AUDIT RECOMMENDATION STATUS REPORT

AUDIT NAME: SAP Information System
AUDIT NUMBER: 2012
DEPARTMENT/AGENCY/ENTITY: Department of Transportation and Governor's Office of Information Technology
Note: Since the audit, the IT employees at the Department of Transportation now are part of the Governor's Office of Information Technology. All status updates are provided only by the Governor's office of Information Technology.
DATE: January 15, 2011

SUMMARY INFORMATION

Recommendation Number *(e.g., 1a, 1b, 2, etc.)*	**Agency's Response** *(i.e., agree, partially agree, disagree)*	**Original Implementation Date** *(as listed in the audit report)*	**Implementation Status** *(Implemented, Partially Implemented, or Not Implemented)* * *A recommendation that is in progress should be denoted as "partially implemented."*	**Revised Implementation Date** *(Complete only if agency is revising the original implementation date.)*
1a.	Agree	September 2010	Implemented.	
1b.	Agree	August 2010	Partially Implemented.	March 2011
1c.	Agree	January 2011	Implemented.	
1d.	Agree	January 2011	Partially Implemented. *(On Schedule)*	
2a.	Agree	December 2010	Implemented.	
2b.	Agree	December 2010	Implemented.	
2c.	Agree	December 2010	Partially Implemented.	March 2011
2d.	Agree	December 2010	Implemented.	
2e.	Agree	December 2010	Partially Implemented.	March 2011
2f.	Agree	December 2010	Implemented.	
2g.	Agree	December 2010	Partially Implemented.	March 2011
3a.	Agree	March 2011	Partially Implemented. *(On Schedule)*	
3b.	Agree	March 2011	Partially Implemented. *(On Schedule)*	
4.	Agree	July 2010	Partially Implemented.	July 2011
5.	Agree	December 2010	Partially Implemented.	February 2011

ATTACHMENT C

DETAIL OF IMPLEMENTATION STATUS

Recommendation #: 1a.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

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

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.

Agency's Original Response *(i.e., Agree, Partially Agree, Disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Current Comments on Implementation Status of Recommendation:

Implemented.

Recommendation #: 1b.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

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

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.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Partially Implemented.

The Office of Cyber Security is updating the State Incident Response plan to include: 1) Localized incident response procedures; 2) Roles and responsibilities for a CDOT Cyber Security Incident Response Team; and 3) Training on incident response reporting requirements for agency staff. The CDOT Information Security Officer will be following the IR plan provided by OCS.

Revised Implementation Date: March 2011.

Recommendation #: 1c.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

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

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Implemented.

A centralized linux based syslog-ng server has been installed to collect logs from SAP, network and the CDOT active directory. Log analysis tools were installed to identify anomalous and malicious activity and send automated alerts to the CDOT ISO and the OCS ISOC.

Recommendation #: 1d.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

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

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Partially Implemented. *(On schedule.)*

Recommendation #: 2a.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Department of Transportation should work with the Governor's Office of Information Technology to strengthen user access management controls by:
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.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Implemented.

Recommendation #: 2b.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Department of Transportation should work with the Governor's Office of Information Technology to strengthen user access management controls by:
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.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Implemented.

Recommendation #: 2c.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Department of Transportation should work with the Governor's Office of Information Technology to strengthen user access management controls by: Identifying and documenting an owner for every network ID. Unless a specific business need is identified, generic IDs should be eliminated.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Partially Implemented.

The CDOT SAP team is 64% completed (303 of 471) with addressing the findings for generic IDs.
A risk assessment of remaining generic IDs is being performed with the CDOT ISO and is expected to be completed by March 2011

Revised Implementation Date: March 2011.

Recommendation #: 2d.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Department of Transportation should work with the Governor's Office of Information Technology to strengthen user access management controls by:
Ensuring all user IDs have passwords configured to comply with State Cyber Security Policies for both the network and the SAP system.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Implemented.

Recommendation #: 2e.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Department of Transportation should work with the Governor's Office of Information Technology to strengthen user access management controls by:
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.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:
Partially Implemented.

With the transition of IT employees on the SAP team to OIT, most procurement privileges were removed from OIT employees.
OIT will create a spreadsheet listing all privileged accounts for review by March 2011. This review process will be performed on an annual basis.
Access history for transactions by all SAP Technical personnel will be retrieved for the past 3 months and reviewed by CDOT and by the CDOT ISO.
All users with access to the S-Query tool will be reviewed and adjusted by March 2011.

Revised Implementation Date: March 2011.

Recommendation #: 2f.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Department of Transportation should work with the Governor's Office of Information Technology to strengthen user access management controls by:
Identifying critical SAP tools, tables, and transactions and restricting access according to the risk they represent.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Implemented.

Recommendation #: 2g.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
The Department of Transportation should work with the Governor's Office of Information Technology to strengthen user access management controls by: Restricting and monitoring access to all SAP privileged accounts.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Partially Implemented

Roles and authorization requests are reviewed by CDOT Business Process Experts (BPXs).

For existing profiles, OIT will provide a spreadsheet listing all roles to be reviewed by CDOT BPXs and completed by March 2011. CDOT BPX's will perform this review annually.

Revised Implementation Date: March 2011.

Recommendation #: 3a.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
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:

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

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Partially Implemented. *(On schedule.)*

Recommendation #: 3b.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
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:

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

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Partially Implemented. *(On schedule.)*

Recommendation #: 4.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
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.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:
CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Partially Implemented.

The CDOT ISO will be utilizing the OCS CRISC application to manage the agency information security program while updating the current CDOT ACSP to be in compliance with the current ACSP requirements. The ACSP will be completed by July 15th as per OCS rules.
NOTE: OIT is unsure why the original implementation date is the same month in which the audit hearing was conducted. OCS is revamping the ACSP process and will have plans in place by the July 2011 deadline per statute and OCS rules.

Revised Implementation Date: July 2011.

Recommendation #: 5.

Agency Addressed: Colorado Department of Transportation and Governor's Office of Information Technology

Original Recommendation in Audit Report:
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.

Agency's Response *(i.e., agree, partially agree, disagree)*: **Agree**

Agency's Written Response in Audit Report:

CDOT
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.

OIT
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.

Agency's Comments on Implementation Status of Recommendation:

Partially Implemented.

The CDOT ISO will be utilizing the OCS online security awareness training system to provide and manage agency security awareness training for all CDOT employees beginning February 1, 2011. This training program is being rolled out across the state to 31,000 state employees. Instead of developing a training program specifically for CDOT employees in December, we felt that providing them with the statewide training was the better implementation strategy.

Revised Implementation Date: February 2011.