVERY CONTROLS

	System 1	System 2	System 3	System 4	System 5
Agency Data Backup and Recovery Procedures	N/A[1]	✗	✗	✗	✗
Monitoring of Backup and Recovery Processes	✓	✗	✗	✗	✓
Offsite Backup Storage Management	✓	✗	✗	✓	✓
Encryption Requirements for Systems and Media	✗	✗	✗	✗	✗
System Recovery Testing	✗	✗	✗	✗	✓
Access Management to Backup and Recovery Facilities, Systems, and Data	✗	✗	✗	✗	✗

TABLE LEGEND:

✗: The system failed a minimum of one of the test procedures performed for this control activity.

✓: The system passed all test procedures performed for this control activity.

SOURCE: Office of the State Auditor's summary of audit findings by system reviewed.

[1]OIT has a contract with a third party vendor to provide comprehensive IT hardware and software support for System 1. This includes properly configuring the backup procedures for this system. The recovery procedures are maintained and managed by OIT.

OIT Staff do Not Have an Understanding of Current Backup and Recovery Policies. We found a breakdown between OIT management's expectation of backup and recovery requirements as outlined in Colorado Information Security Policies (P-CISPs), and the IT staff's understanding of backup and recovery policies. For the five systems tested, backup and recovery staff were aware that the P-CISPs exist, but were not aware of the backup and recovery requirements within the policies, and were not following the P-CISPs to perform backup and recovery processes. For the five systems tested, backup and recovery staff were performing backup and recovery processes that were in place prior to consolidation of OIT in 2008.

In addition, the agency IT Directors for System 3 and System 4 were aware that the P-CISPs exist but were not aware of the contents in the P-CISPs. The agency IT Director for System 2 was new to the position in late April of 2014 and was not aware of the P-CISPs. While acknowledging that there may be gaps with compliance, the agency IT Director for System 1 reported that he tries to help IT personnel at the agency follow the P-CISPs.

The organizational structures for conducting backup and recovery processes within the agencies are inefficient. The organizational structures for conducting backup and recovery processes within the agencies are inefficient. For three of the five systems we tested (System 3, System 4, and System 5), we found that multiple teams performed different roles within backup and recovery processes for the systems, and that many of the staff within the teams reported to different managers. For example, one team managed the application, another team managed the database, and a third team managed the operating system and servers, but none of them reported to the same manager. Additionally, there were instances in which these various teams did not communicate with one another and were not aware of who their contacts were on the other teams. This organizational structure was a challenge for IT staff to coordinate and perform backup and recovery functions. Finally, agency IT Directors no longer directly manage IT staff. Approximately 2 years ago, their responsibilities for supervising staff were removed; however, the

language in the current P-CISPs requires the agency IT Director to establish data backup procedures. As a result, the agency IT Director can coordinate efforts between teams, but has no authority to require IT staff or their supervisors to comply with data backup procedures.

WHY DID THE PROBLEMS OCCUR?

We found that the problems noted above occurred for the following reasons:

OIT Lacks a Process to Regularly Update, Communicate, and Ensure Compliance of Backup and Recovery Policies. According to OIT management, P-CISPs, including those connected to backup and recovery processes, have been communicated via email. OIT management acknowledged that email communication of policies may not be the most effective way of ensuring that staff understand and follow official policies. In addition, at the time of our audit, the CISO had not updated the P-CISPs in approximately three years and was in the process of updating them but had not finalized them. This has created conflicts within the policies and agency rules, with some policies or rules updated and others not updated. For example, according to OIT's Information Security Planning policy (P-CISP-001 7.9 and 7.10), IT Directors are still required to annually submit agency-specific Disaster Recovery Plans. However, the updated agency rule (C.C.R. 8 1501-5) places the responsibility for submitting disaster recovery plans on the CISO. Finally, the CISO has not ensured compliance with the P-CISPs. The Office of Information Security (OIS) reported that they delayed training personnel on P-CISPs because OIS was in the process of updating the policies and decided to wait to train personnel until the new policies were approved.

Backup and Recovery Roles and Responsibilities are not Formally Defined. The CISO was required to define the roles and responsibilities in the ECSP that was due July 15, 2014. In mid-July 2014 the interim CISO had developed an ECSP. However, as of early October 2014, the ECSP has not been formally submitted to the CIO for approval. Additionally, OIT reported that the Enterprise Disaster

Recovery Plan, which is a component of the ECSP, has not been fully drafted. As a result, no formal roles and responsibilities have been defined at an enterprise level. In addition, agencies have not submitted Disaster Recovery Plans since 2012, and therefore, roles and responsibilities have not been formally identified and provided to backup and recovery personnel.

WHY DOES THIS FINDING MATTER?

When backup and recovery controls are ineffective, policies are not followed, and the organizational structure does not support performing backup and recovery processes adequately, this could lead to critical and essential systems and data not being available as needed when systems fail or disasters occur.

RECOMMENDATION 7

The Governor's Office of Information Technology (OIT) should improve governance over backup and recovery processes by:

A Creating a process for reviewing, updating, and communicating OIT backup and recovery policies to personnel responsible for managing IT backup and recovery processes and establishing a mechanism to hold IT staff accountable for implementing backup and recovery policies and procedures.

B Finalize the ECSP that was due July 15, 2014, including backup and recovery roles and responsibilities within OIT.

RESPONSE

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

A AGREE. IMPLEMENTATION DATE: JULY 2015.

The Governor's Office of Information Technology (OIT) agrees that a process for reviewing, updating, and communicating policies is critical to the business. The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification, are being revised and will be submitted to the executive leadership team for approval. Once approved, these policies will be published and made available to all OIT personnel and state agencies. Currently any new policies that are approved by the executive leadership team are communicated to all OIT staff through email and also published on OIT's internal website. OIT will enhance its policy communication effort by creating a quarterly update with OIT staff. OIT will implement a biannual operational review for all relevant OIT staff to strengthen accountability and ensure compliance with established policies and procedures. Also OIT will partner with

management teams at state agencies to ensure that agencies' personnel are aware of relevant policies.

B PARTIALLY AGREE. IMPLEMENTATION DATE: JULY 2015.

The Governor's Office of Information Technology (OIT) agrees that backup and recovery roles and responsibilities should be defined for all OIT staff. We will implement specific procedures and standards around the backup and recovery process and communicate it to relevant personnel. The roles and responsibilities for backup and recovery are defined within specific policies and procedures. The Enterprise Cyber Security Plan (ECSP) is a high level security plan that will not address the roles or responsibilities for backup and recovery.

AUDITOR'S ADDENDUM

Rules (C.C.R. 8 1501-5) require that the ECSP identify roles and responsibilities to carry out the Enterprise Cyber Security Plan, including backup and recovery.

GLOSSARY

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

TERMS

Critical System

Systems that provide critical data to the public, and serve a vital function to government, but do not affect life-safety and must be recovered within 72 hours to a week of a system failure.

Essential System

Systems where loss or unavailability is unacceptable, due to life-safety issues, and must be recovered within 2 to 24 hours of a system failure.

Executive Branch Agency

All of the departments, divisions, commissions, boards, bureaus, and institutions in the Executive Branch of the state government. This does not include the legislative or judicial department, the department of law, the department of state, the department of the treasury, or state-supported institutions of higher education.

Public Agency

Every state office, whether executive or judicial, and all its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. "Public agency" does not include institutions of higher education or the general assembly.

Recovery

Revert a computer's state (including system files, installed applications, registries, and system settings) to that of a previous point in time, which can be used to recover from system malfunctions or other problems.

System

For the purpose of this audit, the OSA defines a "system" as an application, the application's operating system(s), and the application's database(s).

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