COLORADO
Secretary of Technology &
Chief Information Officer
Governor's Office of Information Technology

Suma Nallapati
601 East 18th Avenue, Suite 250
Denver, CO 80203

September 11, 2015

Dianne E. Ray, CPA
State Auditor
Colorado Office of the State Auditor
1525 Sherman St., 7th Floor
Denver, CO 80203

Dear Ms. Ray:

In response to your request, we have prepared updated status reports regarding the implementation of recommendations contained in the November 2014 *Information Security Assessment* (Public Report) and the *Information Technology Security Assessment Report* (CONFIDENTIAL Report). The attached reports provide a brief explanation of the actions taken by the Governor's Office of Information Technology to implement each recommendation.

If you have any questions, please do not hesitate to contact me at 303.764.7708 or by email at suma.nallapati@state.co.us.

Sincerely,

Suma Nallapati

Secretary of Technology and Chief Information Officer

# AUDIT RECOMMENDATION STATUS REPORT

**AUDIT NAME: Information Security Assessment (Public Report)**
**AUDIT NUMBER: 1404P-A**
**DEPARTMENT: Governor's Office of Information Technology**

**DATE OF STATUS REPORT: September 11, 2015**

**SUMMARY INFORMATION**

| Rec. Number | Agency's Response | Original Implementation Date | Implementation Status | Revised Implementation Date (If applicable) |
|---|---|---|---|---|
| 1a | Agree | December 2015 | Partially Implemented | July 2016 |
| 1b | Agree | December 2015 | Partially Implemented | N/A |
| 1c | Agree | July 2015 | Implemented | N/A |
| 1d | Agree | July 2015 | Partially Implemented | October 2015 |
| 2a | Agree | December 2015 | Partially Implemented | N/A |
| 2b | Agree | December 2015 | Partially Implemented | December 2016 |
| 2c | Agree | December 2015 | Partially Implemented | December 2016 |
| 4a | Agree | July 2015 | Partially Implemented | July 2016 |
| 4b | Agree | September 2015 | Partially Implemented | July 2016 |
| 4c | Agree | July 2015 | Partially Implemented | July 2016 |

**DETAIL OF IMPLEMENTATION STATUS**

## Recommendation No. 1:

The Governor's Office of Information Technology (OIT) should improve IT security governance by:

a. Continuing the consolidation efforts of IT services, including updating outdated operating systems and reconfiguring systems that are using default passwords.

**Current Implementation Status for Recommendation No. 1, part a:** Partially Implemented.

**Agency's Update:**

*Through continued consolidation efforts, OIT is implementing new controls, tools, and technology on an ongoing basis to improve the security posture. Several initiatives and projects are in place to update outdated operating systems and to reconfigure systems using default passwords at an enterprise level. All the instances of default passwords identified during the audit were remediated immediately. OIT anticipates that this part of the recommendation will be fully implemented by July 2016.*

b. Holding vendors and OIT staff accountable for best practices, including industry hardening standards, in administering OIT systems.

**Current Implementation Status for Recommendation No. 1, part b:** Partially Implemented.

**Agency's Update:**

*OIT agrees that systems should be hardened as required by OIT standards that are based on industry best practices. OIT has revised, documented, and published policies and standards for administering and configuring OIT systems. OIT is currently working on operationalizing the annual review process for all relevant OIT staff and vendors to strengthen accountability and ensure compliance with established policies and procedures. OIT expects to implement this recommendation by its original implementation date of December 2015.*

c. Updating its IT security policies, including the Colorado Information Security Policies (CISPs), on a regular basis including the removal of conflicting language and timely communicating these updates to all OIT staff.

**Current Implementation Status for Recommendation No. 1, part c:** Implemented.

*OIT documented, published, and communicated The Colorado Information Security Policies in February 2015. The new set of policies removed any conflicting language identified. OIT has established multiple avenues to communicate policies to its staff. Examples of these include:*

*quarterly newsletters, trainings, operational managers meetings, all-hands meetings, and other efforts. As part of ongoing compliance with state statute the OIT will review and update all Information Security Policies annually.*

d. Implementing a comprehensive internal training program that will ensure all OIT staff are adequately trained on the current IT policies and procedures, and informed on the current strategic plan and its goals and objectives. The program should include accountability and consequences for non-adherence components. Further, implementation of the program should include defined monitoring periods.

**Current Implementation Status for Recommendation No. 1, part d:** Partially Implemented. New implementation date: October 2015.

**Agency's Update:**

*OIT has established multiple avenues to communicate policies and strategic plans, including goals and objectives, to relevant staff such as quarterly newsletters, trainings, operational managers meetings, all-hands meetings, and other efforts. Further, as part of the implementation of online training across the enterprise by October 2015, training will be provided to all OIT staff regarding policies and procedures of OIT on an annual basis and as new policies are created. Sanctions are not addressed via training other than to point out that violating the policies could result in corrective action in accordance with personnel rules. OIT online training platform allows for continuous monitoring and reporting of student progress. All lesson takers progress will be monitored and progress reported to agencies to ensure compliance with training requirements.*

## Recommendation No. 2:

The Governor's Office of Information Technology should improve their ability to manage an interruption of the two enterprise applications by:

a. Working with the business owners of the enterprise application to develop a comprehensive disaster recovery plan for each enterprise application.

**Current Implementation Status for Recommendation No. 2, part a:** Partially Implemented.

**Agency's Update:**

*For one enterprise application a comprehensive disaster recovery plan was implemented. For the other enterprise application we expect to fully implement this recommendation by its original implementation date of December 2015.*

b. Developing comprehensive recovery testing strategies and performing recovery testing on a regular basis.

**Current Implementation Status for Recommendation No. 2, part b:** Partially Implemented, New implementation date: December 2016.

**Agency's Update:**

*For one enterprise application a comprehensive recovery testing strategy was developed and recovery testing was performed. For the other enterprise application, while the disaster recovery plan for this application will be documented by December 2015 it will require additional time to test the plan due to lack of adequate network infrastructure, tools and techniques which is currently being reviewed for gaps and possible solution. We expect to fully implement this part of the recommendation by December 2016.*

c. Updating the disaster recovery plan based on feedback and analysis of the testing done in subpart B.

**Current Implementation Status for Recommendation No. 2, part c:** Partially Implemented, New implementation date: December 2016.

**Agency's Update:**

*For one enterprise application the disaster recovery plan was updated based on feedback and analysis of the testing done in subpart B While the disaster recovery plan for this application will be documented by December 2015 it will require additional time to test the plan due to lack of adequate network infrastructure, tools and techniques which is currently being reviewed for gaps and possible solution. Once the solution is in place the disaster recovery plan will be tested and updated based on the feedback and analysis done in Subpart B. We expect to fully implement this recommendation by December 2016.*

## Recommendation No. 4:

The Governor's Office of Information Technology should improve logical access controls for the two enterprise application(s) reviewed by:

a. Working with the business owners of the two enterprise applications to review all active production user accounts to ensure they are assigned to current employees and to assess the appropriateness of access granted.

**Current Implementation Status for Recommendation No. 4, part a:** Partially Implemented, New implementation date: December 2016.

**Agency's Update:**

*For one enterprise application all active production user accounts were revised to ensure they are assigned to current employees and that access granted was appropriate. For the other enterprise application we expect to implement this recommendation by July 2016. The delay is due to of lack of adequate resources to perform the review. The agency is working on alternate solutions to help remediate this recommendation by July 2016*

b. Ensuring that passwords for administrative accounts for the one critical application, identified and communicated under separate cover, are consistent with the State Information Security Policies, and ensuring that administrative access is adequately logged and monitored.

**Current Implementation Status for Recommendation No. 4, part b:** Partially Implemented, New implementation date: July 2016.

**Agency's Update:**

*The password for the administrative accounts identified were remediated immediately to comply with security policies. We are currently working on ensuring that administrative access is adequately logged and monitored and expect this recommendation to be fully implemented July 2016. The delay is due to identification of prerequisites and competing priorities that need to be in place to fully implement this recommendation.*

c. Developing a segregation of duties matrix for the one critical application identified and communicated under separate cover.

**Current Implementation Status for Recommendation No. 4, part c:** Partially Implemented. New Implementation date: June 2016.

**Agency's Update:**

*Segregation of duties are identified and documented, however, it has not been operationalized systematically due to identification of prerequisites and competing priorities that need to be in place to fully implement this recommendation. We are now implementing the infrastructure needed to launch the new configuration application, which will fully operationalize this recommendation by July 2016.*

# Office of the State Court Administrator

**Gerald A. Marroney**
*State Court Administrator*

**Mindy Masias**
*Chief of Staff*

**Terri Morrison**
*Judicial Legal Counsel*

**DIRECTORS**

**Sherry Stwalley**
*Court Services & Legislative Relations*

**David Kribs, CFO**
*Financial Services*

**Eric D. Brown**
*Human Resources*

**Chad Cornelius, CIO**
*Information Technology Services*

**Eric Philp**
*Probation Services*

September 11, 2015

Dianne E. Ray, CPA
State Auditor
Colorado Office of the State Auditor
1525 Sherman St., 7th Floor
Denver, CO 80203

Dear Ms. Ray:

In response to your request, we have prepared updated status reports regarding the implementation of recommendations contained in the November 2014 *Information Security Assessment* (Public Report) and the *Information Technology Security Assessment Report* (CONFIDENTIAL Report). The attached reports provide a brief explanation of the actions taken by the Judicial Branch to implement each recommendation.

The Judicial Department believes information technology security is critical to the successful administration of the judicial system. As such, the Department has addressed all aspects of the findings contained in the confidential report and is working towards a comprehensive implementation strategy for developing a disaster recovery plan in light of the audit findings in the public report.

If you have any questions, please do not hesitate to contact me at 720-625-5000 or by email at gerald.marroney@judicial.state.co.us .

Sincerely,

Gerald A. Marroney
State Court Administrator

# AUDIT RECOMMENDATION STATUS REPORT

**AUDIT NAME: Information Security Assessment (Public Report)**
**AUDIT NUMBER: 1404P-A**
**DEPARTMENT: Judicial Branch**

**DATE OF STATUS REPORT: 9/10/2015**

**SUMMARY INFORMATION**

| Rec. Number | Agency's Response | Original Implementation Date | Implementation Status | Revised Implementation Date (If applicable) |
|---|---|---|---|---|
| 3a | Agree | June 2016 | Not Implemented | |
| 3b | Agree | June 2016 | Not Implemented | December 2017 |
| 3c | Agree | June 2016 | Not Implemented | December 2017 |
| 5a | Agree | June 2016 | Partially Implemented | |
| 5b | Agree | June 2016 | Partially Implemented | |
| 5c | Partially Agree | November 2015 | Implemented | |

**DETAIL OF IMPLEMENTATION STATUS**

## Recommendation No. 3:

The Judicial Branch should improve their ability to manage an interruption of the one enterprise application by:

a. Developing a comprehensive disaster recovery plan for the one enterprise application.

**Current Implementation Status for Recommendation No. 3, part a:** Not Implemented.

**Agency's Update:**

*The Judicial Department received the necessary funding in Fiscal Year (FY) 2016 to engage IT consulting services to assist with the development of a Disaster Recovery plan. The enterprise application depends on the same underlying IT infrastructure used by many other Judicial Department enterprise applications. Therefore, the Judicial Department's intent is to include all enterprise applications in the Disaster Recovery plan. The Judicial Department plans to implement the recommendation by June 30th, 2016.*

b. Developing comprehensive recovery testing strategies and performing recovery testing on a regular basis.

**Current Implementation Status for Recommendation No. 3, part b:** Not Implemented.

**Agency's Update:**

*To meet the recommended remediation, the Judicial Department will include as part of its DR plan, comprehensive testing and recovery strategies for each enterprise application by June 30th, 2016.*

*To meet the recommended remediation for performing recovery testing, the Judicial Department will need to complete the replacement of its primary mid-range iSeries servers that not only stores data for the one enterprise application, but all other enterprise applications to include the Department's case management system. This is an extensive project scheduled to begin in July 2016 that will involve moving all production servers from the Judicial Department's current production data center to the Ralph L. Carr data center. Additionally, since the application depends on the same underlying IT infrastructure used by other Judicial Department enterprise applications, the Judicial Department will need to complete the Disaster Recovery plan to fully understand the scope of implementing and testing the application, as well as all other enterprise applications at the disaster recovery facility. The Judicial Department anticipates that after completing the Disaster Recovery plan, there will be a need to procure additional hardware and software, implement network changes and upgrades, and implement any necessary software changes to support the Disaster Recovery plan. In order to fully implement and perform recovery testing of the entire Disaster Recovery system on all enterprise applications, the Judicial Department will require an extension to implement this recommendation with a completion date of December 2017.*

c. Updating the disaster recovery plan based on feedback and analysis of the testing done

**Current Implementation Status for Recommendation No. 3, part c:** Not Implemented.

**Agency's Update:**

*The Judicial Department agrees with the need to update the Disaster Recovery plan to address issues and weaknesses identified in testing and fully intends to undertake this effort based on the project plan and timeline identified in the response to Recommendations 3A and 3B.*

## Recommendation No. 5:

The Judicial Branch should improve logical access controls for the one enterprise application reviewed by:

a. Reviewing all active production user accounts to ensure they are assigned to current users and to assess the appropriateness of access granted.

**Current Implementation Status for Recommendation No. 5, part a:** Partially Implemented.

**Agency's Update:**

*The Department is reviewing processes and procedures to determine the correct changes to implement this recommendation. Remediation is on target to be completed by June 2016.*

b. Ensuring that administrative access is adequately logged and monitored.

**Current Implementation Status for Recommendation No. 5, part b:** Partially Implemented.

**Agency's Update:**

*The Department is reviewing processes and procedures to determine the correct changes to implement this recommendation. Remediation is on target to be completed by June 2016.*

c. Developing a segregation of duties matrix for the one critical application identified and communicated under separate cover.

**Current Implementation Status for Recommendation No. 5, part c:** Implemented.

**Agency's Update:**

*The Department has a RASCI chart detailing responsibilities and duties in direct relation to critical applications. The chart outlines the segregation of duties as they can be applied to the Department.*