STATE OF COLORADO

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

601 East 18th Avenue, Suite 250
Denver, Colorado 80203
Phone (303) 764-7700
Fax (303) 764-7725
www.colorado.gov/oit

John W. Hickenlooper
Governor

Kristin Russell
Secretary of Technology and
State Chief Information Officer

October 19, 2012

Dianne E. Ray, CPA
State Auditor
Colorado Office of the State Auditor
200 East 14th Avenue, 2nd Floor
Denver, CO 80203

Dear Ms. Ray:

In response to your request, we have prepared an updated status report regarding the implementation of audit recommendations contained in the performance audit report of the *Consolidation of Executive Branch Information Technology*. The attached report provides a brief explanation of the actions taken by the Governor's Office of Information Technology (OIT) to implement each recommendation.

In summary, the audit contained 12 separate recommendations related to strategic planning, project management, IT budgeting and procurement, IT asset management, and human resources. OIT has implemented or partially implemented nine (75%) of the recommendations contained in the audit report. The three recommendations currently not implemented are related to IT budgeting, which will be addressed through a joint project with the Governor's Office of State Planning and Budgeting related to IT financial reform. This project is scheduled to begin in November 2012.

If you have any questions, please do not hesitate to contact me at (303) 764-7709 or Brenda Berlin at (303) 764-2928.

Sincerely,

Dara Hessee
Chief of Staff
Governor's Office of Information Technology

AUDIT RECOMMENDATION STATUS REPORT

AUDIT NAME: Consolidation of Executive Branch Information Technology
AUDIT NUMBER: 2151
DEPARTMENT/AGENCY/ENTITY: Governor's Office of Information Technology (OIT)
DATE: September 4, 2012

SUMMARY INFORMATION

Please complete the table below with summary information for all audit recommendations. ***For multi-part recommendations, list each part of the recommendation SEPARATELY.*** *(For example, if Recommendation 1 has three parts, list each part separately in the table.)*

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report)*	**Implementation Status** *(Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable)* Please refer to the attached sheet for definitions of each implementation status option.	**Revised Implementation Date** *(Complete only if agency is revising the original implementation date.)*
1a	Agree	October, 2012	Implemented	
1b	Agree	July, 2012	Implemented	
1c	Agree	July, 2012	Implemented	
1d	Agree	June, 2012	Implemented	
2a	Agree	December, 2012	Not Implemented	July 1, 2013
2b	Agree	December, 2012	Not Implemented	July 1, 2013
2c	Agree	October, 2012	Partially Implemented	July 1, 2013
3	Partially Agree	July, 2012	Partially Implemented	July 1, 2013
4a	Agree	October, 2012	Partially Implemented	July 1, 2013
4b	Agree	July, 2012	Partially Implemented	July 1, 2013
4c	Agree	July, 2012	Partially Implemented	July 1, 2013
5	Partially Agree	December, 2012	Not Implemented	July 1, 2013

DETAIL OF IMPLEMENTATION STATUS

Recommendation #: 1a

Agency Addressed: Governor's Office of Information Technology

Recommendation Text in Audit Report:

OIT should strengthen its governance and oversight of the State's consolidation initiative by:

a. Developing a strategy and tactical plans for IT consolidation that aligns with the overall goals of OIT and the goals of the agencies involved in the consolidation.

Agency's Response *(i.e., Agree, Partially Agree, or Disagree)***:** Agree. Implementation date: October, 2012.

Agency's Written Response in Audit Report:

OIT agrees that a strong and stable governance structure is important to ensure operational efficiency across the state. OIT's current CIO was appointed in February 2011 and she immediately put OIT on the path of refining, collecting and in some cases establishing performance plans and performance metrics which did not exist. To date OIT has published its Fiscal Year 2011-12 Playbook (strategic plan), implemented quarterly deliverables for each of the playbook initiatives, implemented monthly operational metrics, and has implemented performance requirements for each of the executive staff that map back to each of the metric and deliverables.

In October 2011 OIT completed work plans with each of the departments. This was a collaborative effort with each department outlining the annual information technology operational priorities. The next step is to incorporate the strategic needs of the departments into our annual planning process which will then feed into the annual technology plan and the next budget cycle as necessary.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Implemented and Ongoing

Agency's Current Comments on Implementation Status of Recommendation:

OIT continues to publish its annual strategic plan, called the OIT Playbook. The FY13 Playbook was released in July 2012. The Playbook consists of annual strategic initiatives by executive leaders and includes quarterly deliverables. The executive team reports on and reviews

the progress towards implementing the Playbook initiatives on a quarterly basis ("Operations Reviews"). In addition, OIT continues to report on monthly operational metrics via the OIT Balanced Scorecard. The Scorecard is reviewed by the OIT CIO and the Governor's Chief of Staff on a monthly basis; additionally, the executive team participates in monthly "Scorecard Reviews" and prepares "Get Well Plans" for those areas in which the organization is underperforming.

One of OIT's key processes continues to be developing work plans with each of the departments. This is a collaborative effort with each agency which outlines annual information technology operational priorities. In addition, OIT executed Service Level Commitment (SLC) documents with the departments which outline OIT responsibilities and commitments related to IT services.

Recommendation #: 1b

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should strengthen its governance and oversight of the State's consolidation initiative by:

b. Developing strong risk criteria to adequately identify and assess risks at the consolidation project level.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Agree. Implementation date: July, 2012.

Agency's Written Response in Audit Report:

OIT agrees that a strong and stable governance structure is important to ensure operational efficiency across the state. OIT's current CIO was appointed in February 2011 and she immediately put OIT on the path of refining, collecting and in some cases establishing performance plans and performance metrics which did not exist. To date OIT has published its Fiscal Year 2011-12 Playbook (strategic plan), implemented quarterly deliverables for each of the playbook initiatives, implemented monthly operational metrics, and has implemented performance requirements for each of the executive staff that map back to each of the metric and deliverables.

OIT has good processes and procedures around assessing risks for projects larger than $5 million and is currently working to bring all medium and small projects under formal project management procedures. In addition, OIT recently completed a risk assessment of 130 of the most critical applications across the state and is in the process of completing an inventory of all applications so that a risk assessment may be completed on the remaining applications. OIT will then complete this assessment annually to identify where operational efforts need to be targeted annually.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Implemented

Agency's Comments on Implementation Status of Recommendation:

During the 2012 Legislative Session, OIT spearheaded the passage of House Bill 12-1288, which significantly changes how IT projects are managed in the state and ensures that we as a state take a smarter and more sustainable approach to IT system implementation and that IT project plans and budgets contain all the necessary components for long-term system success and eventual replacement. House Bill 12-1288 requires that all major IT projects have a project manager, a comprehensive risk assessment and business case, information security and test plans, a disaster recovery plan, an internal verification and validation plan, and a documented funding strategy for on-going maintenance and support. As part of these policies and procedures developed for managing new IT projects, OIT developed a risk assessment process. This process requires that each new project have a Project Scaling and Risk Assessment Worksheet, CARE (Classification Asset Risk Evaluation) Assessment, IT Component Assessment, and Financial Summary worksheet, which is used to assess security, operational and cost risks. The differing levels of risk dictate the level of governance that a project receives. In addition, the results of the risk assessments are documented in the OIT project management tracking system so that risk can be reviewed both on an individual project level and at a state-wide level.

Recommendation #: 1c

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should strengthen its governance and oversight of the State's consolidation initiative by:

c. Developing a standard set of metrics across consolidation projects and implementing a means of tracking such metrics.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Agree. Implementation date: July, 2012.

Agency's Written Response in Audit Report:

OIT agrees that a strong and stable governance structure is important to ensure operational efficiency across the state. OIT's current CIO was appointed in February 2011 and she immediately put OIT on the path of refining, collecting and in some cases establishing performance

plans and performance metrics which did not exist. To date OIT has published its Fiscal Year 2011-12 Playbook (strategic plan), implemented quarterly deliverables for each of the playbook initiatives, implemented monthly operational metrics, and has implemented performance requirements for each of the executive staff that map back to each of the metric and deliverables.

OIT is tracking existing enterprise projects through our Enterprise Portfolio Project Management Office and the new Director is updating the project management policies, procedures and metrics. Once updated these policies, procedures and metrics will be applied to all IT projects across the state as applicable.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Implemented

Agency's Comments on Implementation Status of Recommendation:

All IT projects managed by OIT's Enterprise Portfolio Project Management Office (EPPMO) are tracked on a monthly basis via standard metrics. These metrics are generated on a monthly basis and include project status related to cost, resources, budget, scope, risks, schedules, and milestones. The metrics are documented in OIT's project management system and are reviewed by the EPPMO Director and the Executive Governance Committee, and are distributed to agency leadership and legislative auditors on a monthly basis.

Recommendation #: 1d

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should strengthen its governance and oversight of the State's consolidation initiative by:

d. Implementing a comprehensive communications plan to guide the effective communication of consolidation project goals, benefits and status to key stakeholders; in addition, the communication plan should include methods for receiving feedback from stakeholders.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Agree. Implementation date: June, 2012.

Agency's Written Response in Audit Report:

OIT agrees that a strong and stable governance structure is important to ensure operational efficiency across the state. OIT's current CIO was appointed in February 2011 and she immediately put OIT on the path of refining, collecting and in some cases establishing performance plans and performance metrics which did not exist. To date OIT has published its Fiscal Year 2011-12 Playbook (strategic plan), implemented quarterly deliverables for each of the playbook initiatives, implemented monthly operational metrics, and has implemented performance requirements for each of the executive staff that map back to each of the metric and deliverables.

OIT agrees that communication is one of the hardest objectives to maintain consistently. OIT has a published communications plan but agrees that more work needs to be done to build out and execute against this plan, including receiving feedback from stakeholders. Effective communication must be maintained internally and externally to OIT to ensure employees, legislators, and citizens understand the role OIT plays and the benefits it can provide.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Implemented and Ongoing

Agency's Comments on Implementation Status of Recommendation:

OIT believes that good communication is key to the success of the organization, and OIT's communications plan is dynamic and evolves with available delivery channels. To that end, OIT has a number of strategic initiatives for FY13 related to improving communications to our employees, legislators, and citizens. A few of these initiatives include establishing a social media strategy, utilizing emerging media such as video live stream and video conferencing, and engaging with an IT-focused group of legislators who can be OIT advocates and champions within the Colorado General Assembly for IT initiatives. Further, with regards to stakeholder feedback, we routinely conduct post-event surveys to garner input from our employees on how to enhance employee events and communications, and we recently completed a customer communications assessment and have strengthened our work in this area through the development of the "Agency Communication Portfolio," which is delivered to agency leadership each month. This document includes: a graphical representation of the total IT spend for the department for the month, current month and year-to-date statistics regarding critical and essential IT system availability, the IT Project Health Index, a three-month rolling window of service desk responsiveness statistics, and OIT's scorecard and good news reports for the month.

Recommendation #: 2a

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should work with the Governor's Office of State Planning and Budgeting, Joint Budget Committee, and General Assembly to move all Executive Branch IT appropriations so as to be under the control of OIT. In addition, OIT should determine whether IT spending is in line with organizational IT goals by:

a. Collaborating more effectively with agencies during the budget process to determine their IT needs.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Agree. Implementation date: December, 2012.

Agency's Written Response in Audit Report:

OIT will work with the Departments, Governor's Office of State Planning and Budgeting, Joint Budget Committee, and General Assembly to determine the best way to control IT budgets and balance statewide versus departmental information technology priorities.

OIT is working to update its current processes to increase collaboration with agencies during the budget process to ensure strategic needs of the departments and the state are compiled annually. This information will then be utilized during the subsequent budget cycle.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Not Implemented

Agency's Comments on Implementation Status of Recommendation:

OIT and OSPB are currently engaged in an "IT Financial Reform" effort to address this issue during the upcoming legislative session. As soon as a draft plan has been formulated, we will engage the Joint Budget Committee for their input. Some of the goals of IT Financial Reform include developing a better, more proactive way to budget and plan for IT resources; allowing budget flexibility to address unforeseen IT needs during the fiscal year; and establishing more strategic, consolidated procurement of IT goods and services.

Recommendation #: 2b

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should work with the Governor's Office of State Planning and Budgeting, Joint Budget Committee, and General Assembly to move all Executive Branch IT appropriations so as to be under the control of OIT. In addition, OIT should determine whether IT spending is in line with organizational IT goals by:

b. Developing policies and procedures that address IT investment and funding decisions.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Agree. Implementation date: December, 2012.

Agency's Written Response in Audit Report:

OIT will work with the Departments, Governor's Office of State Planning and Budgeting, Joint Budget Committee, and General Assembly to determine the best way to control IT budgets and balance statewide versus departmental information technology priorities.

OIT is working to update its current processes including developing policies and procedures that address IT investment and funding decisions to ensure strategic needs of the departments and the state are compiled annually. This information will then be utilized during the subsequent budget cycle.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Not Implemented

Agency's Comments on Implementation Status of Recommendation:

OIT and OSPB are currently engaged in an "IT Financial Reform" effort to address this issue during the upcoming legislative session. As soon as a draft plan has been formulated, we will engage the Joint Budget Committee for their input. Some of the goals of IT Financial Reform include developing a better, more proactive way to budget and plan for IT resources; allowing budget flexibility to address unforeseen IT needs during the fiscal year; and establishing more strategic, consolidated procurement of IT goods and services.

Recommendation #: 2c

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should work with the Governor's Office of State Planning and Budgeting, Joint Budget Committee, and General Assembly to move all Executive Branch IT appropriations so as to be under the control of OIT. In addition, OIT should determine whether IT spending is in line with organizational IT goals by:

c. Centralizing IT procurement of overlapping IT projects and services.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Agree. Implementation date: October, 2012.

Agency's Written Response in Audit Report:

OIT will work with the Departments, Governor's Office of State Planning and Budgeting, Joint Budget Committee, and General Assembly to determine the best way to control IT budgets and balance statewide versus departmental information technology priorities.

OIT has an active project to address the intake and delivery process for all information technology resource requests (i.e. hardware, software, services, and systems). These processes include all aspects of the resource lifecycle such as requirements definition, procurement, contracting, project management, vendor management, deployment and subsequent disposal of the resource. Utilizing the LEAN principles, OIT has engaged a subset of staff from all departments to help design and implement these processes

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Partially Implemented

Agency's Comments on Implementation Status of Recommendation:

OIT recently implemented "IT Storefront," which is a life cycle management process for all IT assets and services and includes a web-based requisition process for IT goods and services. This process gives the OIT executive leaders and procurement team the visibility into departmental IT ordering. With this visibility, OIT is able to make more strategic decisions about IT procurement, including consolidated buying. In addition, OIT and OSPB are currently engaged in an "IT Financial Reform" effort to address this issue during the upcoming legislative session. As soon as a draft plan has been formulated, we will engage the Joint Budget Committee for their input. Some of the goals of IT Financial Reform include developing a better, more proactive way to budget and plan for IT resources; allowing budget flexibility to address unforeseen IT needs during the fiscal year; and establishing more strategic, consolidated procurement of IT goods and services.

Recommendation #: 3

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should perform a full physical inventory and reconciliation of hardware and software assets, including accounting for and reconciling records to inventory and inventory to records, as needed. In addition OIT should implement mechanisms to keep this inventory current and remain fully informed of all key IT assets across the state to improve decision making, reduce overall risk, effectively manage costs, and improve operational efficiencies. OIT should also consider implementing more stringent policies for managing IT assets and, if funding becomes available, consider the cost and benefits of implementing an integrated IT asset management system.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Partially Agree. Implementation date: July, 2012.

Agency's Written Response in Audit Report:

OIT agrees that asset management is critical to the state and should be maintained and managed at the enterprise level. OIT has an active project to build processes and procedures to track and manage all information technology resources from the moment they are procured throughout their entire lifecycle. This project will go live on July 1, 2012 and OIT will test and refine the processes and procedures throughout the first quarter of the fiscal year. While OIT agrees that enterprise asset management is critical, OIT does not have the resources available to complete a full statewide inventory of all information technology assets and is why OIT has initiated the project to track all newly purchased assets from procurement to disposal.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Partially Implemented

Agency's Comments on Implementation Status of Recommendation:

OIT recently hired a Statewide IT Asset Manager whose function is to implement an IT asset management strategy for the state. This includes developing processes and procedures for IT asset management, which include developing processes and procedures for tracking an IT asset from ordering, receiving, deployment, retirement, and annual inventorying. The IT asset management strategy will help OIT make better decisions about IT asset needs.

Recommendation #: 4a

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should improve its HR function and more aggressively manage organizational change by:

a. Performing a RACI-like analysis of OIT staff roles and responsibilities to properly align the functional and reporting structure, standardize job titles and identify inefficiencies that impact the OIT consolidation initiative.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Agree. Implementation date: October, 2012.

Agency's Written Response in Audit Report:

OIT agrees that improvements in our Human Resources operations is a priority and is included as one of the six priorities identified in our Fiscal Year 2011-12 Playbook. OIT is very committed to its employees and wants to ensure they have a productive work environment in which to operate.

OIT is completing a nationwide search for an experienced human resources director who can address both the strategic and tactical needs of our office. OIT expects to have this director on board in April 2012 and the immediate priorities of the position will be to identify the operational gaps in our human resource functions and address those gaps. In addition, OIT has an active occupational study underway with the Department of Personnel & Administration to review the current class structure and working titles.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Partially Implemented

Agency's Comments on Implementation Status of Recommendation:

OIT has hired a Director, an Operations Manager, and a Total Rewards professional for our Office of Human Resources. Priorities have been identified via Playbook initiatives. In addition, an audit by a third party (Mountain States Employers Council), is scheduled to begin in November 2012 for purposes of identifying operational and compliance gaps in our human resource functions. The occupational study performed by the Department of Personnel & Administration is complete, and OIT is implementing a human capital resource strategy. Guidelines, procedures, and policies are currently being developed for implementation in concert with the Office of the Governor's launch of a new employee manual, anticipated to be completed in FY 13.

Recommendation #: 4b

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should improve its HR function and more aggressively manage organizational change by:

b. Implementing resource management planning to handle staff attrition and aging of the workforce, identify skill gaps and implement training and tools to mitigate skill gaps.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Agree. Implementation date: July, 2012.

Agency's Written Response in Audit Report:

OIT agrees that improvements in our Human Resources operations is a priority and is included as one of the six priorities identified in our Fiscal Year 2011-12 Playbook. OIT is very committed to its employees and wants to ensure they have a productive work environment in which to operate.

The first priority of the new human resources director will be to complete a Human Capital Resource Strategy to address attrition, succession planning, skills and skill gaps and the aging workforce.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Partially Implemented

Agency's Comments on Implementation Status of Recommendation:

The Human Resources Director has crafted a Human Capital Business Plan to address attrition, succession planning, skills and skill gaps and the aging workforce. These initiatives are captured in our OIT Balanced Scorecard and are components of our FY13 Playbook initiatives. Guidelines, procedures, and policies are currently being developed for implementation in concert with the Office of the Governor's launch of a new employee manual, anticipated to be completed in FY 13.

Recommendation #: 4c

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT should improve its HR function and more aggressively manage organizational change by:

c. Implementing robust knowledge management tools to allow staff the flexibility to perform multiple functions and address succession planning.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Agree. Implementation date: July, 2012.

Agency's Written Response in Audit Report:

OIT agrees that improvements in our Human Resources operations is a priority and is included as one of the six priorities identified in our Fiscal Year 2011-12 Playbook. OIT is very committed to its employees and wants to ensure they have a productive work environment in which to operate.

The first priority of the new human resources director will be to complete a Human Capital Resource Strategy to address attrition, succession planning, skills and skill gaps and the aging workforce.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Partially Implemented

Agency's Comments on Implementation Status of Recommendation:

The Human Resources Director has crafted a Human Capital Business Plan to address attrition, succession planning, skills and skill gaps and the aging workforce. These initiatives are captured in our OIT Balanced Scorecard and are components of our FY13 Playbook initiatives.

Recommendation #: 5

Agency Addressed: Governor's Office of Information Technology

Original Recommendation in Audit Report:

OIT could improve their cost allocation model by implementing billing that is based on real-time consumption of services where practical. More specifically, OIT could eliminate the process of billing based on estimated consumption and implement mechanisms to track, document and report actual utilization for services outlined in the service catalog. Alternatively, OIT could perform its "true up" process on a more frequent basis (e.g., quarterly) to minimize the lag time state agencies experience in understanding their IT consumption. However, resource constraints will need to be considered when assessing the feasibility of this alternative as well.

Agency's Response *(i.e., agree, partially agree, disagree)***:** Partially Agree. Implementation date: December, 2012.

Agency's Written Response in Audit Report:

In the majority of cases, OIT could build tracking mechanisms to collect monthly utilization data by service and use that information to complete monthly billing adjustments. However, neither OIT nor the Departments have the ability to adjust budget outside of the annual or supplemental budget cycles. Therefore, while OIT could under bill or provide monthly credits to departments, OIT would not have the ability to charge a department more than they were budgeted even if they utilized more service(s). Statewide the consumption of information technology goods and services has increasedd by ~5% annually. OIT operates as an internal service organization and is not allowed to carry a large fund balance. If OIT were required to move to real-time billing for all services, OIT would not be able to impact budgets accordingly and would be unable to absorb the resulting budgetary shortfalls.

OIT will work with the Governor's Office of State Planning and Budgeting and the Joint Budget Committee to determine if there is an acceptable budgetary solution which would allow OIT the flexibility to move to a real-time billing model for services.

Current Implementation Status of Recommendation (i.e., Implemented, Implemented and Ongoing, Partially Implemented, Not Implemented, or No Longer Applicable):

Not Implemented

Agency's Comments on Implementation Status of Recommendation:

OIT and OSPB are currently engaged in an "IT Financial Reform" effort to address this issue during the upcoming legislative session. As soon as a draft plan has been formulated, we will engage the Joint Budget Committee for their input. Some of the goals of IT Financial Reform include developing a better, more proactive way to budget and plan for IT resources; allowing budget flexibility to address unforeseen IT needs during the fiscal year; and establishing more strategic, consolidated procurement of IT goods and services.

STATE OF COLORADO

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

601 East 18th Avenue, Suite 250
Denver, Colorado 80203
Phone (303) 764-7700
Fax (303) 764-7725
www.colorado.gov/oit

John W. Hickenlooper
Governor

Kristin Russell
Secretary of Technology and
State Chief Information Officer

M E M O R A N D U M

TO:	Joint Budget Committee and Legislative Audit Committee
FROM:	Kristin Russell, Secretary of Technology and Chief Information Officer
DATE:	October 8, 2012
RE:	Statutory Email Consolidation ("COPE") Reporting

Members of the Joint Budget Committee and the Legislative Audit Committee:

In accordance with Section 24-37.5-105(3.5)(a), C.R.S., I am pleased to present you with a report on our statewide email consolidation project – Google Apps for Government. This project meets the statutory definition of "COPE," which is collaboration, office productivity, and electronic mail software delivered via a "Software as a Service" (or SaaS) model.

Statute requires reporting to the Joint Budget and Legislative Audit Committees for COPE projects. Specifically:

> *If [OIT] initiates any COPE services in a state agency on or after January 1, 2010, through an agreement with the statewide internet portal authority or any private sector provider of information technology resources, it shall file a report with the joint budget committee and the legislative audit committee no later than thirty days after the last day of the fiscal quarter in which the COPE service was initiated.*

On July 12, 2012 OIT entered into a contract with the Statewide Internal Portal Authority (SIPA) to initiate deployment of the Google Apps for Government email and calendar platform for the more than 26,000 employees in the Executive Branch, enabling the state to eliminate disjointed and aging email systems, to provide a single email solution to all employees, and to realize approximately $1.4 million per year in cost avoidance over the next five years. The statewide Go Live date is today - October 8, 2012.

Currently, the State has 15 siloed and disparate email systems that in most cases are not integrated with each other. Moving to Google will allow state agencies to interconnect email and calendar functions through a common statewide address book while maintaining strong security and privacy standards. Google's cloud-based system will allow the state to pay only for what technology is used

and will reduce ongoing maintenance costs. This will enable the state to better plan and budget for email and calendaring services and more quickly adapt to changing demands from individual agencies.

OIT completed a thorough testing and assessment of multiple products, including conducting an independent third-party comparative analysis, before selecting Google. Google's security architecture meets or exceeds that State's standards and Google Apps is the first cloud email system that has achieved Federal Information Security Management Act certification, ensuring data is safe and secure.

This is a unique and exciting opportunity for the State of Colorado. For the very first time, state employees, regardless of their agency or work location, will be able to easily connect, collaborate, create, and share. With the move to Google, employees will have the ability to quickly locate email addresses and see "open" meeting times for their peers in other agencies.

Although the primary goal of this initiative is to provide a single, statewide email and calendaring service, state agencies will also benefit from the many other components of the Google Apps for Government suite, which includes spreadsheets, presentations, word processing, collaboration sites, instant messaging, point-to-point video and soft phone, email filtering, mobile access, archiving, encryption where needed, and a service level agreement that includes full redundancy and 99.999% uptime.

This report is divided into four sections. The first three sections specifically address the statutory reporting requirements. Section I provides the implementation plan and timeline for the project, Section II includes the Google implementation cost-benefit analysis, and Section III presents the results of the comprehensive security assessment that we performed on the Google Apps for Government platform. Section IV, which is not specifically required by statute, describes the email and productivity functionality and features available to state employees through the Google suite.

Thank you very much for your time and interest in this important statewide endeavor. Should you have any questions or require additional information, I can be reached at 303-764-7835 or kristin.russell@state.co.us with any questions that you have.

Sincerely,

Kristin D. Russell
Secretary of Technology and Chief Information Officer
State of Colorado
Governor's Office of Information Technology

COLLABORATION, OFFICE PRODUCTIVITY, & E-MAIL ("COPE") REPORT

OCTOBER 2012

SECTION I – IMPLEMENTATION PLAN

The table below represents key milestones in the implementation schedule for the statewide Google Apps for Government email consolidation initiative. The following state agencies are included in the project and will be migrated over to the Google platform.

- Governor's Office[1]
- Department of Agriculture
- Department of Corrections
- Department of Health Care Policy & Financing
- Department of Human Services
- Department of Labor & Employment
- Department of Local Affairs
- Department of Military and Veterans Affairs
- Department of Natural Resources
- Department of Personnel & Administration
- Department of Public Health & Environment
- Department of Public Safety
- Department of Regulatory Agencies
- Department of Revenue
- Department of Transportation
- Department of the Treasury
- History Colorado

Implementation Task Name	Start Date	Finish Date
Email Consolidation Pre-Planning Activities		
➢ Customer Environment Profiles	4/16/2012	5/04/2012
➢ State Security Requirements	5/11/2012	5/31/2012
➢ Formation of Integrated Project Teams	4/16/2012	5/18/2012
Email Consolidation Project Planning Activities		
➢ Project Organization	6/04/2012	6/15/2012
➢ Project Governance Checklist	6/04/2012	6/08/2012
➢ Validate Project Plan	6/05/2012	6/18/2012
➢ Create Ongoing Communications Plan	4/17/2012	10/30/2012
➢ Create Training Plan	6/05/2012	7/02/2012
➢ Create Data Migration Strategy	6/05/2012	10/01/2012
Email Consolidation Deployment Activities		
➢ Contract with SIPA Executed	7/12/2012	7/12/2012
➢ Configuration & Transition Preparation	5/03/2012	7/17/2012
➢ Technical Deployment & Readiness	6/13/2012	9/17/2012
Email Consolidation Go-Live Dates & Related Activities		
➢ OIT 100 Go-Live (pilot of 100 OIT employees)	7/30/2012	7/30/2012
▪ Communications	6/28/2012	8/08/2012
▪ Training	7/03/2012	8/15/2012
➢ Early Adopter Go-Live (pilot of 1,000 state employees)	8/27/2012	8/27/2012
▪ Communications	7/25/2012	9/03/2012
▪ Training	7/30/2012	9/03/2012
➢ Global Go-Live (26,000 state employees in Executive Branch)	10/08/2012	10/08/2012

[1] This includes the Colorado Energy Office, the Office of Economic Development and International Trade, and the Office of Information Technology.

▪ Communications	7/19/2012	10/15/2012
▪ Training	9/6/2012	10/12/2012
▪ Full Deployment Support	10/08/2012	11/02/2012
Email Consolidation Project Close-Out Activities		
➢ Review Project Close-Out Criteria	11/05/2012	11/06/2012
➢ Confirm All Deliverable Documentation	11/05/2012	11/09/2012
➢ Close All Remaining Open Issues	11/05/2012	11/09/2012
➢ Hold Project Close-Out Meeting	11/12/2012	11/12/2012

SECTION II – COST BENEFIT ANALYSIS

Currently, the State of Colorado spends $5.2 million annually supporting 29,000 electronic mailboxes across the Executive Branch. The average monthly cost per mailbox is $15. This includes users in the following departments/agencies:

- Governor's Office, including the Colorado Energy Office, the Office of Economic Development and International Trade, and the Office of Information Technology
- Colorado Department of Agriculture
- Colorado Department of Corrections
- Colorado Department of Health Care Policy & Financing
- Colorado Department of Human Services
- Colorado Department of Labor & Employment
- Colorado Department of Local Affairs
- Colorado Department of Military and Veterans Affairs
- Colorado Department of Natural Resources
- Colorado Department of Personnel & Administration
- Colorado Department of Public Health & Environment
- Colorado Department of Public Safety
- Colorado Department of Regulatory Agencies
- Colorado Department of Revenue
- Colorado Department of Transportation
- Colorado Department of the Treasury
- History Colorado

The current email environment in the Executive Branch is fragmented, inefficient, and costly. There are 15 disparate email installations based in two separate platforms (Microsoft & GroupWise) at four different release levels with limited redundancy and failover. Supporting this complex environment is challenging from a personnel perspective, and many of these email instances reside in data centers that lack adequate security, power, and cooling.

Below are the 15 separate email environments that are currently in production:

1. OIT (includes Agriculture, Governor's Office, History Colorado, Personnel & Administration, & Treasury)
2. Corrections
3. Energy Office
4. Health Care Policy & Financing
5. Human Services
6. Labor & Employment
7. Local Affair
8. Military & Veterans Affairs
9. Natural Resources
10. Office of Economic Development and International Trade
11. Public Health & Environment
12. Public Safety
13. Regulatory Agencies
14. Revenue
15. Transportation

Google Apps for Government Cost Analysis

Moving to a single cloud-based platform will allow state employees to interconnect email and calendar functions through a common statewide address book and enable the State to pay only for services are used and thereby significantly reduce maintenance costs. As a result, the State will be able to better plan and budget for email and calendaring services and more quickly adapt to changing demands from individual agencies.

The estimated average annual cost for Google Apps for Government is $3,780,513. This includes implementation costs and costs associated with required state personnel. The table below provides a breakdown of these costs over a five-year period.

Google Apps for Government	**Annual Cost**					
	Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Totals**
Migration	$326,200	$326,200	$326,200	$326,200	$326,200	**$1,631,000**
Licensing	$1,276,000	$1,363,000	$1,363,000	$1,392,000	$1,392,000	**$6,786,000**
Archive	$840,000	$840,000	$840,000	$840,000	$840,000	**$4,200,000**
Encryption	$420,000	$420,000	$420,000	$420,000	$420,000	**$2,100,000**
Operation	$456,239	$190,052	$190,052	$190,052	$190,052	**$1,216,447**
Annual State Personnel Costs	$593,823	$593,823	$593,823	$593,823	$593,823	**$2,969,115**
Totals	**$3,912,262**	**$3,733,075**	**$3,733,075**	**$3,762,075**	**$3,762,075**	**$18,902,562**

**implementation costs amortized across five years*

The overall Google cost includes a wide range of benefits, such as installation, migration, ten-year data archive, spam filtering, cloud hosting, mobile access, storage, software licensing, full redundancy, access from anywhere across the globe, and 99.999% uptime.

The expected monthly email cost per mailbox is $9.67. For an encrypted mailbox, the cost is $12.58.

With the Google Apps for Government platform in place, the estimated cost avoidance is approximately $1.4 million per year. This includes eliminating 89 servers and associated software and an estimated annual savings of $47,000 in power and cooling costs.

It should be noted that although the Department of Education, Department of Law, Institutes of Higher Education, Secretary of State's Office, and the Legislative and Judicial Branches are not included in these estimates and are not currently in the Google migration project, these state agencies are invited to participate at any time.

Comparison of Google and Microsoft

OIT performed a comparative analysis of the Google and Microsoft email and productivity cloud offerings and found that it would have cost the State $9.2 million annually (including State Personnel) to go with the Microsoft solution. Below is a breakdown of annual costs for both Google and Microsoft and the difference between the two. Google presented itself as the more cost-effective and innovative solution for the State of Colorado.

Email & Productivity Suite	**Annual Cost**					
	Year 1	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Totals**
Microsoft Office 365 E3 Annual Cost	$9,188,097	$9,188,097	$9,188,097	$9,188,097	$9,188,097	**$45,940,485**
Google Apps Annual Cost	$3,912,262	$3,733,075	$3,733,075	$3,762,075	$3,762,075	**$18,902,562**
Cost Difference	**$5,275,835**	**$5,455,022**	**$5,455,022**	**$5,426,022**	**$5,426,022**	**$27,037,923**

SECTION III – SECURITY ASSESSMENT

Google's security strategy provides controls at multiple levels of data storage, access, and transfer. The strategy includes the following ten components:

- Google corporate security policies
- Organizational security
- Data asset management
- Access control
- Personnel security
- Physical and environmental security
- Infrastructure security
- Systems and software development and maintenance
- Disaster recovery and business continuity

Office of Information Security Assessment Process

The Office of Information Security (OIS) performed a comprehensive assessment of the Google Apps for Government solution. The assessment process involved a Non-Disclosure Agreement (NDA) review of multiple internal Google documents and processes by the Colorado State Chief Information Security Officer (CISO) with the Google CISO and Google security staff.

The State CISO reviewed and validated the 300+ page Google Federal System Security Plan (SSP) required by the federal government. The purpose of the SSP is to provide an overview of the security requirements of the system and describe the security controls in place or planned responsibilities and expected behavior of all individuals who access the Google Apps for Government solution. SSP summary information can be requested by contacting the State's Chief Information Security Officer, Jonathan Trull, at Jonathan.Trull@state.co.us.

The initial assessment found Google Apps for Government to be compliant with OIS and Federal security requirements. The following section provides a summary of the validated security program and security controls implemented and maintained by Google.

Google Corporate Security Policies

Google's security policies cover a wide array of security related topics ranging from general policies that every employee must comply with such as account, data, and physical security, along with more specialized policies covering internal applications and systems that specific employees are required to follow.

These security policies are periodically reviewed and updated. Employees are also required to receive regular security training on topics such as the safe use of the Internet, working from remote locations, and how to label and handle sensitive data. Additional training is routinely given on policy topics of interest, including in areas of emerging technology, such as the safe use of mobile devices and social technologies.

Organizational Security

Google's security organization is broken down into several teams that focus on information security, global security auditing, and compliance, as well as physical security for protection of Google's hardware infrastructure. These teams work together to address Google's overall global computing environment.

Information Security Team

Google employs a full-time Information Security Team that is composed of over 250 experts in information, application, and network security. This team is responsible for maintaining the company's perimeter and internal defense systems, developing processes for secure development and security review, and building customized security infrastructure. It also has a key role in the development, documentation, and implementation of Google's security policies and standards.

Global Internal Audit and Global Compliance Team

In addition to a full-time information security team, Google also maintains several functions focused on complying with statutory and regulatory compliance worldwide. Google has a Global Compliance function that is responsible for legal and regulatory compliance as well as a Global Internal Audit function responsible for reviewing and auditing adherence to said compliance requirements, such as Sarbanes-Oxley and Payment Card Industry standards (PCI).

Physical Security Team

Google maintains a global team of staff, headquartered in the United States, dedicated to the physical security of Google's office and data center facilities. Google's security officers are qualified with training to protect high security enterprises with mission-critical infrastructures.

Data Asset Management

Google's data assets - comprising customer and end-user assets as well as corporate data assets – are managed under strict security policies and procedures. In addition to specific controls on how data is handled, all Google personnel handling data assets are also required to comply with the procedures and guidelines defined by internal security policies.

Information Access

Google has controls and practices to protect the security of customer information. The layers of the Google application and storage stack require requests coming from other components be authenticated and authorized. Service-to-service authentication is based on a security protocol that relies on specific infrastructure built into the Google production platform to broker authenticated channels between application services.

Access by production application administrative engineers to production environments is similarly controlled. A centralized group and role management system is used to define and control engineers' access to production services.

Data and Access Protection

Administrative access to the production environment for debugging and maintenance purposes is based on secure shell (SSH) connections. SSH connections into the production environment are authenticated using short-lived public-key certificates that are issued to individual administrative users; issuance of such certificates is in turn authenticated via two-factor authentication.

Customer access to Google Apps for Government is accomplished through SSL protected connections.

Google provides many services that make use of the Hypertext Transfer Protocol Secure (HTTPS) for more secure browser connections. Services such as Gmail, Google Search, and Google+ support HTTPS by default for users who are signed into their Google Accounts. Information sent via HTTPS is encrypted from the time it leaves Google until it is received by the recipient's computer.

Email Encryption

Google Message Encryption (GME), powered by Postini, is a secure, hosted service that provides automated and end-user driven email and attachment encryption capabilities to protect sensitive data and email communication.

Reference: http://www.google.com/postini/

Archiving and E-Discovery

Google Message Discovery, powered by Postini, provides comprehensive email archiving and message discovery capabilities. Google Message Discovery allows the state to:

- create a centralized and searchable email repository for the state
- quickly search across the archive to find emails and save result sets
- set central email policies to manage content and compliance requirements

Data At-Rest Encryption

Google already provides several means of industry leading security layers to keep protected information confidential and private as required by industry standards and federal regulations. For example, all hard drives within Google data centers employ full disk encryption. Also, customer data is further obfuscated by being parsed and stored on several different servers. Therefore, neither physical nor logical access to a single server would reveal customer data.

As an added level of protection, OIT has procured an optional encryption solution for state entities if necessary, called CipherCloud, to further encrypt all emails (subject, body, and attachments) on the way to Google's servers, so the contents are secure and cannot be accessed by anyone outside the state while the email is stored within the Google Apps for Government cloud. Colorado is the first state in the nation to make this solution available to state agencies.

Media Disposal

When retired from Google's systems, disks containing customer information are subjected to a data destruction process before leaving Google's premises. First, their policy requires the disk to be logically wiped by authorized individuals using a process approved by the Google Security Team and that meets DOD sanitization requirements.

Next, another authorized individual is required to perform a second inspection to confirm the disk has been successfully wiped. These erase results are logged by the drive's serial number for tracking.
Finally, the erased drive is released to inventory for reuse and redeployment. If the drive cannot be erased due to hardware failure, it must be securely stored until it can be physically destroyed. Each facility is audited on a weekly basis to monitor compliance with the disk erase policy.

Access Control

Google employs a number of authentication and authorization controls that are designed to protect against unauthorized access.

Authentication Controls

Google requires the use of a unique User ID for each employee. This account is used to identify each person's activity on Google's network, including any access to employee or customer data. This unique account is used for every system at Google. Google makes widespread use of two-factor (2-step) authentication mechanisms, such as certificates and one-time password generators. Two-factor authentication is required for all access to production environments and resources through Google's Single Sign On system.

Two-factor authentication will be required for customer access to Google Apps for Government through a web browser.

Authorization Controls

Access rights and levels are based on a Google employee's job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities.

Google Apps for Government provides a feature rich set of access controls for customer access and sharing of resources. Audit capabilities exist to ensure the integrity and effectiveness of access controls implemented through the customer portal.

Personnel Security

Google employees are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

Upon hire, Google verifies an individual's education and previous employment, and performs internal and external reference checks. Where local labor law or statutory regulations permit, Google also conducts criminal, credit, immigration, and security checks.

All Google staff, who access and maintain Google Apps for Government, are required to pass and maintain a Federal GSA approved background check, to include fingerprints.

Physical Security

Google has policies, procedures, and infrastructure to handle both physical security of its data centers as well as the environment from which the data centers operate.

Google's data centers are geographically distributed and employ a variety of physical security measures. The technology and security mechanisms used in these facilities may vary depending on local conditions such as building location and regional risks. The standard physical security controls implemented at each Google data center include the following: custom designed electronic card access control systems, alarm systems, interior and exterior cameras, and security guards. All of the State's data will reside only in the United States.

Google has released a seven-minute video to demonstrate their level of security, data protection and server reliability protocols Google follows at their data centers to protect its customers.

Reference: Google Data Center Security Video
http://youtu.be/1SCZzgfdTBo

Infrastructure Security

Google security policies and practices provide a series of threat prevention and infrastructure management procedures.

Malware Protection

Google takes malware threats to its networks and its customers very seriously and uses a variety of methods to address malware risks. This strategy begins with manual and automated scanners that analyze Google's search index for websites that may be vehicles for malware or phishing. This threat information is integrated into internal security threat protection controls and processes. Additionally, Google utilizes anti-virus software and proprietary techniques in Gmail, on servers, and on workstations to address malware.

Google Message Discovery, powered by Postini, provides enterprise-grade spam and virus protection to all Gmail users.

Monitoring

Google's security monitoring program analyzes information gathered from internal network traffic, employee actions on systems, and outside knowledge of vulnerabilities. At multiple points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections.

This analysis is performed using a combination of open source and commercial tools for traffic capture and parsing. A proprietary correlation system built on top of Google technology also supports this analysis. Network analysis is supplemented by examining system logs to identify unusual behavior, such as unexpected activity in former employees' accounts or attempted access of customer data.

Vulnerability Management

Google employs a team that has the responsibility to manage vulnerabilities in a timely manner. The Google Security Team scans for security threats using commercial and in-house-developed tools, automated and manual penetration efforts, quality assurance (QA) processes, software security reviews, and external audits. The vulnerability management team is responsible for tracking and managing vulnerabilities throughout the Google Apps for Government and Corporate infrastructures.

Incident Management

Google has an incident management process for security events that may affect the confidentiality, integrity, or availability of its systems or data. This process specifies courses of action and procedures for notification, escalation, mitigation, and documentation.

Google staff are trained in forensics and handling evidence in preparation for an event, including the use of third party and proprietary tools. Testing of incident response plans is performed for identified areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities.

The Google incident management process will be tied into the State of Colorado incident management process.

Network Security

Google employs multiple layers of defense to help protect the network perimeter from external attacks. Only authorized services and protocols that meet Google's security requirements are permitted to traverse the company's network. Unauthorized packets are automatically dropped.

Operating System Security

Based on a proprietary design, Google's production servers are based on a version of Linux that has been customized to include only the components necessary to run Google applications, such as those services required to administer the system and serve user traffic. The system is designed for Google to be able to maintain control over the entire hardware and software stack and support a secure application environment.

Google servers are maintained by proprietary software that continually monitors systems for binary modifications. If a modification is found that differs from the standard Google image, the system is automatically returned to its official state. These automated, self-healing mechanisms are designed to enable Google to monitor and remediate destabilizing events, receive notifications about incidents, and slow down potential compromise on the network. Using a change management system to provide a centralized mechanism for registering, approving, and tracking changes that impact all systems, Google reduces the risks associated with making unauthorized modifications to the standard Google operating system.

System Development and Maintenance

It is Google's policy to consider the security properties and implications of applications, systems, and services used or provided by Google throughout the entire project lifecycle. Google's "Applications, Systems, and Services Security Policy" calls for teams and individuals to implement appropriate security measures in applications, systems, and services being developed, commensurate with identified security risks and concerns. The policy states that Google maintains a security team chartered with providing security-related guidance and risk-assessment.

Security Consulting and Review

With regards to the design, development, deployment, and operation of applications and services, the Google Security Team provides the following primary categories of consulting services to Google's Product and Engineering Teams:

- Security Design Reviews — design-level evaluations of a project's security risks and corresponding mitigating controls, as well as their appropriateness and efficacy.
- Implementation Security Reviews — implementation-level evaluation of code artifacts to assess their robustness against relevant security threats.
- Security Consulting — ongoing consultation on security risks associated with a given project and possible solutions to security concerns, often in the form of an exploration of the design space early in project life cycles.

Implementation-Level Security Testing and Review

Google employs a number of approaches intended to reduce the incidence of implementation-level security vulnerabilities in its products and services:

- Implementation-level security reviews, which are conducted by members of the Google Security Team typically in later stages of product development, aim to validate that a software artifact has protection against relevant security threats.
- Automated testing for flaws in certain relevant vulnerability classes. We use both in-house developed tools and some commercially available tools for this testing.
- Security testing performed by Software Quality Engineers in the context of the project's overall software quality assessment and testing efforts.

Disaster Recovery and Business Continuity

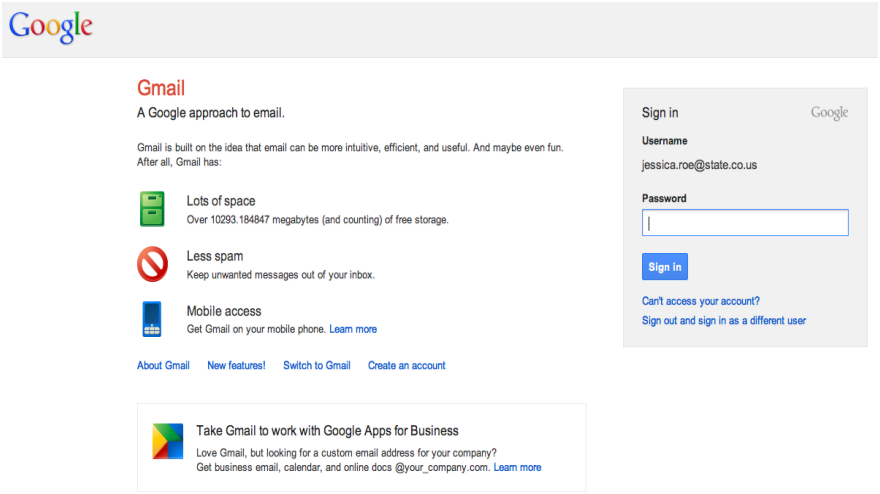
To minimize service interruption due to hardware failure, natural disaster, or other catastrophe, Google implements a disaster recovery program at all of its data centers. This program includes multiple components to minimize the risk of any single point of failure, including the following:

- Data replication and backup: Google application data is replicated to multiple systems within a data center, and in some cases also replicated to multiple data centers.
- Google operates a geographically distributed set of data centers that is designed to maintain service continuity in the event of a disaster or other incident in a single region. High-speed connections between the data centers help to support swift failover. Management of the data centers is also distributed to provide location-independent, around-the-clock coverage, and system administration.

SECTION IV – GOOGLE EMAIL AND PRODUCTIVITY FEATURES AND FUNCTIONALITY

With Google Apps for Government, state employees, regardless of their agency or work location, will be able to easily connect, collaborate, create, and share, creating a statewide community that is more than 26,000 strong. They can be productive from anywhere, using any device with an internet connection, and can easily access their email, calendar, files, and documents all from a single location.

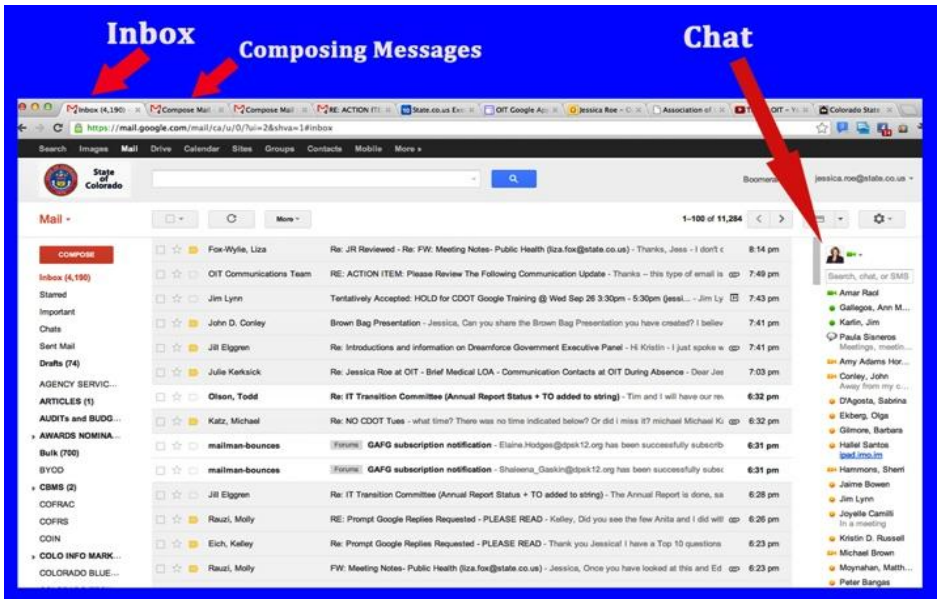
Logging in remotely is easy and all work is automatically saved in the cloud.



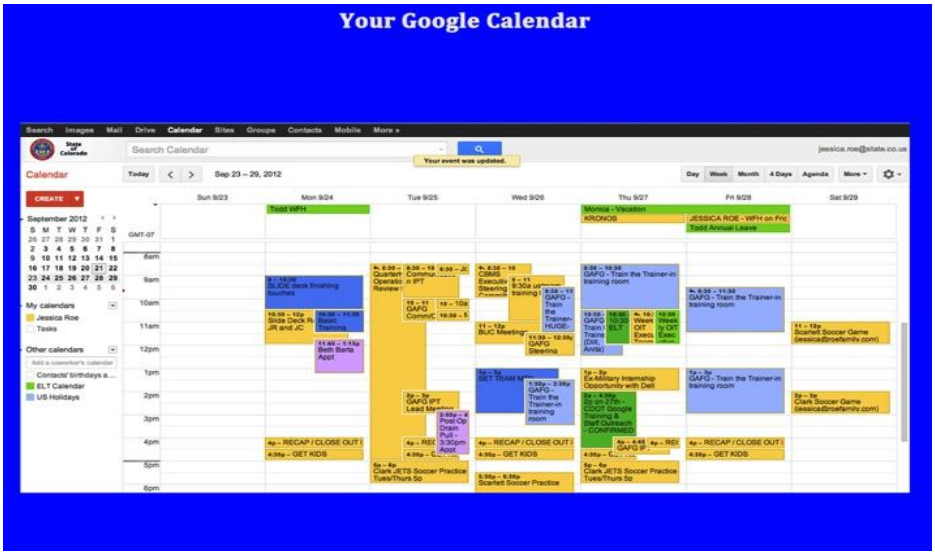
Once a user logs in, they will instantly have access to a suite of user-friendly features and functionality, including:

- Email
- Calendar
- Contacts
- Spreadsheets
- Presentations
- Word processing
- Collaboration sites
- Instant messaging/chat
- Point-to-point video and soft phone
- Email filtering
- Archiving
- Encryption

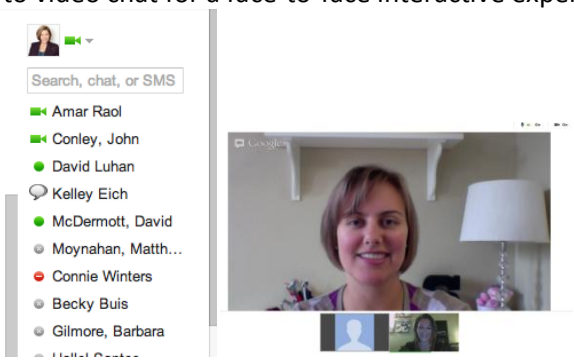
For the very first time, state employees will have the ability to quickly locate email addresses for anyone in the State. They can also “chat” with a colleague in another city or even a co-worker down the hall and have the quick, informal conversations needed to be productive and accomplish their tasks.



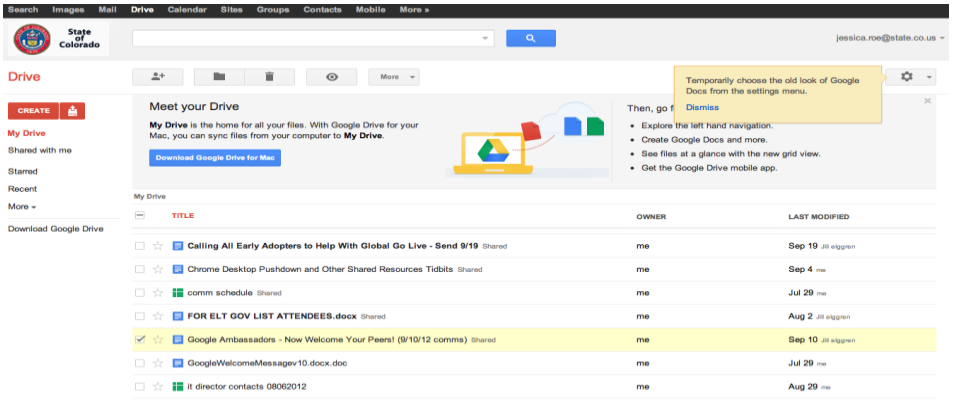
They will be able to easily check the availability of and schedule meetings with their peers in other agencies.



There is even the capability to video chat for a face-to-face interactive experience.



Further, with Google Docs and Google Drive, employees will have the ability to create, share, and edit many types of files – docs, spreadsheets, presentations, and more – in real time. The need to email documents back and forth for editing is eliminated when using this tool.



Google Apps for Government enables individuals and groups to work better together by making it easy for everyone – employees, partners, contractors, anyone – to collaborate effortlessly across teams, agencies, and locations. The worker productivity benefits of the Google email service and collaboration tools are numerous, and state agencies will be more efficient and effective as a result.

Office of the State Auditor

Dianne E. Ray, CPA
State Auditor

MEMORANDUM

Date: November 28, 2012

To: Members of the Legislative Audit Committee

From: Dianne E. Ray, CPA, State Auditor

Re: Contract Award for Email Services

The OSA received a request in July 2012 from Representative Brian DelGrosso to audit the Governor's Office of Information Technology's (OIT) contract award for email services to the State (audit request attached). Representative DelGrosso has approved an alternative to pursuing an audit at this time, which is to request that OIT discuss the following issues at the LAC hearing in December 2012. These questions will be discussed immediately following the OIT presentation of the COPE Report.

1. What mechanisms does OIT have in place for monitoring whether the implementation of Google email services is successful? For example, how will OIT get feedback from staff about implementation? Are there fixed points in the future (e.g., 6 months, a year) when OIT will do a formal assessment of the implementation?

2. What cost-benefit analysis did OIT do to show that contracting with Google through SIPA (and its subcontractor Tempus Nova) was a more cost-effective option than contracting with Google directly?

3. The COPE report about the Google project explains that a cost-comparison was made between Google and Microsoft. How did OIT obtain the figures from Google and Microsoft to make this comparison? For example, did you sent out requests for figures to both companies? If so, were the specifications in the requests to each company identical? In other words, how does OIT know that the numbers from Google and Microsoft included in the COPE report represent an apples-to-apples comparison?

4. What cost-benefit analysis did OIT do to demonstrate that other companies besides Google and Microsoft could not provide a better email product at a cheaper price?

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

5. The COPE report details the extensive security features of the Google email product. How will OIT ensure that the Google email product complies with the State's information security plan? In other words, what monitoring will OIT do to ensure that these security features are working as intended?

6. What analysis did OIT do to demonstrate that Google email will provide the most effective security features for email and not put sensitive state information at risk? As part of this analysis, did OIT look into the alleged security problems with Google email reported by other state and local governments?

State Representative
BRIAN DELGROSSO
Colorado State Capitol
200 East Colfax Avenue, Room 271
Denver, Colorado 80203
Capitol: 303-866-2947
E-mail: brian@briandelgrosso.com

Chairman:
Finance Committee
Member:
Appropriations Committee
Judiciary Committee

COLORADO

HOUSE OF REPRESENTATIVES

STATE CAPITOL

DENVER

80203

July 13, 2012

Dianne E. Ray
State Auditor
Office of the State Auditor
200 East 14th Avenue
Denver, CO 80203

Ms. Ray,

I am writing to request that the Legislative Audit Committee conduct a thorough review and audit to evaluate the Governor's Office of Information Technology's (OIT) decision to spend millions of taxpayer dollars on what appears to be a sole source contract award to Google for email services for approximately 26,000 state employees.

On March 8, 2012, the Colorado General Assembly was notified that OIT selected Google to provide email and calendar services for state employees in the Executive Branch. This is a significant IT procurement from a private vendor, and it raises a number of concerns and questions that should be addressed.

The foundation of Colorado's procurement system is that state requirements must be fulfilled through full and open competition to the greatest practical extent. Competition serves to maximize the state's purchasing power by ensuring that the state obtains reasonable prices. Competition also furthers the state's policies of increasing public confidence in the Colorado procurement system and ensuring fair and equitable treatment of potential vendors by eliminating any appearance of impropriety or favoritism. Why did OIT not issue a Request for Proposal (RFP) with clearly stated factors for evaluation to give all interested parties a full and equal opportunity to compete for the opportunity to provide the state with a secure, cloud-based email and calendar solution in accordance with Colorado procurement laws and regulations?

It is my understanding that OIT intends to acquire the Google services through a contract signed two years ago between the Colorado Statewide Internet Portal Authority (SIPA) and a Google reseller. What criteria and justification did OIT use to determine that this was an appropriate contractual vehicle to procure these services?

The committee should explore whether OIT is exempt from following the state's procurement code by awarding the contract for Google services to SIPA. Why should this major procurement be exempt from the competition requirements of our state's procurement code when SIPA is not providing the services, but rather, is acting as an intermediary? And in this era of rapidly changing technologies, is it in the best interest of Colorado taxpayers to make a major IT acquisition based on a two-year-old contract? The committee should evaluate the role of SIPA, and determine what changes are required to ensure that agencies do not use SIPA contracting authority to attempt to circumvent Colorado procurement laws and regulations.

Because of the perceived lack of a fair competitive process used to award this contract, I also have concerns about OIT's assessment of security risks and OIT's evaluation of the vendors' privacy policies and their impact on state data. I am concerned that state employees will be forced to adhere to Google's privacy policies, which, it is my understanding, have come under scrutiny from consumer groups, 36 state Attorneys General, the Federal Trade Commission, and regulators around the world. How do Google's privacy policies impact Colorado state employees? The committee should investigate whether Colorado state employee data will be used for target advertising by Google and explore the relationship between Google's advertising and privacy policies with state employee use of Google's email, calendar, web search, and other services provided by Google. Will Google benefit and profit from the collection of Colorado state employee information?

Furthermore, I am concerned about the negative impact that this decision could have on Colorado law and public safety agencies. It is my understanding that two years after winning a contract to provide cloud email services for the City of Los Angeles, the city and Google had to abandon plans to move 13,000 law enforcement employees to Google since Google could not meet the unique security needs of crucial law enforcement agencies. How will OIT and Google avoid similar problems in Colorado?

In light of the appearance that OIT avoided following Colorado's procurement laws for this major IT procurement, this contract requires additional oversight from the legislature. If OIT continues to feel that it will not revisit this award decision and will not conduct a thorough, open, and fair competition, then at a minimum, OIT should provide the Audit Committee with monthly reports detailing the status of implementation of the Google services. These reports need to include, at a minimum, detailed updates on how the vendor and OIT are meeting all of their deadlines, adhering to budgets, managing migration, preventing security breaches, and ensuring that the privacy of state employees and state-held data is being protected.

Thank you in advance for your interest in ensuring the integrity and effectiveness of the Colorado procurement system, and your commitment to security and privacy.

Sincerely,

Representative Brian DelGrosso

cc: Representative Cindy Acree, Chair
Representative Angela Williams, Vice-chair
Senator Lucia Guzman
Representative James Kerr
Senator Steve King
Senator Scott Renfroe
Representative Su Ryden
Senator Lois Tochtrop
Kristin Russell, OIT Secretary of Technology and State Chief Information Officer