SAP Information System
Department of Transportation

Information Technology Audit
June 2010

OFFICE OF THE
STATE AUDITOR

LEGISLATIVE AUDIT COMMITTEE
2010 MEMBERS

Senator David Schultheis
Chair

Senator Lois Tochtrop
Vice-Chair

Senator Morgan Carroll
Representative Jim Kerr
Representative Frank McNulty
Representative Joe Miklosi
Senator Shawn Mitchell
Representative Dianne Primavera

OFFICE OF THE STATE AUDITOR

Sally Symanski
State Auditor

Dianne Ray
Deputy State Auditor

Jonathan C. Trull
Legislative Audit Manager

Annette Argo
Julie Chickillo
Rosa Olveda
Manjula Udeshi
Legislative Auditors

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

STATE OF COLORADO

Sally Symanski, CPA
State Auditor

OFFICE OF THE STATE AUDITOR
303.869.2800
FAX 303.869.3060

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

June 23, 2010

Members of the Legislative Audit Committee:

This report contains the results of an information technology audit of the Department of Transportation's SAP information system. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Department of Transportation and the Governor's Office of Information Technology.

Sally Symanski

Glossary of Terms and Abbreviations

ACS – Affiliated Computer Services, Inc. The vendor supporting the Department's SAP information system.

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

COFRS – Colorado Financial Reporting System. The financial information system that maintains the official accounting records for Colorado state government.

CPPS – Colorado Personnel and Payroll System. State system that maintains data on employee demographics, employee salaries, and job classifications.

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

Department – Colorado Department of Transportation. A principal department within the Colorado state government responsible for planning and implementing the State's transportation system. As part of its mission, the Department conducts traffic safety planning and analysis and implements projects to improve roadway safety.

Enterprise Resource Planning System – an information system designed to integrate and streamline an organization's business processes, including accounting, purchasing, human resources, and other functions.

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

FMIS – Fiscal Management Information System. The Federal Highway Administration's system for managing federally funded highway projects within the Federal-aid Highway Program.

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

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

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

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

IT – information technology.

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

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

SAP – Systeme, Anwendungen, Produkte (German for Systems, Applications, and Products). The proprietary, integrated enterprise resource planning software developed and owned by SAP AG, a German software development and consulting corporation.

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

SAP Information System

Background

The Colorado Department of Transportation (Department) is responsible for planning, operating, maintaining, and constructing the state-owned transportation system. Specifically, these responsibilities include operating the State's highway system, managing highway construction projects, and maintaining the statewide aviation system plan. The Department is one of state government's largest employers, with more than 3,000 full-time equivalent (FTE) staff.

The Department's Fiscal Year 2009 revenue totaled almost $1.4 billion, including about $507 million (36.7 percent) in federal funds, $873 million (63.1 percent) in cash funds, and $3 million (0.2 percent) in cash funds exempt. Financing for construction and other expenditures comes from the Federal Highway Administration, the Department's portion of the State Highway Users Tax Fund, local entities, and aviation-related taxes. In Fiscal Year 2009, the Department expended approximately $1.3 billion, with about 74 percent related to construction. The Department is responsible for establishing internal controls to accurately account for, track, and report on its use of all funds.

Prior to April 2006, the Department relied on 60 different outdated legacy information systems to manage its operations. Based on evolving business needs and the costs associated with maintaining existing systems, Department management decided to procure and implement an enterprise resource planning system to consolidate its primary business functions—including accounting and budgeting, human resources, time entry and payroll, project management and reporting, highway maintenance, and procurement—into one modern, adaptable system. The Department selected SAP for this modernization initiative. As of November 2007, the Department officially completed the rollout of SAP for a total cost of approximately $38 million. The Department reports that the ongoing budget for the operation and development of SAP is approximately $9 million annually, including state personnel and contract staff, computer operations (software, power, security), and new capital purchases (i.e., hardware).

Every division and workgroup within the Department uses and relies upon SAP to accomplish essential business functions. The system's almost 3,200 users are located throughout the state and depend on SAP to provide up-to-date and accurate information. Additionally, SAP interfaces or sends critical financial, payroll, and highway project data to state and federal systems and agencies,

including to the Colorado Financial Reporting System (COFRS), Colorado Personnel and Payroll System (CPPS), and the Federal Highway Administration's Fiscal Management Information System (FMIS).

Authority, Purpose, and Scope

This audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. Compromise of the confidentiality, integrity, or availability of the data maintained and processed in SAP could negatively impact the Department's and State's ability to process payroll, issue warrants, or provide accurate financial statements. Such an event could also hamper the federal government's ability to monitor, track, and approve federal highway transportation projects in Colorado. Because of SAP's importance to the state and federal governments and the large dollar amount of transactions processed through SAP, the Office of the State Auditor performed an information technology audit of the SAP information system, including the Department's supporting infrastructure. We evaluated and tested the following aspects of the Department's information technology network and SAP:

General computer controls, which relate to security management, access controls, configuration and change management, segregation of duties, and contingency planning. General computer controls relate to the environment within which computer-based applications are developed, maintained, and operated. The objectives of general computer controls are to ensure the proper development and implementation of computer applications like SAP and the confidentiality, integrity, and availability of program and data files.

Application-level controls over the expenditure module in SAP, which are those controls unique to SAP that help ensure transactions are complete, accurate, valid, confidential, and available.

As part of the audit, we reviewed policies and procedures; interviewed key personnel; examined system configurations; reviewed computer-generated reports; and used automated computer security evaluation software to test security over the Department's network, servers, and databases related to SAP. The audit work was performed between September 2009 and April 2010 and was conducted 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.

The remainder of the report is divided into two sections. The first section provides descriptive information about SAP and identifies and defines the Department's and the Governor's Office of Information Technology's (OIT's) management and oversight responsibilities. The second section discusses our specific findings and recommendations.

SAP Infrastructure

SAP is an enterprise resource planning system designed to automate and integrate the majority of the Department's business processes by sharing common data and automating routine transactions based on programmable system modules. As of the completion of our audit, the Department had upgraded to and was running SAP ECC 6.0, the most current version of SAP. The Department has deployed the SAP system in a Microsoft environment and is currently running Microsoft Server 2003 and Microsoft SQL Server 2005 on its primary production server. To effectively manage the security and availability of SAP, it is important that information system controls be established and implemented at each tier or layer of the system's architecture. As shown in the figure on page 4, SAP is based on a three-tiered client/server model that includes the following tiers:

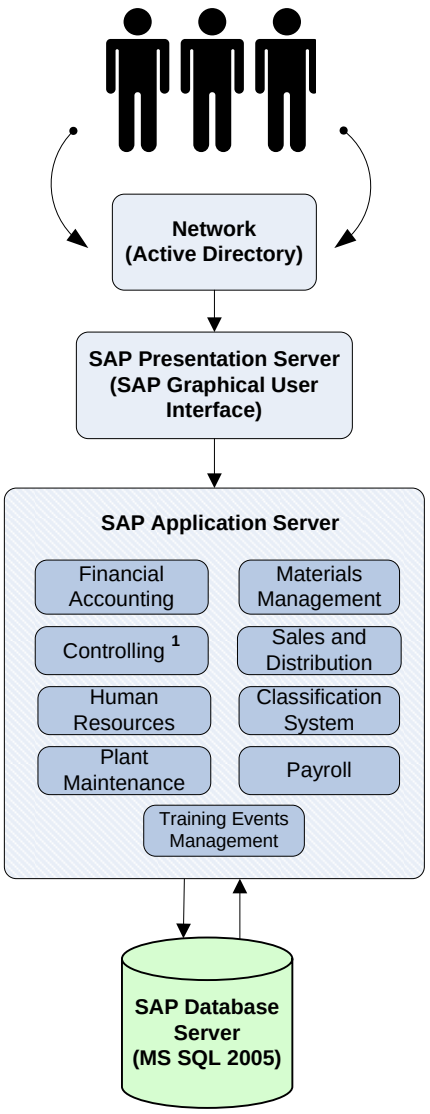
- **Presentation Server** (SAP Graphical User Interface). After a user logs onto a Department computer, the user clicks on a desktop icon or selects the appropriate menu path to access the SAP Graphical User Interface, which accepts user input and sends requests to the application server to be processed. The application server processes the user's requests and sends the results back to the SAP Graphical User Interface to format and properly display the results for the user.

- **Application Server.** The application server collectively interprets SAP's Advanced Business Application Programs. These programs are typically grouped within modules that reflect the business functions they are designed to automate, such as financial accounting, human resources, procurement, and payroll. If an Advanced Business Application Program needs to interact with the SAP database, the application server will format the request and send it to the database server.

- **Database Server.** The database server is the part of the SAP system where the actual data related to the various program modules reside. The database server is responsible for processing requests submitted by the application server to add, retrieve, or modify SAP data.

The following diagram depicts SAP's client/server model.

SAP Client/Server Architecture



Source: Office of the State Auditor analysis of Department and SAP information.

[1] The Controlling module provides supporting information to management for the purpose of planning and reporting, as well as maintaining operations. Includes information on costs and revenues, costs incurred by division, and job/project costs.

Department and OIT Management and Oversight

SAP is maintained and supported by 24 FTE who report through different Department IT business support groups to the Department's Chief Information Officer (CIO). With the passage of Senate Bill 08-155, the Department's CIO reports directly to the Agency Services Director at the Governor's Office of Information Technology, who in turn reports to the State Chief Information Officer (State CIO). Although OIT has oversight responsibility for the Department's IT systems, the Department maintains responsibility for funding SAP operations and providing the strategic direction or identifying the business needs for future SAP enhancements. On July 1, 2010, all Department IT staff will be transferred to OIT as part of the statewide IT consolidation initiative under Senate Bill 08-155.

The following is a brief description of the different work groups and organizations supporting SAP. These groups and organizations are listed in the organizational chart on page 6:

- **State CIO (OIT):** administrative head of OIT responsible for the management, administration, and oversight of state agency information technology resources, such as SAP, and other IT projects.

- **Agency Services Director (OIT):** member of OIT's Executive Leadership Team responsible for overseeing the IT services provided to each state agency.

- **State Chief Information Security Officer (OIT):** responsible for establishing and enforcing State Cyber Security Policies, network monitoring, vulnerability and threat identification and mitigation, and incident response.

- **Department CIO:** head of all IT operations at the Department, including the support, maintenance, development, and operation of the SAP system. The Department CIO reports to the OIT Agency Services Director.

- **Department Deputy CIO:** responsible for providing, managing, and maintaining the technology infrastructure for the Department, including non-SAP application design and development, workstation and network support, and vendor management. The Application Development (non-SAP), Infrastructure Operations, and Information Security groups report directly to the Department's Deputy CIO.

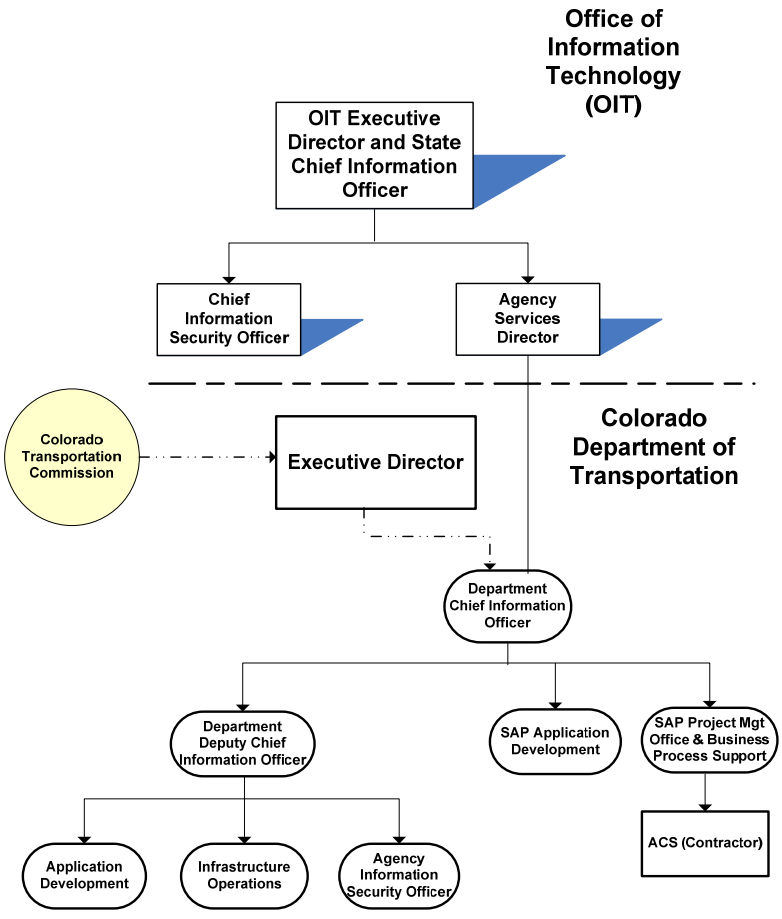
- **SAP Project Management Office and Business Process Support:** promotes overall project management for SAP, including configuration

management, training, and vendor management, and functions as a liaison between the Department's information technology and business divisions. The SAP Project Management Office and Business Process Support report to the Department CIO.

- **SAP Application Development Group:** responsible for the development and maintenance of the SAP Advanced Business Application Programs and interfaces with other information systems such as COFRS and CPPS. The SAP Application Development Group reports directly to the Department's CIO.

- **Affiliated Computer Services, Inc. (ACS)**: Department contractor responsible for the development and maintenance of SAP programs and for training Department staff on the use and support of SAP.

SAP Oversight Structure



Source: Office of the State Auditor analysis of Department organizational chart.

Summary of Findings

Our audit found that the Department had designed and effectively implemented system controls for change management and virus protection related to the SAP information system. However, our audit identified three significant deficiencies and two control deficiencies related to the Department's network and SAP, which are listed below. (See Appendix A for an explanation of significant deficiency and control deficiency.) Specifically, we found that:

- The Department lacks an intrusion detection system and sufficient procedures and processes for responding appropriately to IT security incidents. Also, the Department does not sufficiently log network and system activity or review existing logs to identify and respond to attacks or anomalous activity.

- The Department needs to improve controls related to user access, including system configuration settings related to password length, complexity, and expiration.

- The Department has not completed a SAP disaster recovery plan or tested the plan as required by State Cyber Security Policies and industry best practices.

- The Department is not performing periodic IT security assessments and keeping state-required information security documents up to date.

- The Department is not performing annual security awareness training.

In the remainder of this report, we discuss these problems, starting with significant deficiencies.

Incident Identification and Response

The first significant deficiency concerns the Department's lack of adequate controls over unauthorized attempts to access the Department's network and SAP system. State agency systems are continually at risk of being exploited by cyber attacks that could allow attackers to control state IT systems or gain access to confidential information. For instance, SAP houses confidential data, such as employee payroll information and contractor and financial data that could be vulnerable to a cyber attack if it is not properly safeguarded. To detect and respond to cyber security incidents, agencies need to develop a comprehensive and layered system of network and application controls, including automated intrusion detection; incident response policies, procedures, and training; network and application-level logging; and automated and/or manual log analysis.

We assessed the Department's capabilities for detecting and responding to cyber security incidents related to its network and the SAP system. Overall, we found that the Department lacks the necessary infrastructure, procedures, and practices to effectively identify and respond to a cyber security incident. In the following sections, we discuss specific issues we identified related to intrusion detection and response and network and system logging.

Intrusion Detection and Response

Intrusion detection is a combination of tools and processes used to detect unauthorized use of or unusual activity on systems and networks. State Cyber Security Policies require that all public agencies implement intrusion detection capabilities. Industry best practices recommend that an automated intrusion detection system be utilized when possible. An intrusion detection system is a network device or combination of devices that continuously monitors network traffic to detect probes, unauthorized access, denial-of-service attacks, viruses, malware, and other forms of malicious attacks. Once an attack is identified, the intrusion detection system will automatically alert IT security staff of the incident and provide a history of the network traffic that triggered the alert. Although the Department has requested funding for an intrusion detection system, these requests have been unsuccessful. The Department estimates that an intrusion detection system would cost approximately $700,000 to implement. However, the Department may be able to use the State's enterprise intrusion detection system which could help reduce the cost of implementing such a system at the Department.

Network and System Logging

In conjunction with an automated intrusion detection system, it is important that agencies have the ability to log network and system activity and have procedures in place to periodically review this activity. A security or system log is a record of events that have taken place within an organization's systems and networks. Logs are composed of entries containing information about specific events, such as the date, time, and Internet Protocol address (IP address) attempting to log on to a specific system. Logs are essential for alerting security staff to anomalous or malicious activities and act as evidence or an audit trail should an incident occur. State Cyber Security Policies and industry best practices require that all network devices supporting an agency's infrastructure possess logging capabilities and that agencies develop standards and procedures for generating logs. At a minimum, all state systems must record successful and failed access or logon attempts. Additionally, state agencies are required to preserve and securely store system logs for a period of at least one year with three months of log activity available online. Agency IT staff are also responsible for periodically monitoring system logs to detect anomalous or inappropriate activity.

We assessed the Department's practices for generating, retaining, safeguarding, and monitoring network device and SAP logs and identified the following problems.

- **System access not logged**. First, we found that the Department's logs do not record all of the information necessary to track a remote user's activities on the network. To remotely gain access to SAP and other network devices, employees and contractors must first establish connections through either a virtual private network (VPN) or a dial-in modem. Neither the Department's VPN device nor its dial-in modem logs the source IP address from where the connection originated, date and time of the connection, or user ID attempting to establish the connection. As such, it is currently impossible to determine the location from where an attack is launched against the Department's network and SAP, or to identify the date and time of the incident or the user ID being used by the attacker. Second, we found that the Department has not enabled logging within the SAP application. As a result, the activity of users within SAP is not tracked and is therefore not available for analysis should an incident be reported.

- **Successful logon attempts not recorded.** The Department's primary authentication server is only logging failed logon attempts. State Cyber Security Policies require that both failed and successful logon attempts be logged. Both failed and successful logon attempts need to be recorded to ensure that a complete record of each user's activities is available for review and analysis should an incident occur.

- **Log activity not properly retained.** For those devices with logging enabled, we reviewed the Department's practices for retaining system logs and found that the Department has not configured network devices to securely store one year's worth of log activity as required by State Cyber Security Policies. For example, we found that the Department has configured its perimeter firewall to retain only six months of system activity. Maintaining 12 months of system activity is important because the average security incident or data breach is not detected for many months from the date of the incident. Insufficient log activity retention could hamper any investigative efforts should an incident occur.

- **Log activity not consistently reviewed.** We found that Department staff are not consistently reviewing those logs currently available to identify anomalous activities. We interviewed staff and learned that system logs are only reviewed if a specific problem is reported by a system user. It is important that logs be reviewed to proactively identify attacks and other inappropriate system activity.

The problems we identified with the Department's logging capabilities can be attributed to a lack of direction and planning. Specifically, we found that the Department has not developed or implemented a comprehensive log management strategy based on identified risks to its computing environment. Because system logs can take up significant resources and slow down network traffic, it is important that organizations have well thought out plans for the specific type of activity that needs to be logged. Such plans should include identifying required log retention periods and procedures for safely storing logs. In discussions with Department IT staff, we found that no such plans exist and that decisions about the type of activities to log and log retention periods have been left to the individual system and network administrators. Additionally, we found that the Department has not designated specific staff responsible for periodically reviewing system logs or developed procedures directing staff on the type and frequency of reviews to conduct.

Incident Response Capabilities

We also found that the Department lacks the capability to respond to a cyber security incident if one were identified. Colorado's Cyber Security Incident Response Plan and State Cyber Security Policies require all state agencies to develop and implement localized procedures that will guide the escalation of responses and help manage the recovery from malicious attacks. At a minimum, incident response procedures must identify the personnel responsible for incident response; establish reporting and escalation procedures; develop strategies for containment, investigation, root cause analysis, recovery, and training; and define the records that are to be maintained and processes to protect evidence. We found that the Department has not developed localized incident response procedures and that IT staff do not report incidents to the CISO as required by policy. Failure to respond in a coordinated and forensically sound manner could result in increased damages and system downtime, as well as the inability to prosecute the attacker due to inadequate and inadmissible information or evidence.

Improvements

The Department needs to take immediate steps to improve the security of its network. First, the Department needs to work with OIT to improve its incident identification and response capabilities. One alternative is for the Department to utilize the State's enterprise intrusion detection system, which is already in place on the network utilized by most state agencies. This alternative could potentially reduce the cost associated with the Department deploying and monitoring its own intrusion detection system. Additionally, the Department needs to develop incident response procedures and train IT staff on their use. Second, the Department needs to evaluate the risks posed to its computing environment and develop a comprehensive plan or strategy for logging network and system

activity. At a minimum, the Department should enable logging on all network devices that allow individuals to remotely connect to their network. This logging is necessary to correlate remote activities and identify the source location of potential attacks. The Department should also identify critical SAP transactions and user IDs and enable logging to track application-level activity. These logs should be securely maintained and available for analysis as required by State Cyber Security Policies. Finally, the Department needs to configure its primary authentication server to log both failed and successful logon attempts, as required by Cyber Security Policies. The Department should also develop procedures and implement the necessary tools to ensure system logs are securely retained for at least one year.

(Classification of Finding: Significant Deficiency – See Appendix A)

Recommendation No. 1:

The Department of Transportation should work with the Governor's Office of Information Technology (OIT) to improve its incident detection and response capabilities by:

a. Evaluating the feasibility of using the State's enterprise intrusion detection system and incident monitoring capabilities for the Department's network. The Department should leverage OIT's expertise in deploying an intrusion detection system and develop a plan and implement the necessary intrusion detection system sensors and software.

b. Developing localized incident response procedures that comply with State Cyber Security Policies and training Department staff in the proper identification and reporting of cyber security incidents.

c. Developing a comprehensive plan or strategy for logging important network and SAP system activity. This should include identifying all critical computing resources where logging should be enabled; defining the specific activity or events to be logged; identifying the roles and responsibilities of those tasked with log management; and developing operating procedures to ensure that staff with log management responsibilities comply with State Cyber Security Policies, such as requirements to periodically monitor system logs for anomalous or inappropriate activity.

d. Logging both failed and successful logon attempts and developing procedures and implementing the necessary tools to ensure system logs are securely retained for at least one year.

Department of Transportation Response:

a. Agree. Implementation date: September 2010.

The Department has procured and received new Intrusion Detection (IDS)/Intrusion Prevention (IPS) System software blades and has started the implementation and configuration project for the new equipment. The Department will also be installing a centralized log management server to correlate traffic and log and prioritize events for both the firewall and IDS/IPS systems. Logs will also be sent to OIT's QRadar (enterprise IDS) system for correlation.

b. Agree. Implementation date: August 2010.

The Department has developed a standard operating procedure for incident management. This procedure addresses the requirements listed within Cyber Security Policies and the Cyber Security Incident Response Plan.

The Department is currently defining incident prioritization. Exact levels and time frames for functional and hierarchic incident escalation will be agreed to during service level agreement negotiations with OIT for each service. After finalization of these service level agreements, IT staff will be trained in the proper identification and reporting of cyber security incidents.

c. Agree. Implementation date: January 2011.

The Department will develop and implement a strategy for logging and monitoring important network and SAP system activity. This will include identifying all critical computing resources where logging should be enabled; defining the specific activity or events to be logged; identifying the roles and responsibilities of those tasked with log management; and developing operating procedures to ensure staff with log management responsibilities comply with State Cyber Security Policies. This will also include using QRadar to correlate all network events.

d. Agree. Implementation date: January 2011.

The Department will ensure that successful logons are recorded and monitored as required by State Cyber Security Policies. This will be completed by August 2010.

The Department will also investigate purchasing a third party product to store system logs for one year or work with OIT to use QRadar to log these events by January 2011.

Governor's Office of Information Technology Response:

a. Agree. Implementation date: September 2010.

The Office of Cyber Security (OCS) will work with the Department's Information Security Officer (ISO) on an intrusion detection strategy and the implementation of a comprehensive IDS solution. This will include an architectural review, capacity evaluation of the enterprise QRadar solution to accept the Department's IDS logs and events, threat & vulnerability management program IDS testing capabilities to evaluate the effectiveness of the Department's IDS solution, development of a lifecycle management plan for the Department's IDS solution, and creation of a long-term strategy to incorporate the Department's IDS solution into the OCS enterprise detection and monitoring strategy for the State of Colorado.

b. Agree. Implementation date: August 2010.

The OCS will work with the Department's ISO in reviewing and providing recommendations for areas of improvement on the agency incident response plan to meet the security requirements of the OCS Incident Response policy and ensuring the agency incident response plan integrates into the OCS State Incident Response Plan.

c. Agree. Implementation date: January 2011.

The OCS will work with the Department's ISO by providing guidance and evaluating and approving a comprehensive logging and monitoring plan for the Department's SAP system and other network devices. An architectural and capacity evaluation of the OCS enterprise QRadar solution to accept the Department's logs and events will be performed to ensure the current QRadar implementation can provide a scalable and sustainable solution for the Department.

d. Agree. Implementation date: January 2011.

The OCS will work with the Department's ISO in evaluating the effectiveness of the Department's current logging and monitoring process. The enterprise OCS QRadar solution can provide automated analysis and reporting of events and incidents collected by system and

application logs. An architectural and capacity evaluation of the OCS enterprise QRadar solution to accept the Department's logs and events will be performed to ensure the current QRadar implementation can provide a scalable and sustainable solution for the Department.

Management of User Access

The second significant deficiency we identified concerns the need for the Department to improve controls over who has access to its systems and data, as well as what actions they can perform. In total, the Department is responsible for managing 4,275 network IDs and 3,181 SAP user IDs. Access management entails managing who has access to specific information, ensuring the access is directly relevant to a particular job or function, and controlling and monitoring user access. User access to SAP and the Department's network must be tightly controlled and managed because of the critical nature of the information processed by the application and transmitted over the network. State Cyber Security Policies require state agencies to provide users only with the least amount of access necessary to perform their job duties and to establish procedures to ensure that IT security administrators are immediately notified when an employee resigns or is terminated. Additionally, state agencies are required to immediately remove all system access belonging to terminated employees.

User Access

To access the SAP application, users must complete an access request form that is signed by their supervisor. The request form designates the applications and level of access to be granted. Once signed by the user's supervisor, the form is forwarded to the IT Security Operations Group. The IT Security Operations Group is then responsible for adding the user to the system and assigning the appropriate roles or system access levels. Once a user has been issued valid credentials, he or she must log on or authenticate first to the Department's network and then again to the SAP application. Each time a user logs on, the user must provide his or her authentication credentials consisting of a valid username and password, to gain access.

We reviewed the Department's controls related to user identity and access management and identified the following deficiencies.

Access authorization. State Cyber Security Policies require that all access to state systems be authorized by management and that written records of access requests, changes, terminations, and transfers be retained for one year after the term of the user's employment. We tested the Department's controls to determine if they ensure access to SAP is consistently authorized by management. We

selected a sample of 25 SAP user IDs created during Fiscal Year 2009 and requested documentation of management approval for the levels of access granted to these users. We found that Department personnel were unable to locate forms showing management approval for 16 (64 percent) of the SAP user IDs sampled. We interviewed Department staff and determined that IT security staff do not always require a completed access request form prior to setting up a user on the Department's network or in SAP. IT security staff will establish users based on requests received via e-mail or the phone. This practice violates State Cyber Security Policies and increases the risk that an individual may gain unauthorized or inappropriate access to Department computer resources.

Periodic user access reviews. According to State Cyber Security Policies, state agencies are to develop procedures for periodically reconciling lists of terminated users with active user accounts on agency IT systems to ensure that terminated employees' user access credentials have been revoked. Additionally, agencies are required to periodically review all active network and SAP system user accounts to validate that the IDs are still necessary and that users have the appropriate levels of access for their current job duties. Our audit found that Department staff do not perform periodic user access reviews. This has resulted in the following problems:

- **IDs belonging to terminated users.** We evaluated all of the active network and SAP user IDs to determine if active IDs belonging to terminated users existed. Of the 4,275 active network IDs, we identified 20 belonging to terminated users. These network IDs were active from 28 to 1,139 days since the user's termination, an average of 383 days. Of the 3,181 active SAP IDs, we identified nine belonging to terminated users. These SAP IDs were active from 99 to 121 days since the user's termination, an average of 105 days.

- **Inactive IDs.** We also reviewed controls related to the monitoring of inactive or unused IDs and noted that of the 4,275 network IDs, 182 (4 percent) had been activated but never used. To determine how long these IDs have been unused, we compared their creation date to the date we reviewed them and noted some as old as nine years. Out of the total network IDs, 855 (20 percent) of the IDs had not been used in at least 60 days. Inactive or unused IDs provide attackers an unnecessary avenue for compromising state systems. Inactive IDs should either be set to automatically suspend after a given period of time or be disabled manually by Department IT security staff.

- **Generic IDs.** We also found 474 (11 percent) generic network IDs. Generic IDs are active IDs with no identifiable owner. Generic IDs represent risk in that there is no one who can be held accountable for the activity performed through them. Department IT security staff should

review these IDs to determine if they are still necessary. If not needed, these IDs should be immediately disabled. Additionally, for those generic IDs that are needed, IT security staff should identify the ID's owner and add this information to the authentication server.

Password parameters. State Cyber Security Policies require that passwords be a minimum of eight characters, be changed at least every 60 days, and be complex (i.e., a password should contain a combination of capital letters, lowercase letters, numbers, and special characters). We identified problems with both the Department's network and SAP password parameters. For the Department's network passwords, we found that the default configuration settings complied with State Cyber Security Policies. However, in analyzing individual network IDs, we found that the default password configuration settings were routinely overridden by Department IT security staff. Specifically, of the 4,275 network IDs, 999 (23 percent) had passwords older than 60 days, and 187 (4 percent) had passwords that were set to never expire. Additionally, we found that Department IT security administrators had misconfigured the password settings for 993 network IDs. This misconfiguration made it possible for an IT security administrator to reset the password for these IDs to a null or blank password; in other words, no password would be required.

For the SAP application, we found that the Department's default password parameters do not comply with State Cyber Security Policies. SAP passwords have a minimum required length of six characters instead of eight; passwords are only required to be changed after 300 days instead of 60 days; and password complexity is not enforced. Additionally, the SAP application is not configured to prevent users from recycling previously used passwords or from using a password very similar to the one previously used.

The Department's inadequate network and SAP password parameters make it easier for attackers to guess passwords and gain inappropriate and unauthorized access to computing resources and Department data. To prevent password guessing attacks from being successful, the Department needs to ensure all password parameters comply with State Cyber Security Policies, including those for both the primary authentication server and SAP.

SAP User Profiles

In SAP, security is implemented by controlling a user's access to tables within the system. SAP is comprised of thousands of tables in which data are stored. Users interact with these tables through the SAP Graphical User Interface. Based on the privileges, or level of access, associated with the user's ID, the SAP system will either process the user's request (e.g., create a new vendor record) or deny it and display an error message. Instead of creating custom privileges for each user, the Department has implemented a role-based access control system. Basically, users

who share the same role within the organization are assigned the same system privileges or user profile.

We tested the appropriateness of SAP user profiles related to the module that tracks and processes Department expenditures. We focused on the expenditure module because this module processes over $1 billion in payments annually and because of the risk of errors or fraud if access controls are inappropriate. For example, SAP user profiles should not allow the same person to both add or modify vendor information and to both initiate and approve a payment. Such levels of access could enable a user to circumvent manual controls and allow unauthorized payments to be made.

Overall, we found that the Department has not evaluated SAP user access profiles and identified and documented those profiles, or combination of profiles, that are appropriate for different system users. Although SAP user access profiles have not been defined, we used industry best practices and vendor recommendations to assess the appropriateness of SAP users' access to critical expenditure tables, such as the ability to create and approve a purchase order. We identified the following specific problems with inappropriate access.

- **Critical Expenditure Tables.** The Department has 19 IT staff with access to critical expenditure tables, allowing them to perform specific business functions that are not part of their assigned jobs. These excessive access rights were left over from the pre-implementation environment. This level of access is inappropriate and provides unnecessary risk, and should be eliminated. We provided the specific details of this finding, including a complete list of the specific expenditure tables affected, to the Department under separate cover.

- **System Tools.** The Department does not properly control access to and monitor the use of special system tools. Specifically, we found that more SAP users than necessary had access to the S_Query tool. The S_Query tool can be used to develop customized system queries to view SAP's most sensitive data, including human resources, financial accounting, and project pricing data. According to SAP and industry best practices, access to this tool should be extremely limited. During our audit, we found that 42 SAP users had access to the S_Query tool. In discussions with Department staff, we found that the S_Query tool should be restricted to the SAP administrative team, which is comprised of five staff.

- **Privileged Transactions.** The Department has not restricted or locked access as recommended by industry best practices to the many highly privileged transactions that can be used to modify administrative tables. For example, the use of the SE11 transaction can be used to modify the SAP data dictionary, and the SU10 transaction can be used to add and

delete user profiles. This means that it is possible for SAP users to make significant changes to the system that may not be authorized to perform. Unauthorized changes to these critical administrative tables could have a significant impact on SAP and the data it stores and processes. We provided the specific details of this finding, including a complete list of the privileged transactions that should be restricted or locked as recommended by industry best practices, to the Department under separate cover.

- **Privileged Account.** The Department is not properly monitoring and controlling access to a privileged account used by vendors to install upgrades and troubleshoot problems. This privileged account has full permissions to all tables within SAP, including the expenditure module. Failure to properly monitor and control access to this account provides an unnecessary opportunity for disgruntled employees of the Department's vendors or outside attackers to gain full access to the system and perform unauthorized functions, such as viewing or downloading Department employee information.

To determine if the inappropriate access we identified resulted in specific problems, we requested SAP transaction logs for further review and analysis. However, as previously discussed, the Department has not enabled the logging function within SAP. As a result, we were unable to determine the impact of these inappropriate levels of access. The Department's lack of logs that would enable it to monitor user activity exacerbates the risks that result from inadequate controls over user access.

The Department needs to take several steps to ensure access to SAP is appropriate and properly controlled. First, the Department should evaluate SAP user access profiles and identify and document those profiles, or combination of profiles, that are appropriate for different system users. Second, the Department should periodically review SAP users' levels of access and require unit managers to annually validate in writing that such access is still appropriate. Third, Department staff should remove the excess levels of access we identified during our audit and provided to the Department under separate cover. Additionally, the Department should evaluate and restrict access to tools, transactions, and tables and limit vendor access to the privileged SAP user account for only the time period necessary and should log and closely monitor this account's activities.

(Classification of Finding: Significant Deficiency – See Appendix A)

Recommendation No. 2:

The Department of Transportation should work with the Governor's Office of Information Technology to strengthen user access management controls by:

a. Ensuring user access is consistently approved by management and that records of approvals are retained for the time period specified by State Cyber Security Policies.

b. Implementing a combination of manual and automated controls for identifying and disabling inactive IDs and IDs belonging to employees and contractors no longer employed by the Department. The Department should immediately disable those accounts we identified as belonging to terminated users.

c. Identifying and documenting an owner for every network ID. Unless a specific business need is identified, generic IDs should be eliminated.

d. Ensuring all user IDs have passwords configured to comply with State Cyber Security Policies for both the network and the SAP system.

e. Reviewing, identifying, and documenting profiles and combinations of profiles that are appropriate for different SAP users. These profiles should be designed to ensure that users only have access to the SAP tables and tools necessary to accomplish their job duties.

f. Identifying critical SAP tools, tables, and transactions and restricting access according to the risk they represent.

g. Restricting and monitoring access to all SAP privileged accounts.

Department of Transportation Response:

a. Agree. Implementation date: August 2010.

The Department will review the 16 exceptions noted in the report and ensure that evidence of approval exists for these users and all others.

The Department believes that the existing processes and procedures for recording access authorizations are sufficient. The Department will retrain IT security staff on these processes and procedures and emphasize the importance that proper documentation be submitted and maintained for all access authorization changes.

b. Agree. Implementation date: September 2010.

The Department will review and remove all inactive network IDs that are no longer needed. Controls will be implemented to ensure new user IDs are inactivated if they remain unused for an extended period of time.

The Department will also review the exceptions noted in the report that are related to IDs belonging to terminated users and remove the access.

A process will be implemented to ensure user access is reviewed on an annual basis as required by State Cyber Security Policies. This review will identify and investigate all IDs that have been inactive for at least six months. These IDs will be validated through the Department's manager responsible for the ID and if determined unnecessary, the ID will be disabled.

c. Agree. Implementation date: March 2011.

The Department will review each generic Active Directory ID and an analysis will be completed to determine the necessity and/or the repercussions of eliminating the ID. Controls will be implemented to ensure that all new IDs created in the future will have an identified owner.

d. Agree. Implementation date: September 2010.

This recommendation has been partially implemented. With the upgrade to ERP 6.0, password length, complexity, and expiration controls now comply with State Cyber Security Policies.

The Department will review and correct individual Active Directory IDs to ensure regular password changes are enforced on all user IDs as required by State Cyber Security Policies. The Department will additionally train staff to ensure that default password parameters are not overridden.

e. Agree. Implementation date: July 2010.

Profiles that are appropriate for different SAP users have been reviewed, identified and documented based upon job duties and the authorizations included when in combination with all roles assigned to a user.

The Department determined that the benefit to purchase a tool to better compile and define all possibilities was not warranted by the cost of such tools on the marketplace. As such, the Department has been managing role security based upon in-house staff knowledge.

Based on this recommendation, a business case will be presented to the Department's governing committees of the SAP implementation, recommending that a full analysis be completed using a tool and/or the expertise of the Department's Application Managed Services vendor, ACS. This business case will be presented no later than July 23, 2010.

In addition, the SAP Support team will work with OIT security to ascertain if there is already an enterprise tool that will facilitate the determination and creation of user roles designed to secure business assets accessible through SAP.

f. Agree. Implementation date: July 2010.

Identifying critical SAP tools, tables, and transactions and restricting access according to the risk they represent is an ongoing activity and due to upgrades and support packs will be an ongoing effort.

Based on this recommendation from the State Auditor, however, a full analysis will be recommended in a business case to the governing committees for the Department's SAP implementation. This business case will be presented no later than July 23, 2010.

In addition, the SAP Support team will work with OIT security to ascertain if there is already an enterprise tool that will facilitate the determination as well as mitigation/access restriction of SAP tools, tables and transactions that present a risk to the Department's business assets accessible through SAP.

g. Agree. Implementation date: December 2010.

The Department will implement procedures to ensure that access to the special SAP ID used by the SAP vendor for troubleshooting, is consistently monitored. In addition, the SAP Support team will work with OIT security to ascertain if there is already an enterprise tool that will facilitate a mechanism to restrict and monitor access to all SAP privileged accounts so as to secure business assets accessible through SAP.

Governor's Office of Information Technology Response:

Agree. Implementation date: December 2010.

The Office of Cyber Security and Enterprise Application group will work with the Department's Information Security Officer in providing guidance and recommendations for access control in accordance with State Cyber Security Policy requirements and industry best practices.

Disaster Recovery

The third significant deficiency we identified relates to the Department's inability to recover the SAP system within the time frames specified by Department management should disaster strike. Information system disaster recovery refers to the process of identifying, testing, and evaluating all of the resources and procedures needed to make specific information system based functions operational after services have been disrupted. Disaster recovery planning is essential if government is to continue providing services in the event of natural or man-made disasters or more routine interruptions, such as localized power failures or data corruption. State Cyber Security Policies require state agencies to develop comprehensive disaster recovery plans for critical applications. Because SAP is used for most of the Department's business processes, the Department considers SAP a critical application. According to the policy, agency disaster recovery plans must include the following components:

- **Roles, responsibilities, and contact information** for the individuals responsible for implementing the disaster recovery plan.

- **Recovery time frames** outlining both response and recovery requirements.

- **Recovery procedures** detailing the ways in which services will be restored and operations returned to normal.

- **Plan training**, to be conducted on a regular basis, for the individuals who have specific roles and responsibilities in implementing the disaster recovery plan.

- **Plan testing**, to be conducted on a regular basis, to ensure services can be effectively restored and any problems addressed.

- **Plan maintenance** to ensure the plan is updated or modified to reflect changes in recovery requirements, time frames, personnel, or other factors. The plan should also include procedures for distributing the plan to stakeholders and notifying them of any changes to it.

We reviewed the Department's disaster recovery testing procedures and planning documents for SAP and found two problems. First and of critical importance, the Department has not conducted a comprehensive disaster recovery test of the SAP system. Therefore, the Department cannot ensure that the SAP system could be recovered within an acceptable time frame in the event of a disaster. Second, we found that the Department's disaster recovery plan for SAP is not current and fails to address all critical components as required by State Cyber Security Policies. Specifically, we reviewed the Department's disaster recovery plan for SAP and found that it lacked the following components:

- Evidence of stakeholder approvals.
- Contact information for essential line and management staff.
- Backup procedures, retention cycles, and onsite and offsite backup storage policies.
- Testing strategies.
- Recovery time objectives to guide the timing of the restoration process.
- Hardware and software inventory needed for full recovery.
- Service level agreements for critical hardware and software.

A comprehensive and well-tested disaster recovery plan is needed for the Department to be able to successfully resume operations following a disaster or system disruption. Because key accounting functions depend entirely upon the SAP application, a significant emergency could halt critical functions such as payroll, purchasing, accounts payable, and accounts receivable for an extended period of time, severely interrupting essential Department functions. The Department should improve its ability to recover from a disaster by performing a comprehensive disaster recovery test within the next year and updating its disaster recovery plan to include all required and necessary components to guide staff through the restoration process.

(Classification of Finding: Significant Deficiency – See Appendix A)

Recommendation No. 3:

The Department of Transportation should work with the Governor's Office of Information Technology to improve its disaster recovery planning and preparedness for SAP by:

a. Performing a full-scale disaster recovery test within the next 12 months.

b. Ensuring that the disaster recovery plan includes all components required by State Cyber Security Policies.

Department of Transportation Response:

a. Agree. Implementation date: March 2011.

The current Disaster Recovery Plan was last revised on December 31, 2009. The plan will be updated with all State Auditor recommendations no later than July 31, 2010. This plan will make possible the ability to conduct a tabletop disaster recovery exercise at any point in time.

A condensed test, including failover to the current disaster recovery site in Lakewood, Colorado as well as failback to the Department's headquarters will be conducted on the third weekend of October 2010.

A full test, based on the plan, executed with tape backups, and documented disaster recovery personnel will be conducted in March 2011.

b. Agree. Implementation date: March 2011.

All components of a disaster recovery plan required by State Cyber Security Policies will be included in the Department's SAP disaster recovery plan.

Governor's Office of Information Technology Response:

Agree. Implementation date: March 2011.

The Office of Cyber Security (OCS) requires all agencies to submit an annual Disaster Recovery (DR) plan and summary of DR testing results with their Agency Cyber Security Program (ACSP) package. OCS will

not approve incomplete ACSP packages submitted by an agency Information Security Officer (ISO) and will report non-compliance to the OIT Executive Management Team.

Information Security Management

Statute [Section 24-37.5-404, C.R.S.] and State Cyber Security Policies require state agencies to develop annual information security plans. These plans are essential to both the Department's and the Governor's Office of Cyber Security's ability to effectively manage state information security operations. The Governor's Office of Cyber Security, within OIT, relies on agency security plans to assess risk of cyber attacks, develop statewide mitigation plans, identify and mitigate known vulnerabilities, and establish budget and resource priorities. According to State Cyber Security Policies, the Department's information security plan is required to contain information about the agency's:

- Organizational structure, mission, and objectives
- Information technology environment
- Risk management procedures
- Information security program
- Incident warning, advisory, and response procedures
- Training and security awareness plans

As part of the planning process, State Cyber Security Policies also require agencies to annually update and submit a Risk Based Gap Analysis and Plan of Actions and Milestones. The Risk Based Gap Analysis is used as a tool to identify the deficiencies in the agency's information security environment. The Plan of Actions and Milestones is the tool used to identify the specific details, resources, and time frame for mitigating these deficiencies.

We reviewed the Department's current Cyber Security Plan, including the Risk Based Gap Analysis and Plan of Actions and Milestones, and found that these documents were incomplete, were not updated, and did not reflect the Department's current computing environment or level of compliance with State Cyber Security Policies. For example, the Risk Based Gap Analysis lacked up-to-date information for SAP, such as information related to management of access privileges, software change control, and data handling. The Plan of Actions and Milestones is incomplete as well, because its accuracy depends directly on the

information contained within the Risk Based Gap Analysis. To ensure the Governor's Office of Cyber Security has the necessary information to manage state security operations, the Department should ensure that comprehensive security risk assessments are completed annually and that its Cyber Security Plan, including the Risk Based Gap Analysis and Plan of Actions and Milestones, are updated and accurate.

(Classification of Finding: Control Deficiency – See Appendix A)

Recommendation No. 4:

The Department of Transportation should work with the Governor's Office of Information Technology to improve its information security management program, including performing annual security risk assessments and updating state-required information security documents, including the annual information security plan.

Department of Transportation Response:

Agree. Implementation date: July 2010.

The Department will work with OIT and the Office of Cyber Security to improve its security management program including performing annual risk assessments. The Department has already performed a new Risk Based Gap Analysis in order to establish new security baselines and update security documents and the annual security plan.

Governor's Office of Information Technology Response:

Agree. Implementation date: July 2010.

The Office of Cyber Security (OCS) requires all agencies to submit an annual Agency Cyber Security Program (ACSP) package consisting of:

- Cover letter requesting ACSP approval
- Agency Cyber Security Plan (ACSP)
- Agency-wide Risk Assessment
- Agency Disaster Recovery Plan Summary
- Agency Disaster Recovery Plan test results
- Agency Self-Assessment results
- Agency Cyber Security Plan of Action and Milestones (POA&M)

OCS will not approve incomplete ACSP packages submitted by an agency Information Security Officer (ISO) and will report non-compliance to the OIT Executive Management Team. An ACSP scorecard has been developed by OCS to provide areas of improvement to the agency ISO on the ACSP to assist in the prioritization of limited agency resources for cyber security improvements within the agency.

Security Awareness Training

Information security awareness training is important to an organization's information security strategy. Users are the first line of defense against threats posed by malicious code, disgruntled employees, and malicious third parties. Information system users need to know what an organization considers appropriate security-conscious behavior and what security best practices they need to incorporate into their daily business activities. Because of the importance of having security-conscious users, State Cyber Security Policies require that all employees, contractors, and users of state systems receive initial and ongoing security awareness training on at least an annual basis. Agencies are to track the completion of this training centrally and require users to attest in writing that they have completed the training and agree with the agency's acceptable use policy.

We found that the Department is not complying with State Cyber Security Policies regarding security awareness training. While all new employees and contractors complete initial training, we found that the Department does not provide SAP users with ongoing security awareness training or require that users annually recertify their understanding and compliance with the Department's acceptable-use policy. Additionally, the Department does not provide specialized, system-specific training to Department employees with information security responsibilities, such as those staff charged with establishing and monitoring user access within the SAP system.

It is difficult, if not impossible, to protect the confidentiality and integrity of information without ensuring that all people involved in using and managing data have adequate knowledge of the various controls required and available to protect computing resources under their scope of responsibility. Employees who have limited knowledge of security practices can put the Department at risk through bad habits or lack of attention. Raising and maintaining the awareness level of potential security threats is an essential component of an effective overall security strategy. One of the best ways to make sure employees do not make costly errors with regard to information security is to implement organization-wide security-awareness training initiatives that ensure employees have a solid understanding of the organization's security policy and procedures as well as industry best

practices. This effort should include providing specialized security training for those with assigned information security responsibilities.

(Classification of Finding: Control Deficiency – See Appendix A)

Recommendation No. 5:

The Department of Transportation should work with the Governor's Office of Information Technology to implement an annual information security awareness training program for all system users, including staff and contractors. This program should address both general and Department-specific security risks. The Department should also ensure that users re-certify their understanding and compliance to the Department's Acceptable Use Policy on an annual basis. Specialized system security training should be provided to those with SAP information security responsibilities.

Department of Transportation Response:

Agree. Implementation date: December 2010.

The Department will ensure that employees and system users consistently receive annual security awareness training that addresses the Department's unique environment, risks, and policies. The Department will also ensure that employees and system users annually recertify their understanding and compliance with the Department's Acceptable Use Policy. Department employees with information security responsibilities will be provided specialized system-specific training to ensure information security tasks are carried out consistently and effectively.

The Department will also be working closely with the Office of Cyber Security in rolling out the updated state-wide Security Awareness Training project.

Governor's Office of Information Technology Response:

Agree. Implementation date: December 2010.

The Office of Cyber Security (OCS) procured an online training system in 2007 to be used by agency Information Security Officers to provide and track security awareness training within their agency. The security awareness training content was updated and a state-wide cyber security awareness training project will be kicked off in July 2010. Completion of

agency staff security awareness training will be tracked by OCS and reported to the OIT Executive Leadership Team and the Governor's Office on a monthly basis.

Appendix

Appendix A

Report Findings by Classification of Finding

Definition of Finding Classifications	
Classification	**Description**
Material Weakness	A material weakness produces an immediate risk directly impacting the confidentiality, integrity, and availability of information systems and data. For IT projects, a material weakness represents an immediate threat to the overall success of the project. This would be considered a high risk finding.
Significant Deficiency	Significant deficiencies do not alone produce an immediate risk, but could affect the confidentiality, integrity, or availability of systems in conjunction with other factors. For IT projects, significant deficiencies do not represent an immediate threat to the overall success of the project but could result in project delays, cost overruns, or incomplete deliverables. This would be considered a moderate risk finding.
Control Deficiency	Control deficiencies do not present an immediate risk but could be indicative of operating deficiencies and/or have the potential to adversely affect the confidentiality, integrity, or availability of systems over an extended period of time. For IT projects, control deficiencies may not represent an immediate threat to the overall success of the project but could, over an extended period of time and in conjunction with other deficiencies, result in project delays, cost overruns, or incomplete deliverables. This would be considered a low risk finding.

Rec. No.	Page No.	Audit Finding	Classification of Findings		
			Material Weakness	Sig. Deficiency	Control Deficiency
1	11	Improve the Department's incident detection, response, and reporting capabilities and practices.		X	
2	19	Strengthen the Department's access management controls, including ensuring that critical SAP tools, tables, and privileged accounts are tightly controlled and monitored.		X	
3	24	Update the SAP disaster recovery plan and conduct a comprehensive disaster recovery test.		X	
4	26	Complete annual risk and vulnerability assessments and update the Department's Cyber Security Plan, including the Risk Based Gap Analysis and Plan of Actions and Milestones.			X
5	28	Ensure Department users are provided annual information security awareness training and are recertifying their understanding and compliance with the Department's acceptable-use policy.			X

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

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

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

Report Control Number 2012

Report Control Number 2012