CONTRACT AMENDMENT NUMBER 1

I. PARTIES

This Amendment to the above-referenced Original Contract (hereinafter called the Contract) is entered into by and between R & A, Solutions, Inc. (dba Randa Solutions, hereinafter referred to as Contractor), 5000 Meridian Blvd. Suite 400, Franklin, Tennessee 37067, and the State of Colorado (hereinafter called the State) acting by and through the Colorado Department of Education (hereinafter called CDE), 201 East Colfax, Denver, Colorado 80203.

II. EFFECTIVE DATE AND ENFORCEABILITY

This Amendment shall not be effective or enforceable until it is approved and signed by the Colorado State Controller or designee (hereinafter called the Effective Date). The State shall not be liable to pay or reimburse Contractor for any performance hereunder including, but not limited to, costs or expenses incurred, or be bound by any provision hereof prior to the Effective Date.

III. FACTUAL RECITALS

The Parties entered into the Contract to create an online performance management system to be used for the entry of principal and teacher education evaluation data pursuant to Senate Bill 10-191 and State Board of Education educator effectiveness rules and policy.

IV. CONSIDERATION-COLORADO SPECIAL PROVISIONS

The Parties acknowledge that the mutual promises and covenants contained herein and other good and valuable consideration are sufficient and adequate to support this Amendment. The Parties agree to replacing the Colorado Special Provisions with the most recent version (if such have been updated since the Contract and any modification thereto were effective) as part consideration for this Amendment.

V. LIMITS OF EFFECT

This Amendment is incorporated by reference into the Contract, and the Contract and all prior amendments thereto, if any, remain in full force and effect except as specifically modified herein.

VI. MODIFICATIONS

The Amendment and all prior amendments thereto, if any, are modified as follows:

A. Paragraph IV. shall be amended by adding the following new definitions:

"Confidential Information" means information, data, records, and documentary materials belonging to the State regardless of physical form or characteristics, including but not limited to any non-public State records, sensitive State data, protected State data, State personnel records, personally identifiable information ("PII"), and other information or data concerning individuals, which has been communicated, furnished or disclosed by the State to Contractor. Notwithstanding the foregoing, Confidential Information shall not include State Data and Records.

"Personally Identifiable Information (PII) includes, but is not limited to the student's name; the name of the student's parent or other family members; the address of the student or student's family; a personal identifier, such as the student's social security number, student number, or biometric record; other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

PII also means a dataset that is linked to a specific individual and that would allow a reasonable person in a school community, who does not have knowledge of the relevant circumstances, to identify the individual with reasonable certainty.

"State Data and Records" means information, data, records, and documentary materials belonging to the State regardless of physical form or characteristics, including but not limited to any public State records, non-sensitive State data, and other information or data concerning individuals that is not deemed confidential but nevertheless belongs to the State, which has been communicated, furnished or disclosed by the State to Contractor which (i) is subject to disclosure pursuant to the Colorado Open Records Act, C.R.S. Sections 24-72-200.1, *et seq.*; (ii) is already known to Contractor without restrictions at

the time of its disclosure by Contractor; (iii) is or subsequently becomes publicly available without breach of any obligation owed by Contractor to the State; (iv) is disclosed to Contractor, without confidentiality obligations, by a third party who has the right to disclose such information; or (v) was independently developed without reliance on any Confidential Information.

B. Paragraph V.A. shall be amended by extending the performance period through June 30, 2016.

C. Paragraph VII.A.5.d shall be deleted and replaced with the following new paragraph:

d. Contractor's User Interface (UI) technologists will work with CDE Stakeholders to design user friendly screen formats that incorporate the required Measures of Student Learning, Rubric and Quality Standards, and that will work in the web browser, including iPad and Android tablets.

D. Paragraph VII.B.7. shall be deleted.

E. Paragraph VII.B.8.h. shall be deleted.

F. Paragraph VII.D.3. shall be deleted.

G. Paragraph VII. shall be amended by adding the following new paragraph P.

P. Escrow

1. For each period that this Contract is active and associated annual hosting fees are paid in full, Contractor shall establish and then maintain for the remaining term of this Contract (and for so long as Contractor is obligated to provide hosting, maintenance and support services for the Software, under this Contract or any other agreement), a source code escrow deposit agreement for the Software with an escrow agent mutually agreed upon by the Parties, with CDE identified as a beneficiary. "Source Code" means the human-readable version of the Software that can be compiled into machine-readable code. Within 30 days of the Effective Date, Contractor shall add and maintain the State as a beneficiary of the Escrow Deposit Agreement during the Contract term including any extensions and Contractor shall pay all fees charged by the escrow agent to add and maintain the State as a beneficiary. The Source Code of the Software shall be released to the State from escrow according to the procedure described in the Escrow Deposit Agreement upon the occurrence of the events described therein. At least annually, Contractor shall deposit with the agreed escrow agent Source Code for all Software and any updates and upgrades released by Contractor (this specifically excludes all State customizations and configurations).

2. The State is hereby granted a limited, non-transferable, non-assignable, non-sub-licensable (except as provided below), non-exclusive license to use and modify, execute, and compile the Source Code, solely in the event in the occurrence of a Release Condition as set out under the terms of the Escrow Deposit Agreement, solely for the purpose of supporting the Software for the State, and only to the extent necessary to: (a) correct errors and support the number of copies of the Software legally installed by the State in accordance with the associated Software License Agreement, and to which such Source Code relates, or (b) to achieve interoperability with other programs.

3. The Source Code shall at all times remain the sole and exclusive property of Contractor. Upon the occurrence of a Release Condition as defined under the Escrow Deposit Agreement, the State agrees to, and shall require any third party service provider to agree to:

   a. Maintain the confidentiality of the released Source Code at all times;

   b. Use the Source Code only within the premises of the State;

   c. Keep the Source Code, at all times, in a secure area, such that only those individuals who have a need to know shall be permitted to access the Source Code;

   d. Keep a record of the name and title of the individual(s) having access to the Source Code and a summary of the use of the Source Code; and

   e. Exercise its best efforts to avoid publication, disclosure or unauthorized dissemination and use of the Source Code, which shall be no less than those efforts the State employs with respect to its own highly proprietary information and trade secrets.

4. Upon the occurrence of a Release Condition as defined under the Escrow Deposit Agreement, the State further agrees that it shall ensure that the secure area within which the Source Code shall be located shall have:

   a. Physical security controls that isolate the secure area from physical access by anyone not directly authorized to access or use the Source Code;

b. Logical access controls that enforce positive control over access to the Source Code, the applications, and operating systems functions that interact with the Source Code;

c. Code integrity controls that verify the integrity of the Source Code; and

d. Connectivity controls that ensure that all network connections to the Source Code are under the positive control of those personnel with direct responsibility for the security of the Source Code.

H. Paragraph VIII.A. shall be amended by revising deliverables 3 and 4 and adding deliverables 7 through 12 as follows:

CONTRACTOR DELIVERABLES	TIMELINE	COST
3. Complete the design and development for the web-based Colorado State Model Performance Management System. Modifications to deliverable item 3 are for purposes of adding specificity to the required design and development of the performance management system and revising the timeline for delivery. There is no change to the cost for this deliverable. a. Gather report to display bar charts of aggregate rubric ratings by standard and element (compare all) b. Gather report to show matrix data c. Gather report to show matrix data by selected school d. Allow charter school principals to set their own evaluator(s) e. Major system revisions to allow editing of MSL/MSO worksheet and Final Effectiveness Rating after the academic year has already closed f. System revisions to allow principals and other administrators to view historical evaluation data per security requirements g. Goal-setting and Performance Planning PDF report (export from webpage)	Estimated release on or before May 20, 2015 for 3.a through 3.g.	$0
4. Create video and written training materials for CDE personnel and Stakeholders to use the Colorado State Model Performance	February 1, 2015 through	$0

CONTRACTOR DELIVERABLES	TIMELINE	COST
Management System. The modifications to deliverable item 4 are for the purpose of revising the timeline for delivery. There is no change to the cost for this deliverable.	May 29, 2015	
7. Produce a detailed scope of work for the amendment items identified in deliverable 8 with timeline/schedule for each requested enhancement to be approved by CDE staff.	April 27, 2015	$25,000
8. Design and develop the following enhancements to the web-based Educator Performance Management System:		
a. Add a "formal/informal" column on the observations table. Randa item number 16835. Required item.		$4,500
b. Add capability to select one or more templates to be released/finalized. Randa item number 17346. Required item.		$6,750
c. Add Observation Standard comments to appear in the Evaluator Assessment evidence list. Randa item number 22144. Required item.		$4,500
d. Provide backup method for direct login when single sign on goes down for extended time. Randa item number 16469. Required item.		$20,000
e. Provide a heat map report (gather tool revision in Excel). Randa item number 15542.		$18,000
f. Provide capability to copy previous academic years' Measures of Student Learning (MSL) templates for quick editing. Randa item number 13874.		$27,000
g. Provide capability to create a copy of a MSL template for a different group than the group defined on the original template. Randa item number 15783.		$13,500
h. Provide capability to view professional practice ratings from current year and last year while completing goal setting for the next academic year. Randa item number 9551.		$34,000
i. Provide capability to view professional practice ratings from current year and last year while completing Professional Growth Plan. Item "i." is dependent on item "h." being		$0

CONTRACTOR DELIVERABLES	TIMELINE	COST
completed. Randa item number 12722.		
j. Provide capability for educator goals/growth plan for current year to be pre-entered from last year's data. Randa item number 2545.		$11,000
k. Provide capability for educator end-of-year review remaining goals/actions to be pushed into Goal-Setting and Performance Planning form. Randa item number 22187.		$11,000
l. Add an LEA-specific announcement/documents to all of my users on the dashboard page. Randa item number 15786.		$11,000
m. Provide capability for LEA settings to roll to the next academic year. Randa item number 16234.		$4,500
n. Provide an option to roll content from the self-assessment from year to year by standard. Randa item number 22127.		$36,500
o. Provide an option to roll content from the evaluator assessment from year to year by standard. Randa item number 22128.		$4,500
p. Provide professional development Tab for generic entry of assignments per work utilizing a basic version of a district customization. Randa item number 22189.		$13,500
q. Provide a report to monitor educator growth over time (year to year). Randa item number 16236.		$11,000
r. Provide capability to notify users when a form is awaiting user's signature. Randa item number 13826.		$6,750
s. Provide email notification to educators who have not completed a specified step in the process. (Nudge button to email when filtered on evaluation page). Randa item number 6983.		$18,000
t. Include the Standard Description text within the Assessment Review grid. Randa item number 15220		$500
u. Provide a search field below the username (in the top right hand corner). Randa item number 16240.		$6,750
v. Make pie charts accessible via the evaluations tab. Randa		

CONTRACTOR DELIVERABLES	TIMELINE	COST
item number 17351		$18,000
w. Provide capability to review a roster with MSL templates assigned that can be filtered by MSL template type. Randa item number 17348.		$11,000
x. Provide capability to select "other" as a mentor/person overseeing an action step in my PGP. Randa item number 22122.		$2,000
y. Add an alternative Evaluator Assessment rubric for districts to use. Randa item number 22125.		$13,500
z. Provide capability to bulk upload elements of the user profile including grade, content area and probationary status. Randa item number 8163.		$16,000
aa. Provide capability to add specific educators' evaluation activities for secondary evaluators. Randa item number 15785.		$9,000
bb. Provide capability to filter educators on profile data for MSL template assignment. Randa item number 6666.		$11,000
cc. Provide capability to pull a report of evaluation force closures by "reason" code (e.g., Refusal to Sign, Officially Promoted, Terminated, etc.) Randa item number 6660.		$4,500
dd. Provide ability to upload new evidence and attach it from within the Evaluator Assessment. Randa item number 12507.		$2,000
ee. Provide capability to batch assign goals with action items on the professional growth plan. Randa item number 22338.		$25,000
ff. Provide ability to batch assign collective measures and ratings for the measures of student learning worksheet. Randa item number 16239.		$39,000
gg. Provide a report that shows all evaluation activities that were forcibly closed by an administrator. Randa item number 9208.		$4,500
hh. Provide capability to filter notifications in work stream to limit the number of items that are displayed. Randa item		$6,750

CONTRACTOR DELIVERABLES	TIMELINE	COST
number 22121. ii. Show the name of the evaluator that signed each form/activity. Randa item number 18009. jj. Provide ability to maintain settings for the number of items in tables/lists (10, 20, 50). Randa item number 15770. kk. Provide a one-click option to select all practices for a column (select all "basic" for standard 1a) in self-assessment. Randa item number 15788. ll. Provide a one-click option to select all practices for a column (select all "basic" for standard 1a). Randa item number 15787. mm. Provide capability to compare the evaluator assessment ratings/review page to the self-assessment results. Randa item number 12892. nn. Provide reference Resource Guide information to assist in selecting professional practices when completing self-assessments. Randa item number 12858. oo. Provide ability to track a goal with no action steps (PGP, Goal-Setting). Randa item number 22343. pp. Provide ability to reset training accounts at any time. Randa item number 22344.		$2,000 $4,500 $4,500 $4,500 $9,000 $4,500 $9,000 $9,000 NOT TO EXCEED $472,500 for item 8
9. Update training videos and application manuals limited to enhancements identified in item 8 of this amendment.	Upon end user need from July 1, 2015 through June 30, 2016	$45,000
10. Advanced Support/Data Services		$31,605
11. Annual fee for base TOWER software license, hosting and help	Invoice on June	Dependent

CONTRACTOR DELIVERABLES	TIMELINE	COST
desk fees, as determined by number of users in system: Any educator, administrator or other State personnel who should continue to be observed or administering the observation process utilizing the TOWER system represents an annual software license user. 0 – 9,999 users $ 78,000 10,000 – 19,999 users $100,000 20,000 – 29,999 users $132,000 30,000 – 49,999 users $156,000	30, 2015 Services provided from July 1, 2015 through June 30, 2016	on number of users in system up to a maximum of $156,000*.
12. Initial fees and annual fee for escrow service for compliance with Paragraph VII.P	June 30, 2015	$3,895
TOTAL		$734,000

*Estimated as $132,000 for 2015-2016

I. Paragraph VIII.B. shall be amended by increasing the maximum amount payable under the Contract by $734,000 for a total maximum amount payment of $2,706,000.

J. Paragraph XI. shall be deleted and replaced with the following new Paragraph XI.:

Contractor shall comply with and shall cause each of its Subcontractors and any other party performing Work under this Contract to comply with the provisions of this Section if it becomes privy to Confidential Information and/or State Data and Records in connection with its performance hereunder.

A. Confidentiality

Contractor shall keep all Confidential Information confidential at all times and comply with all laws and regulations concerning confidentiality of Confidential Information. Any request or demand by a third party for Confidential Information and/or State Data and Records in the possession of Contractor shall be immediately forwarded to the State's principal representative.

B. Notification

Contractor shall notify its agent, employees, Subcontractors and assigns who may come into contact with Confidential Information that each is subject to the

confidentiality requirements set forth herein, and shall provide each with a written explanation of such requirements before permitting them to access such Confidential Information.

C. Use, Security, and Retention

Confidential Information and/or State Data and Records of any kind shall not be distributed or sold to any third party or used by Contractor or its agents in any way, except as authorized by this Contract or approved in writing by the State. Contractor shall provide and maintain a secure environment that ensures confidentiality of all Confidential Information and/or State Data and Records wherever located. Confidential Information and/or State Data and Records shall not be retained in any files or otherwise by Contractor or its agents, except as permitted in this Contract or approved in writing by the State. All Confidential Information and/or State Data and Records of any kind shall be stored, processed, or transferred only in or to facilities located within the United States.

D. Protection

If Contractor provides physical or logical storage, processing or transmission of Confidential Information and/or State Data and Records, Contractor shall provide, and shall cause its Subcontractors to provide, physical and logical protection for State hardware, software, applications and data that meet or exceed industry standards and requirements as set forth in the Contract. Contractor shall provide the State with access, subject to Contractor's reasonable access security requirements, seven (7) days a week, twenty-four (24) hours a day, for the purpose of inspecting and monitoring access and use of Confidential Information, State Data and Records, maintaining State systems, and evaluating physical and logical security control effectiveness. Contractor, if it retains, stores, or is given Confidential Information and/or State Data and Records, at all times shall maintain, and shall cause its Subcontractor's to maintain, network, system, and application security, which includes network firewalls, intrusion detection, and annual security testing. Contractor, if it retains, stores, or is given Confidential Information and/or State Data and Records, shall comply and shall cause its Subcontractors to comply, with State and federal regulations and guidelines related to security, confidentiality and auditing. Contractor, if it retains, stores, or is given Confidential Information and/or State Data and Records shall ensure, and shall cause its Subcontractors to ensure, that security is not compromised by unauthorized access to computers, program, software, databases, or other electronic environments and shall promptly report all breaches or attempted breaches to a representative of the Office of Information Security ("OIS"). Neither Contractor nor its Subcontractors shall have any rights to use or access

any Governor's Office of Information Technology ("OIT") or other State agency data or information, except with the prior approval of OIT or the State. Contractor shall review, on a semi-annual basis, the Colorado Cyber Security Program (CCSP), posted at http://www.colorado.gov/cs/Satellite/Cyber/CISO/1207820732279, and its related documents, including its policies and procedures to ensure compliance with the standards and guidelines published therein. Contractor shall cooperate, and shall cause its Subcontractors to cooperate, with the performance of security audit and penetration tests by OIS or its delegate. Contractor shall follow, and shall cause its Subcontractors to follow, the State's Data Handling and Disposal policy, which can be found at www.colorado.gov/oit/security_policies. Contractor shall perform, and shall cause its Subcontractor's to perform, in a form reasonably acceptable to the State, current background checks on all of its respective employees and agents performing services or having access to State Confidential Information and/or State Data and Records provided under this Contract. A background check performed within thirty (30) days prior to the date such employee or agent begins performance or obtains access shall be deemed to be current.

E. Security-Notice

Contractor is responsible for the security of all Confidential Information and/or State Data and Records provided to it by the State. If Confidential Information and/or State Data and Records is provided to Contractor or any Subcontractor by the State, Contractor shall comply with and shall cause its Subcontractors to comply with the State's Cyber Security Policies, which the OIS has promulgated pursuant to CRS §§24-37.5-401 through 406 and 8 CCR §1501-5. The Policies are posted at http://www.colorado.gov/cs/Satellite/Cyber/CISO/1207820732279.

F. Security Breach Remediation

If Contractor becomes aware of a data security breach involving any Confidential Information and/or State Data and Records that Contractor has received from the State ("Security Breach"), it shall notify the State immediately and cooperate with the State regarding recovery, remediation, and the necessity to involve law enforcement, if any. Unless Contractor can establish that Contractor or any of its Subcontractors is not the cause or source of the Security Breach, Contractor shall be responsible for the cost of notifying each Colorado resident and residents of other states whose personal information may have been compromised by the Security Breach. Notice shall be made as soon as possible within the legitimate needs of law enforcement and according to the requirements of the State.

Contractor shall be responsible for performing an analysis to determine the cause of the Security Breach, and for producing a remediation plan to reduce the risk of incurring a similar type of breach in the future. Contractor shall present such analysis and remediation plan to the State within ten (10) days of notifying the State of the Security Breach. The State reserves the right to adjust this plan, in its sole discretion. If Contractor cannot produce the required analysis and plan within the allotted time, the State, in its sole discretion, may perform such analysis, produce a remediation plan, and Contractor shall reimburse the State for the reasonable costs thereof.

G. Disclosure-Liability

Disclosure of Confidential Information and/or State Data and Records by Contractor or any Subcontractor for any reason may be cause for legal action by third parties against Contractor, the State or their respective agents. Contractor shall indemnify, save, and hold harmless the State, its employees and agents, against any and all claims, damages, liability and court awards including costs, expenses, and attorney fees and related costs, incurred as a result of any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees pursuant to this Section. Notwithstanding any other provision of this Contract, Contractor shall be liable to the State for all consequential and incidental damages arising from a Security Breach. The Work under this Contract may require the State to supply data to the Contractor that contains PII. The State, in its sole discretion may securely deliver data that contains PII, Confidential Information and/or State Data and Records directly to the facility where such data is used to perform the Work. PII, Confidential Information and/or State Data and Records is not to be maintained or forwarded to or from any other facility or location except for the authorized and approved purposes of backup and disaster recovery purposes. The Contractor shall ensure that PII, Confidential Information and/or State Data and Records are not retained beyond timeframes established by the State.

H. End of Agreement Data Handling

Upon request by the State made before or within sixty (60) days after the effective date of termination of the Contract, Contractor will make available to the State a complete and secure (i.e. encrypted and appropriately authenticated), download file of all system data in XML format, or other format as agreed to by the Parties in writing, including all schema and transformation definitions, and/or delimited text files with documented, detailed schema definitions along with attachments in their native format. The Parties agree that on the termination of the provision of

data processing services, the Contractor shall, at the choice of the State, return all data, records, PII, Confidential Information and/or State Data and Records transferred, and the copies thereof to the State, or shall destroy all the data, records, PII, Confidential Information and/or State Data and Records and certify to the State that it has done so, unless legislation imposed upon the Contractor prevents it from returning or destroying all or part of the data, records, PII, Confidential Information and/or State Data and Records transferred. In that case, the Contractor warrants that it will guarantee the confidentiality of PII, Confidential Information and/or State Data and Records transferred and will not actively process the data transferred anymore.

I. Disposition of Data

The State retains the right to use the established operational services to access and retrieve Confidential Information and/or State Data and Records stored on Contractor's infrastructure at its sole discretion. The Contractor and Subcontractor warrant that upon request of the State and/or of the supervisory authority, the Contractor will submit its data processing facilities for an audit of the measures referred to in §IX.D. The State reserves all right, title and interest, including all intellectual property and proprietary rights, in and to system data, Confidential Information, State Data and Records and content.

J. Safeguarding Personal Identifiable Information (PII)

If Contractor or any of its Subcontractors will or may receive PII under the Contract, Contractor shall provide for the security of such PII, in a form acceptable to the State, including, without limitation, non-disclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections and audits. Contractor shall take full responsibility for the security of all data in its possession or in the possession of its Subcontractors, and shall hold the State harmless for any damages or liabilities resulting from the unauthorized disclosure of loss thereof.

K. Data Security Assurances

1. Strong access control must be in place on Contractor's servers and workstations. All data must be at a minimum protected with a complex password, workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended. Passwords must be confidential and sharing of passwords

is prohibited, must not be written down or stored in an insecure location, and periodically changed and not reused or a reasonable time period.

2. Unused and terminated user accounts of the Contractor must be disabled and/or deleted immediately; account inactivity must be periodically assessed for potential stale accounts.

3. Care must be exercised by the Contractor on Contractor's servers and workstations in inadvertently sharing data on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes.

4. Systems must be in place for logging and monitoring access and use of data.

5. At a minimum, annual intrusion penetration/vulnerability testing will be implemented.

6. Laptop/mobile device password locks and full disk/storage encryption are required.

7. Data at rest on central computing systems must be encrypted; any backup, backup media, removable media, tape or other copies must also be encrypted, and not used to transport data.

8. Mandatory annual Security awareness training on how to handle PII is required.

9. Appropriate endpoint security anti-virus and anti-malware software must be installed and maintained on computers accessing or processing PII.

10. Transmitting data by Contractor must occur via a secure method such as Secure File Transfer Protocol (SFTP) or comparable and never sent via email or transported on removable media.

11. Physical security in buildings housing PII, along with controlled physical access to buildings and/or data centers.

12. After prescribed use is concluded, data disposal policies must apply for cleaning up all data. This includes secure scrubbing and securely overwriting data from storage, or physically destroying the storage media.

13. Devices used to copy or scan hard copies of data must have encrypted storage and have storage devices appropriately scrubbed when equipment is retired. Hard copy containing PII is discouraged and must be physically secured, not left unattended, and physically destroyed.

14. All data processing systems, servers, laptops, PCs, and mobile devices must be regularly scanned and have all security patches applied in a timely manner.

15. Data stored in cloud based systems must be protected in the same manner as local data, as described throughout this document. Use of free cloud based services is prohibited, and secondary encryption must be used as appropriate to protect data in cloud storage.

16. Cloud environments, when employed, must be fully documented and open to CDE inspection and verification.

17. Access to cloud based computing environments is only permitted via restricted access, by VPN or least privileged access lists, and never accessible directly via the Internet.

VII. START DATE

This Amendment shall take effect on the later of its Effective Date or April 17, 2015.

VIII. ORDER OF PRECEDENCE

Except for the Special Provisions, in the event of any conflict, inconsistency, variance, or contradiction between the provisions of this Amendment and any of the provisions of the Contract, the provisions of this Amendment shall in all respects supersede, govern, and control. The most recent version of the Special Provisions incorporated into the Contract or any amendment shall always control other provisions in the Contract or any amendments.

IX. AVAILABLE FUNDS

Financial obligations of the state payable after the current fiscal year are contingent upon funds for that purpose being appropriated, budgeted, or otherwise made available.

THE PARTIES HERETO HAVE EXECUTED THIS AMENDMENT

Persons signing for Contractor hereby swear and affirm that they are authorized to act on Contractor's behalf and acknowledge that the State is relying on their representations to that effect.

CONTRACTOR

R & A, Solutions, Inc., dba Randa Solutions

By: MARTIN REED
Name of Authorized Individual

Title: CEO
Official title of Authorized Individual

*Signature

STATE OF COLORADO

John W. Hickenlooper, GOVERNOR

Colorado Department of Education
Robert Hammond, Commissioner

By: Robert Hammond, Commissioner

Date: 4-16-15

ALL CONTRACTS REQUIRE APPROVAL by the STATE CONTROLLER

CRS §24-30-202 requires the State Controller to approve all State Contracts. This Contract is not valid until signed and dated below by the State Controller or delegate. Contractor is not authorized to begin performance until such time. If Contractor begins performing prior thereto, the State of Colorado is not obligated to pay Contractor for such performance or for any goods and/or services provided hereunder.

STATE CONTROLLER

Robert Jaros, CPA, MBA, JD

By:
Dave Grier, CDE Controller

Date: 4-16-15