Audit of Three Information Technology Systems at the Colorado Department of Public Health and Environment

Colorado Department of Public Health and Environment
Governor's Office of Information Technology

Information Technology Performance Audit – Public Report
August 16, 2017
Myers and Stauffer LC

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

LEGISLATIVE AUDIT COMMITTEE

Representative Tracy Kraft-Tharp – Chair	Senator Tim Neville – Vice-Chair
Senator Kerry Donovan	Representative Lori Saine
Senator Cheri Jahn	Senator Jim Smallwood
Representative Dan Nordberg	Representative Faith Winter

OFFICE OF THE STATE AUDITOR

Dianne E. Ray	State Auditor
Matt Devlin	Deputy State Auditor
Myers and Stauffer LC	Contractor

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 1676P WHEN REQUESTING THIS REPORT

MYERS AND STAUFFER LC
CERTIFIED PUBLIC ACCOUNTANTS

August 16, 2017

Members of the Legislative Audit Committee:

This report contains the results of an information technology performance audit of three information technology systems at the Colorado Department of Public Health and Environment. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits and assess the security practices of information technology systems of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Colorado Department of Public Health and Environment and the Governor's Office of Information Technology.

We conducted this information technology performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

During our audit work, we identified certain matters that are not included in this audit report that were reported to the Colorado Department of Public Health and Environment and the Governor's Office of Information Technology management in a separate confidential report dated August 16, 2017. These matters were considered sensitive to protecting state information technology assets.

Myers and Stauffer LC

Myers and Stauffer, LC
Austin, Texas

11044 Research Blvd, Ste C-500 | Austin, TX 78759
PH 512.342.0800 | FX 512.342.0820
www.mslc.com

TABLE OF CONTENTS

REPORT HIGHLIGHTS

Audit of Three Information Technology Systems at the Colorado Department of Public Health and Environment (CDPHE)

IT Performance Audit,1676P, August 2017

Colorado Department Of Public Health And Environment (CDPHE)

Governor's Office of Information Technology (OIT)

AUDIT CONCERN

The Governor's Office of Information Technology (OIT) is the Information Technology Service Provider for the Colorado Department of Public Health and Environment (CDPHE). However, CDPHE continues to perform certain IT related functions for the three departmental information systems that were reviewed during this audit. Security controls implemented for these three systems did not comply with all State policy requirements and need to be remediated to ensure the protection of the confidentiality, integrity, and availability of these systems and the data they maintain.

KEY FACTS AND FINDINGS

- OIT does not perform all IT related functions for CDPHE.
- Three information systems did not comply with multiple Colorado Information Security Policy (CISP) and OIT Cyber Policy requirements, and did not comply with several best practice recommendations.

BACKGROUND

The Colorado Department of Public Health and Environment

- CDPHE's mission is to protect and improve the health of Colorado's people and the quality of its environment. CDPHE has multiple divisions and programs. The audit included a review of three information systems that help support CDPHE's mission.

The Governor's Office of Information Technology

- OIT is the State's centralized Information Technology Service Provider responsible for managing information technology resources and staff for CDPHE.
- OIT hosts and manages CDPHE's three information systems that were under review during the audit.
- OIT is also responsible for maintaining the State's IT Security Program and managing Colorado Information Security Policies and OIT Cyber Policy requirements at executive branch agencies, including CDPHE.

OUR RECOMMENDATIONS

The Governor's Office of Information Technology and the Colorado Department of Public Health and Environment should strengthen controls over information technology governance by evaluating whether additional resources should be allocated by OIT in order to fully manage the three CDPHE departmental information systems and to provide sufficient program level knowledge to manage all IT functions. OIT and CDPHE should ensure information systems comply with CISP and OIT Cyber Policy requirements.

FOR FURTHER INFORMATION ABOUT THIS REPORT,
CONTACT THE OFFICE OF THE STATE AUDITOR
303.869.2800 – WWW.STATE.CO.US/AUDITOR

CHAPTER 1

About the Colorado Department of Public Health and Environment (CDPHE or the Department)

The Department serves the people of Colorado by providing high-quality, cost-effective public health and environmental protection services that promote healthy people and healthy places. The Department focuses on evidence-based best practices in the public health and environmental fields and plays a critical role in educating citizens so they can make informed choices. In addition to maintaining and enhancing its core programs, the Department continues to identify and respond to emerging issues that could affect Colorado's public and environmental health.

The Department pursues its mission through broad-based health and environmental protection programs and activities. These include population-based disease prevention strategies, control of disease outbreaks; provision of health statistics and vital records; health facilities licensure and certification; health and wellness promotion for both the general population and specific subpopulations such as children/adolescents, women, workers and the aging; prevention and treatment of sexually transmitted infections and HIV; suicide and injury prevention; laboratory and radiation services; and emergency preparedness. The Department's environmental responsibilities span a full array of activities including air and water quality protection and improvement, hazardous waste and solid waste management, pollution prevention and environmental leadership, and consumer protection.

About the Governor’s Office of Information Technology (OIT)

The Chief Information Officer and Secretary of Technology (CIO) is responsible for the overall administration of OIT, as well as supervising the Chief Information Security Officer (CISO). The state’s CISO is responsible for overseeing the Office of Information Security and the Colorado Information Security Program which includes governance, compliance, and risk management.

With the passage of Senate Bill 08-155, during the 2008 Legislative Session, the state agency information technology (IT) resources, procurement, and the IT service delivery were consolidated under the management of OIT. On July 1, 2008, OIT became responsible for the operation and delivery of technology services across 17 Executive Branch agencies including the Departments of Agriculture, Corrections, Education, Health Care Policy and Financing, Higher Education (excluding institutions), Human Services, Labor and Employment, Local Affairs, Military and Veterans Affairs, Natural Resources, Personnel & Administration, Public Health and Environment, Public Safety, Regulatory Agencies, Revenue, Transportation, and the Governor’s Offices of Economic Development and Energy. The state agencies, departments, offices, and institutions that were not included in the centralization of the state’s IT resources include the Legislative and Judicial Branches, the Departments of Law, State and Treasury, and the state-supported institutions of higher education. However, these agencies may rely on OIT to provide certain IT services or resources, such as data center services and resources, based on C.R.S 24-37.5-602(1)(a).

OIT oversees technology initiatives for the consolidated Executive Branch agencies and recommends strategies to maximize service delivery efficiency in a cost-effective manner through the application of enterprise technology solutions. OIT provides services to state agencies on a cost reimbursement basis acting as a vendor of IT services to State agencies. Services provided by OIT include enterprise application management and support, database management, network security and management, communication technology services, data center operations, information security, help desk services, public safety communications, procurement, project management, IT economic development, geographic

information services, data management, and governance. OIT has assigned IT Directors to the consolidated state agencies, who are primarily responsible for maintaining agency relationships, leading application development, and overseeing the execution and management of IT projects and programs, at their respective state agencies.

The responsibilities of CDPHE and OIT are as shown in Table 1:

Table 1 – CDPHE and OIT Responsibilities

CDPHE	OIT
• As a consolidated agency, the CDPHE is required to use the OIT as its IT service provider and to maintain the Information Security Program requirements for the Department. • The CDPHE Security Officer, Program Managers, and Business Technology Liaisons work with OIT IT Steering Committee members to prioritize projects, maintenance, and personnel resources.	• As described in the Colorado Information Security Policies (CISPs), OIT is responsible for documenting the Information Security Program details in the Enterprise Cyber Security Plan and sets forth security policy for the consolidated agencies in the OIT Information Security Policies, also known as the OIT Cyber Policies. • OIT is the Information Technology Service Provider for all consolidated agencies. • OIT provides security services, which include governance and compliance, security operations, and access control. • OIT provides Hosted Services, which include server hosting, and provides database administration services. • OIT manages the hosted environments. • OIT performs Identity and Access Management services.

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 and assess the security practices of information technology systems of all departments, institutions, and agencies of state government. Audit work was performed from December 2016 through April 2017. We acknowledge the cooperation and assistance by staff and management at the Colorado Department of Public Health and Environment (CDPHE) and the Governor's Office of Information Technology (OIT).

We conducted this IT 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 objectives of the audit were to determine whether appropriate controls were in place and were designed and operating effectively to:

- Align with and support departmental business objectives and operations.
- Ensure that data, information, and reports generated, processed, and maintained by a sample of departmental systems are reliable.
- Ensure that a sample of departmental systems and the information and data they contain are secure.
- Ensure compliance with applicable IT and information security laws, rules, regulations, policies, procedures, standards, guidelines, and industry best practices.

The audit focused on three mission-critical departmental systems that were preselected for inclusion in the scope of this audit.

We performed the following procedures to accomplish our audit objectives:

- Reviewed CDPHE and OIT IT, systems, services, and information security governance, management and operational processes.
- Interviewed CDPHE management and staff.
- Interviewed OIT management and staff.
- Gathered and analyzed documentation and data.
- Evaluated system processes and documentation against policy requirements.
- Performed tests and observations of system and process controls, including security configurations and procedures for monitoring security such as logging, log reviews, and system alerts.

We planned our audit work to assess the design and effectiveness of security, and operation of the three departmental information systems including compliance with applicable IT and information security laws and regulations. The primary sources of criteria for the audit were the Colorado Information Security Policies (CISP) and the OIT Cyber Policies that were in effect starting in 2015.

During our audit work, we identified certain matters that are not included in this audit report that were reported to management in a separate confidential report dated August 16, 2017. These matters were considered sensitive to protecting state information technology assets.

CHAPTER 2

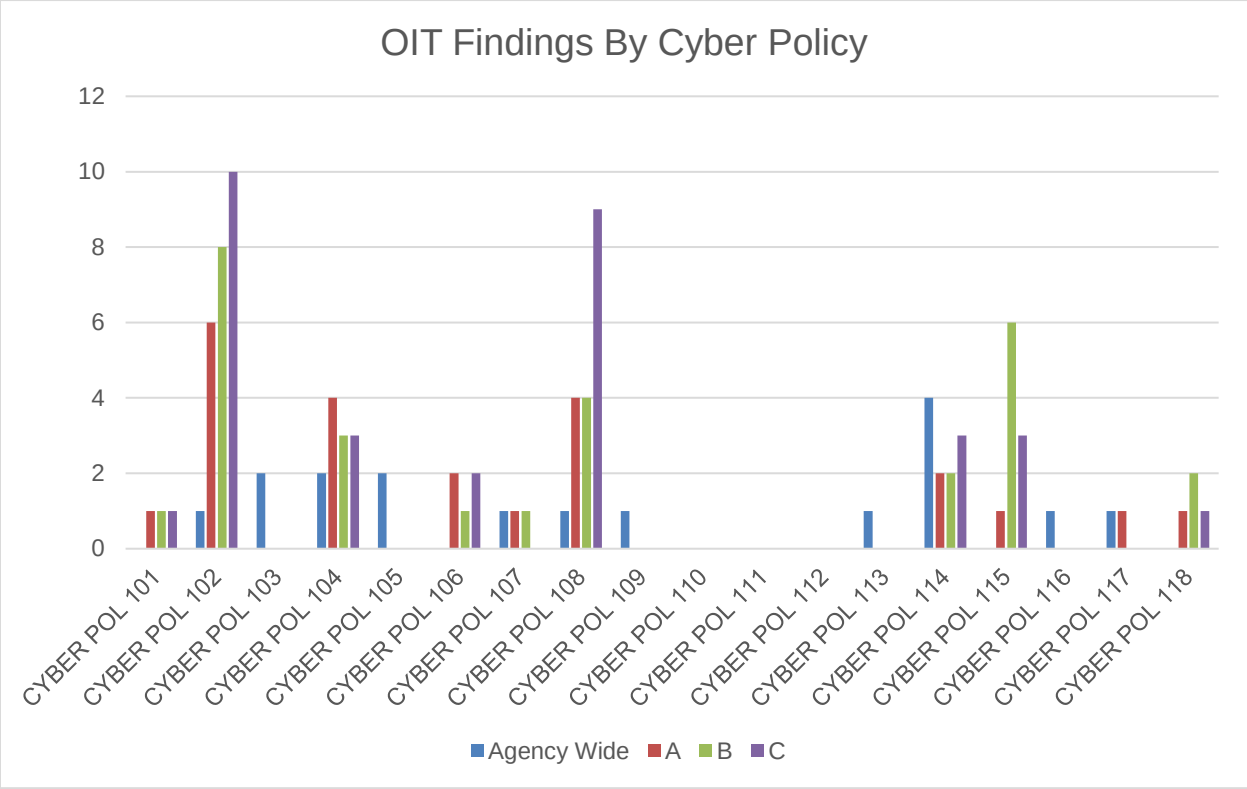
Our audit determined that OIT does not perform all IT related functions for CDPHE, which violates statutory requirements and which may not ensure alignment and support of departmental business objectives and operations. Overall, the three information systems did not comply with multiple Colorado Information Security Policy (CISP) and OIT Cyber Policy requirements, and did not comply with several best practice recommendations. Therefore, the security controls for these systems need to be remediated to ensure the confidentiality, integrity, and availability of the systems and their data. Our audit identified issues in the areas of:

- Information Technology Governance
- Account Monitoring and Control
- Controlled Access Based on Least Privilege
- Data Protection
- Data Recovery Capability
- Incident Response and Management
- Information System Software Security
- Maintenance, Monitoring, and Analysis of Audit Logs
- Secure Configurations for Hardware and Software
- Security Assessment and Remediation
- Security Training
- System Change Management
- System Security Plan
- Vendor Management

The remainder of Chapter 2 describes our findings and recommendations related to the audit at CDPHE. Some of the findings and recommendations presented in this report have been redacted due to the sensitivity of the information. A full description of these findings and recommendations are included in the confidential report dated August 16, 2017.

Figure 1 on the following page depicts the specific issues identified as OIT responsibilities that were not fully compliant with the OIT Cyber Policies for the three systems (identified as A, B, and C in the figure) and at the overall agency level (Agency Wide).

Figure 1



Note: The absence of a bar in the figure indicates that the value is zero (0).

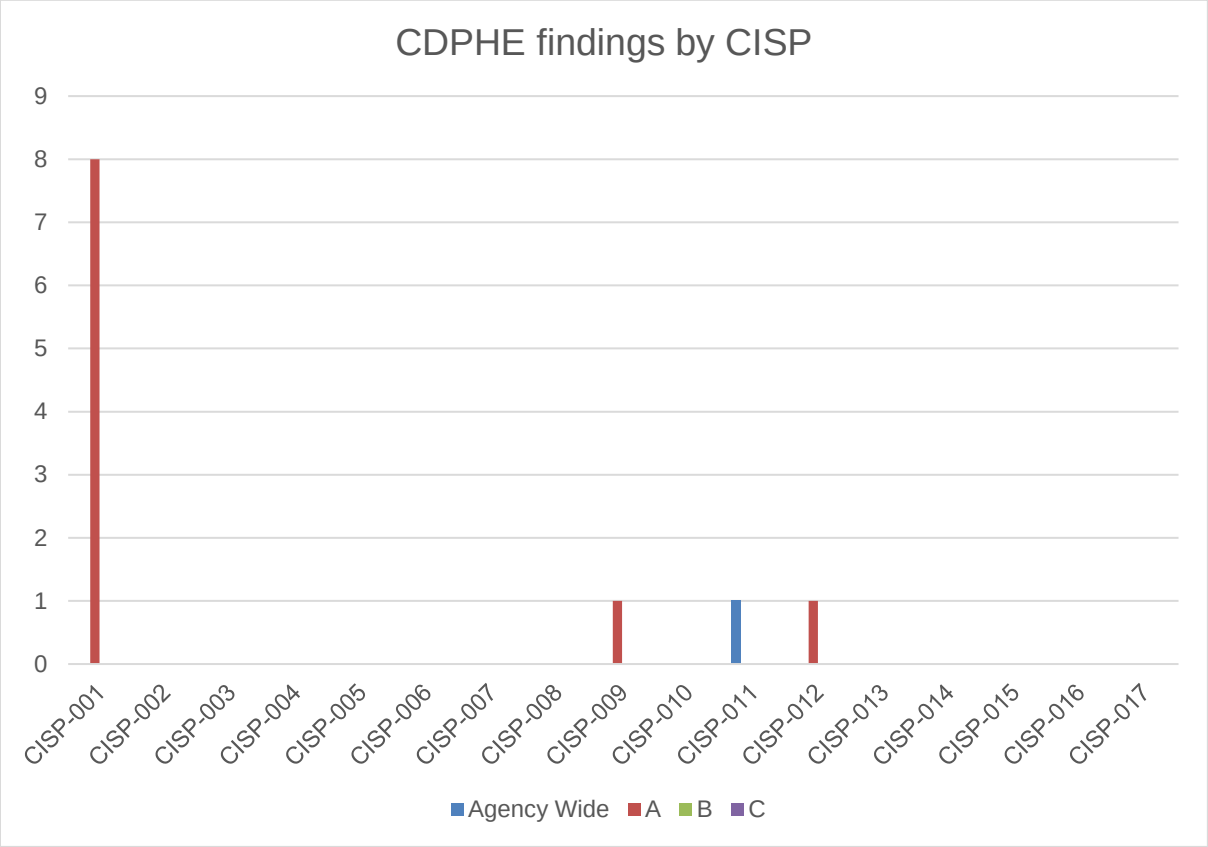
Table 3 – List of OIT Cyber Policy Requirements[1]

Policy Number	Title	Policy Number	Title
CYB-101	Configuration and Patch Management	CYB-110	System Maintenance
CYB-102	Access Control	CYB-111	Media Protection
CYB-103	Security Awareness and Training	CYB-112	Physical and Environmental
CYB-104	Audit and Accountability	CYB-113	Personnel Security
CYB-105	Security Assessment and Authorization	CYB-114	Risk Assessment
CYB-106	Configuration Management	CYB-115	System and Services Acquisition
CYB-107	Contingency Management	CYB-116	System and Communications Protection
CYB-108	Identification and Authentication	CYB-017	System and Information Integrity
CYB-109	Incident Response		

[1]Security policy for the Consolidated Agencies are in these OIT Information Security Policies (called Cyber Policies) which OIT maintains to control risks associated with access, use, storage, and sharing of sensitive citizen and state information.

Similarly, Figure 2 below depicts the specific issues identified as CDPHE responsibilities that were not fully compliant with the CISP's for the three systems (identified as A, B, and C in the figure) and at the overall agency level (Agency Wide).

Figure 2



Note: The absence of a bar in the figure indicates that the value is zero (0).

Table 4 – List of CISP Requirements

Policy Number	Title	Policy Number	Title
CISP-001	Access Control	CISP-010	Media Protection
CISP-002	Security Awareness and Training	CISP-011	Physical and Environmental Protection
CISP-003	Audit and Accountability	CISP-012	Personnel Security
CISP-004	Security Assessment and Authorization	CISP-013	Risk Assessment
CISP-005	Configuration Management	CISP-014	System and Services Acquisition
CISP-006	Contingency and Planning	CISP-015	System and Communications Protection
CISP-007	Identification and Authentication	CISP-016	System and Information Integrity
CISP-008	Incident Response	CISP-017	Security Planning
CISP-009	System Maintenance		

INFORMATION TECHNOLOGY GOVERNANCE

As a consolidated agency, the Colorado Department of Public Health and Environment (CDPHE or the Department) is required to use the Governor's Office of Information Technology (OIT or the Office) as its Information Technology Service Provider (IT service provider) and for providing its Information Security Program. To fulfill its role as the IT service provider for CDPHE, OIT maintains a dedicated IT Director for CDPHE, program level subject matter experts dedicated to CDPHE, and IT personnel who belong to an inter-agency shared resource pool of workers. CDPHE is appropriated funds in the Long Bill, and then re-appropriates the funds to cover OIT costs as listed in the Long Bill. These costs are based upon an amount OIT determines through Common Policy, the methodology, approved by the Joint Budget Committee, used by OIT to allocate IT costs to departments.

OIT's Security Policies were created to support achievement of the Colorado Information Security Act and ultimately to ensure that the information the citizens have entrusted to agencies is safe, secure, and protected from unauthorized access, use, or destruction. We identified control weaknesses indicating CDPHE and OIT were not fully compliant with some requirements related to information technology governance.

What audit work was performed and what was the purpose?

In order to perform our audit work, and in support of the identified findings below, we interviewed OIT management and staff and CDPHE management to determine what processes were in place for implementing IT strategy, policies, standards, and procedures at CDPHE and OIT. Our inquiry included discussions regarding the three systems in scope.

We compared documented CDPHE/OIT IT strategy, policies, standards, and procedures to those described by management to identify differences and/or gaps. We also reviewed IT resource investment and allocation practices including personnel management practices. This included reviewing policies and procedures related to investment, interviewing key personnel responsible for investment decisions, identifying resource investments made over Calendar Year 2016, and reviewing artifacts supporting resource investment decisions and comparing them to expected practices.

We interviewed key CDPHE management personnel responsible for monitoring activities, reviewed evidence that monitoring activities have been performed according to policies and procedures with corrective actions, and reviewed evidence that results (including results of security performance) are being reported to the appropriate executive management and oversight bodies. We interviewed CDPHE and OIT management and staff to determine what processes were in place for ensuring agency-wide policies are kept current and are in compliance with applicable CISP and OIT Cyber Policy requirement. We also observed the CDPHE intranet and reviewed CDPHE IT Security policies to determine whether the policy requirements were aligned with current CISP requirements.

Additionally, we interviewed the appropriate OIT and CDPHE management and staff to understand the processes in place for each of the following specific IT areas and performed further audit procedures as follows:

- **Account Monitoring and Control:** We tested logical account configurations to determine whether accounts are disabled appropriately after a set period of inactivity. For system A, we tested a sample of 20 generic accounts, tested all application privileged accounts, and tested a sample of 23 Site Administrator accounts for compliance with established account management

requirements and for compliance with CISP requirements. We tested the full population of application level and administrator accounts to determine whether accounts were associated with terminated workers. We also observed physical security access controls employed through the CDPHE facility, and observed physical access management system of record operations.

- **Controlled Access Based on Least Privilege:** We observed active accounts on all three system servers, and tested whether the accounts were appropriate based on the account holders job functions for any accounts which did not belong to OIT administrator personnel.
- **Data Protection:** We tested the encryption configurations on various servers and databases. Our testing of the encryption solutions implemented for the three systems included reviewing all components of the encryption solutions used for the applications and comparing the implemented solutions to best practices and recommendations as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52r1.
- **Incident Response and Management:** We reviewed documented incident response plans.
- **Information System Security Software:** We reviewed System Security Plans and project planning documentation; tested password configurations; and observed application administrators performing relevant security tasks.
- **Maintenance, Monitoring, and Analysis of Audit Logs:** We observed audit logs and audit log time sources on a sample of three system A servers, three system B servers, and three system C servers.
- **Secure Configurations for Hardware and Software:** We reviewed CDPHE agency-wide operating system patching and update compliance reports, and we reviewed CDPHE OneView reports, which are generated by OIT and contain agency-wide configuration compliance metrics. We reviewed the patching and operating system update configurations for a sample of servers. We also reviewed the encryption protocols deployed on the CDPHE Virtual Private Network (VPN) service.
- **Security Assessment and Remediation:** We reviewed documented Service Level Commitment services and tested a sample of periodic monitoring reports to determine whether continuous monitoring, risk assessments, security assessments, and vulnerability assessments were being conducted as defined by the CISPs and OIT Cyber Policy requirements.
- **Security Training:** We reviewed and observed cyber security training materials through the state Learning Management System. We also tested training records for a sample of CDPHE and OIT staff who had active user accounts to support the information systems for all three systems to determine whether staff underwent annual cyber security training prior to being given access to these systems.
- **System Change Management:** We reviewed the OIT *Enterprise Change Management Policy and Procedure*. We tested a sample of system A internet application and change tickets associated with code releases and upgrades, and tested change tickets associated with the single change made to system C to determine whether change management activities followed defined requirements.
- **Data Recovery Capability, System Security Plan, and Vendor Management**: We interviewed CDPHE management and staff. We reviewed the system security plans for systems A and B.

What problems did the audit work identify and how were the results measured?

We identified the following problems regarding Information Technology Governance:

1. **OIT does not perform all it related functions for CDPHE.**
    - OIT does not perform all IT related functions for CDPHE, a consolidated agency. CDPHE staff continue to perform certain IT related functions, such as Identity and Access

Management (IAM) for the three systems in scope, and CDPHE staff perform limited server administrator and database administrator functions for systems A and B.

Senate Bill 08-155 was introduced in 2008 which transferred all executive branch agency Chief Information Officers (CIO) to OIT and shifted the reporting structure of agency IT employees to the State of Colorado CIO. The CISPs require that OIT, not CDPHE, be the IT service provider for all consolidated agencies (Purpose statement found in CISP-001 through CISP-017), and CDPHE pays OIT to fulfil all duties as the IT service provider for CDPHE through indirect funds allocated through the Common Policy framework. (Fiscal Year 2016 Service Level Commitment between OIT and CDPHE.)

2. **CDPHE IT policies are out of date.**
    - CDPHE has a repository of agency-wide IT policies which are out-of-date, and may conflict with current CISP and OIT Cyber Policy requirements. Twenty-two of the sample of 24 CDPHE agency-wide IT policies we examined had not been reviewed or updated by CDPHE management in over one year, and did not include, explicitly or by reference, current CISP and OIT Cyber Policy requirements. Additionally, the CDPHE Incident Response policy on the CDPHE intranet is outdated and does not reflect current OIT Incident Response Plan requirements.

      The CISPs require that OIT, not CDPHE, set forth security policy for Consolidated Agencies in the OIT Information Security Policies, and CISPs have been updated as recently as February 2017. (Purpose statement found in CISP-001 through CISP-017)
3. **OIT is not in compliance with all CISPs.**
    - **Account Monitoring and Control**
        i. As the IT service provider for CDPHE, OIT is responsible for providing identity and access management services for all CDPHE information systems and for providing access management help desk functions, such as account creation, password resets, and account lockout services. The OIT Identity and Access Management team performs IAM services for the system B and system C systems. CDPHE assigns the specific application access rights for system B and manages subsequent changes for system C. Additionally, CDPHE independently performs all identity and access management functions for system A within the application. We identified control weaknesses indicating OIT and CDPHE were not fully compliant with some requirements related to account monitoring and control.
    - **Controlled Access Based on Least Privilege**
        i. OIT is responsible for the principle of least privilege. The principle of limiting access to “the least privilege” means that access to the information must be necessary for the conduct of one's official duties. The aim is to make it difficult for unauthorized access to occur, without inconveniencing legitimate access. Least privilege also aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to controlled access based on the principle of least privilege.
    - **Data Protection**
        i. OIT provides services which include data protection and encryption services for hosted information systems. Although CDPHE maintains that they are not required to adhere to Health Insurance Portability and Accountability Act (HIPAA) provisions, CDPHE management stated that the agency maintains HIPAA

compliance in practice given the sensitive nature of the data entrusted to the agency including health-related information and personally identifiable information. Encrypting sensitive data while in storage or in transit is critical to maintaining confidentiality and integrity of an information system's data and essential for maintaining reliability of the system's data. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to data protection.

- **Data Recovery Capability**
    i. OIT provides services which include data recovery capability services. Ensuring that data and information systems can be recovered from a disaster or during contingency efforts is essential for relying on critical information systems. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to data recovery capability.
- **Incident Response and Management**
    i. OIT provides services which include incident response and management. Effective incident response and incident management efforts are important to correct identified computer, privacy, or other security related incidents to reduce the harmful effects of such situations which may impact the accuracy, completeness, and validity of the data provided by an information system. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to incident response and management.
- **Information System Security Software**
    i. OIT provides services which include providing controls enforcing information system software security, this includes enforcing security controls, developing a security architecture for information systems, and ensuring a secure software development lifecycle in accordance with the security categorization for the information system. The security categorization of an information system is based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of the information system would have on operations, assets, other organizations, and the State. This assessment would result in classifying the information system would then be classified with a Public, Low, Moderate, or High security categorization; and this categorization would be a factor in determining the types of security controls needed for the information system. Effective information system software security controls are important to maintain the established processes required to meet CDPHE business objectives and to maintain the confidentiality, integrity, and availability of data for an information system. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to information system software security. Additionally, OIT provides services include security and compliance oversight, and these services include maintenance of System Security Plans (SSP) for all production information systems. An SSP for an information system describes the security controls in place or planned to meet the security requirements of the information system. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to system security plans.

- **Maintenance, Monitoring, and Analysis of Audit Logs**
    i. OIT provides services which include maintenance, monitoring, and analysis of audit logs. These services include employing automated tools to support near real-time analysis of events. Security Information and Event Management controls are essential tools for efficiently detecting and correcting security events throughout an enterprise which may impact the accuracy, completeness, and validity of the data provided by an information system. Effective auditable event management is essential for efficiently detecting security events and unauthorized access in an information system. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to maintenance, monitoring, and analysis of audit logs.
- **Secure configurations for Hardware and Software**
    i. OIT provides services which include server administration and database management. Employing secure configurations for hardware and software is critical to protect against newly discovered weaknesses and for ensuring the configuration requirements defined in an organization's information security program are consistently enforced. OIT also provides services which include flaw remediation services, such as patching and managing operating system updates on hosted information systems. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to secure configurations for hardware and software
- **Security Assessment and Remediation**
    i. OIT provides services, which include continuous monitoring of the CDPHE information security program, conducting security assessments, risk assessments, vulnerability assessments, and managing security related remediation efforts for all CDPHE information systems and resources. Well defined and formalized continuous monitoring efforts are essential to proactively identifying weakness in an organization's IT strategy and is essential for maintaining the health of an organization's Information Security Program. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to security assessment and remediation.
- **Security Training**
    i. OIT provides cyber security training to all state workers. Periodic security training is essential to the successful implementation of an organization's IT strategy and for effective enforcement of an organization Information Security Program. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to security training.
- **System Change Management**
    i. OIT provides services which include providing system change management. Having sufficiently designed and operating change management controls is important to maintain the accuracy, completeness, and validity of data for an information system and essential to ensuring systems are reliable. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to system change management.
- **Vendor management**
    i. OIT provides services which include oversight of third party information system service providers and development vendors. Effective vendor monitoring controls help to ensure that the systems and data entrusted to the State by the citizens of

Colorado are secured when third-party service providers and developers are used. We identified control weaknesses indicating OIT was not fully compliant with some requirements related to vendor management.

Why did the problems occur?

We identified the following causes for the problem identified:

1. **OIT management stated that it does not have sufficient resources to fully manage all CDPHE applications.**
    - OIT management stated that in many OIT service areas, OIT does not have enough staff to fully manage all CDPHE applications.
    - Throughout the audit, OIT management stated that the OIT Teams do not have sufficient resources to implement recommendations (listed by Team):
        i. **OIT Identity and Access Management (IAM) Team**
            - OIT Management stated that staffing levels are not sufficient to enforce all OIT Cyber Policy requirements or to develop formal processes to enforce the requirements.
        ii. **OIT Security Operations Team**
            - OIT Management stated that:
                a. Staffing levels are not sufficient to enforce all OIT Cyber Policy requirements or to develop formal processes to enforce the requirements.
                b. Resources are not sufficient to perform security assessments on older applications.
                c. Although the OIT Security Operations team is responsible for maintaining a continuous monitoring strategy and is responsible for performing risk assessments, security assessments, and vulnerability assessments for all CDPHE information systems and resources; the team is not sufficiently staffed to enforce all OIT Cyber Policy requirements.
                d. OIT only has sufficient resources to fully manage information systems which have gone through the due diligence process.
                e. The OIT Security Operations team is responsible for maintaining a continuous monitoring strategy, and is responsible for performing risk assessments, security assessments, and ongoing vulnerability assessments for all CDPHE information systems and resources, but they are not sufficiently staffed to fully enforce the related Cyber Policies.
                f. The OIT Security Operations team is responsible for maintaining the training materials provided in the annual cyber security training and for managing security training for all state workers; but because of the limited number of staff in the Security Operations Team, the current security awareness and training program has not been enhanced to include awareness and training content on the CISP and OIT Cyber Policies including formal training programs. Also because of limited resources, the security awareness training program has not been enhanced to include monitoring and oversight activities to be conducted by

OIT Security Operations team members or a formal monitoring process to ensure training is completed.

g. OIT Security Operations team is not sufficiently staffed to monitor compliance with Cyber Policies.

iii. **OIT Infrastructure Services Team**

- OIT Management stated that:
  a. The OIT Infrastructure Services team assigned to system A includes one worker who primarily manages system A changes and maintenance and acts as a liaison between CDPHE and the system A vendor. Given current workloads, one worker is not sufficient to ensure the system A components fully enforce OIT Cyber Policy requirements.
  b. The OIT Infrastructure Services team assigned to system A includes one worker who primarily manages system A changes and maintenance. CDPHE acts as the liaison between OIT and the system A vendor. The OIT Infrastructure Services team assigned to system B has not historically included dedicated workers to system B. System B IT administrators have historically been a combination of CDPHE personnel and OIT personnel. The OIT Infrastructure Services team assigned to system C has not historically included dedicated workers to the system C. System C IT administrators have historically been a combination of CDPHE personnel and OIT personnel, and the system C vendor has generally conducted all change activities. Therefore, a formal process to review production changes for adherence to OIT Cyber Policy and OIT agency policy, including the *OIT Enterprise Change Management Policy and Procedure*, has not been implemented.

2. **OIT management represented that OIT does not have sufficient program level knowledge to manage all it functions.**
   - OIT management represented that CDPHE personnel who conduct IT related functions, known as "shadow IT", are typically workers with a high degree of program level experience and knowledge who managed relatively small IT functions, such as database management or management of user account access rights (privileges). OIT personnel do not have the high degree of program level knowledge to perform these functions such as assigning user account access rights for specific applications.
3. **OIT lacks formalized processes to implement CISPS and HIPAA requirements.**
4. **CDPHE management stated that the agency does not have the resources to complete a clean-up review of CDPHE intranet policies.**
   - CDPHE management stated that, since consolidation, some subject matter experts and resources, which previously assisted with the Agency's policy and procedure development, became OIT employees and are no longer available to carry-on this responsibility. Additionally, OIT previously staffed members of the OIT Security Operations team at the CDPHE facility which contributed to timely policy and procedure updates and review; however, these personnel are no longer located at the CDPHE facility which has made them less accessible to complete policy and procedures updates.
5. **CDPHE management stated that it was not aware that agency-wide policy and procedures must adhere to current CISP**.

- CDPHE Management was also not aware that agency-wide documentation must be aligned with OIT Cyber Policies for areas where OIT holds Information Security Program responsibilities.

6. **CDPHE policies and procedures are not periodically reviewed.**
    - A process has not been developed to review agency policies and procedures for compliance with CISP or OIT Cyber Policy requirements.

Why do these problems matter?

CDPHE pays OIT through indirect cost allocation and these funds are allocated by OIT using the Common Policy framework. CDPHE may be paying OIT for services that CDPHE employees are performing. Because funding to OIT occurs through indirect cost allocation, it is not possible to determine the funding amount associated with the specific services performed by CDPHE employees. We could not determine if an overpayment to OIT was made for CDPHE employees performing IT-related services. Additionally, IT personnel at CDPHE who perform IT functions may not be sufficiently trained to follow CISP or OIT Cyber Policy requirements, may not receive periodic security and incident response training to the extent it is provided to OIT staff, and may have elevated privileges in production environments, without adhering to OIT Cyber Policy defined requirements. IT personnel at CDPHE who perform IT services may create elevated areas of risk to the security of CDPHE information systems if they are not trained to implement the CISP requirements, and the activities performed by CDPHE personnel may not be monitored by OIT IT security operations personnel.

CDPHE and OIT are not following statutory requirements as laid out in the 2008 consolidation bill which may limit the ability of the State of Colorado to achieve the intent and vision of the legislation to meet operational efficiency, cost savings, and other measures included in the bill.

The Security Policies were created to support achievement of the Colorado Information Security Act and ultimately to ensure that the information the citizens have entrusted to agencies is safe, secure, and protected from unauthorized access, use, or destruction. The State and citizens of Colorado cannot be certain that information is being adequately secured if Security Policies are not followed consistently between the CDPHE and OIT. Without periodic, timely, and consistent reviews of agency-wide policies for alignment with CISPs and OIT Cyber Policy requirements, consistency cannot be achieved.

RECOMMENDATION 1:

The Governor's Office of Information Technology (OIT) should strengthen controls over information technology governance at CDPHE by

a. Re-evaluating resource allocation and determine if more resources should be allocated to CDPHE IT needs, including the coverage of program level IT functions.
b. Developing, documenting, and implementing formal processes to ensure compliance with all Colorado Information Security Policies and HIPAA requirements.

RECOMMENDATION 2:

OIT should develop, document, and implement formal processes to monitor and perform oversight activities for CDPHE workers who conduct IT related functions as the IT service provider for CDPHE.

RECOMMENDATION 3:

The Colorado Department of Public Health and Environment (CDPHE) should work with the Governor's Office of Information Technology (OIT) to strengthen controls over Information Technology Governance by developing, documenting, and implementing a formal process to:

a. Periodically review agency-wide policy and procedure documentation for alignment with CISP and OIT Cyber Policy requirements. This review should include coordinating with OIT Security Operations and/or OIT Chief Information Security Officer's team members to ensure agency-wide policy requirements do not conflict with current CISP or OIT Cyber Policy requirements.
b. Update the policy documentation found on the CDPHE intranet based upon the results of the review. CDPHE should remove outdated agency-wide policies and agency-wide policies that have been superseded by OIT policy.
c. Utilize OIT training that incorporates, explicitly or by reference, CISP and/or OIT Cyber Policy requirements into policy and training efforts to further provide awareness of the State and OIT requirement and to aid in ensuring alignment is achieved.

Response:

Governor's Office of Information Technology (OIT)

RECOMMENDATION 1:

a. **Agree. Implementation Date: DECEMBER 2017.** The Governor's Office of Information Technology agrees to the finding on strengthening controls over IT governance at CDPHE by re-evaluating and/or allocating additional OIT resources to relieve CDPHE employees from performing OIT-related work. The resource issue is being addressed by CDPHE as one of three Agency Selected Services within their FY18 Service Level Commitment with OIT, one entry that will work to address this issue over three years per the following plan: Year one (FY18): Discovery - Find out which CDPHE employees are doing which OIT work and why; Year two (FY19): Plan - create a plan to address what was found in year one and start formulating requests for resources; Year three (FY20 or FY21) depending on the success of the work in the previous two years): Act - act on the items in the plan from FY19 if resources are available.
b. **Partially Agree. Implementation Date: DECEMBER 2017.** The Governor's Office of Information Technology acknowledges the finding and partially agrees to the finding because Colorado Information Security Policies speak to the HIPAA requirement and CDPHE has some internal policies referencing HIPAA; however it is important to illuminate that CDPHE is not a HIPAA covered entity. Therefore, the Governor's Office of Information Technology agrees to developing, documenting, and implementing formal processes to ensure compliance with all Colorado Information Security Policies but not to HIPAA requirements.

Auditor's Addendum

1.b. The auditor agrees, as noted within the body of this report, that CDPHE maintains it is not required to adhere to HIPAA, but reiterates that the agency endeavors to maintain HIPAA compliance in practice given the sensitive nature of the date entrusted to the agency. Therefore, the sensitive data in CDPHE systems are at an increased risk to exposure that violates HIPAA requirements if formalized processes do not include HIPAA requirements. Additionally, it should be noted that the Governor's Office of Information Technology agreed to the recommendation to make technical database changes to meet HIPAA requirements as noted in the response for recommendation 7a of the confidential report.

Response:

Governor's Office of Information Technology (OIT)

RECOMMENDATION 2:

Agree. Implementation Date: JULY 2018. The Governor's Office of Information Technology agrees with the finding and will work with the agency to establish suggested processes to monitor and perform oversight activities for CDPHE workers who conduct IT functions.

Response:

Colorado Department of Public Health and Environment (CDPHE)

RECOMMENDATION 3:

a. **Agree. Implementation Date: DECEMBER 2017.**
The Department is familiar with OIT's cyber security requirements only insofar as those requirements have been included in required quarterly cyber security training, but was unaware of the OIT CISP policies. Department staff will review our security policies in conjunction with the OIT CISP and Cyber policies to determine alignment, and will establish a continuing review process for these policies as OIT policies are revised.

b. **Agree. Implementation Date: JUNE 2018.**
In conjunction with our review of the OIT CISP and Cyber policies, the Department will make corresponding changes to existing CDPHE policies that are still needed and will eliminate policies that are no longer needed.

c. **Agree. Implementation Date: DECEMBER 2018.**
The Department will work with OIT to obtain training on security standards for staff performing any IT related functions.

   If OIT is unable to provide such training, the Department will work within its limited resources and expertise to create and provide appropriate training.

GLOSSARY 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.

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).

Access Control

Access controls are typically logical controls designed into the hardware and software of a computing system. Identification is accomplished both under program control and physical controls.

Audit Log

A chronological record of information system activities, including records of system accesses and operations performed in a given period.

Authorization

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the State based on the implementation of an agreed-upon set of security controls.

Compensating Security Controls

The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization.

Configuration Control

Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

Configuration Management

A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

External Information System Service Provider

A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.

Information Owner

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Risk

The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the State due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Malicious Code Malware

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Network

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Privileged User

A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Risk Assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the State, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

System Security Plan

Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Vulnerability Assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.