Colorado Department of Education
Original Contract Routing Number 48393
Amendment Contract Routing Number 73430
PO Number 15CWIDA/CORE 2015- 0324

CONTRACT AMENDMENT NUMBER 3

I. PARTIES

This Amendment to the above-referenced Original Contract (hereinafter called the Contract) is entered into by and between the Board of Regents of the University of Wisconsin System, on behalf of the University of Wisconsin-Madison's Wisconsin Center for Education Research, 1025 W. Johnson Street, Madison, WI 53706 (hereinafter called Contractor or WIDA or WCER), 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 (other than those incurred under the original Agreement and Amendment 1), or be bound by any provision hereof prior to the Effective Date.

III. FACTUAL RECITALS

The Parties entered into the Contract to administer and score the Assessing Comprehension and Communication in English State-to-State for English Language Learners" (ACCESS for ELLs®) in Colorado. The purpose of the amendment is to extend the performance period and add funding.

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 V.A. shall be amended by extending the performance period through September 30, 2015.

B. Paragraph VII.A. shall be amended by adding the following new paragraphs VII.A.1.b., VII.A.1.c. and VII.A.2.b.

VII.A.1.b. Colorado's estimated test population for spring 2015 is 114,000 students. For the spring 2014/2015 testing year, CDE shall pay $23 per student. The estimated ACCESS for ELLs cost is $2,622,000 for SFY 2014-2015.

VII.A.1.c. Colorado's estimate test population requiring Braille accommodations for spring 2015 is 15 students. For the spring 2014/2015 testing year, CDE shall pay $160 per student. The estimated Braille ACCESS for ELLs cost is $2,400 for SFY 2014-2015.

VV.A.2.b. CDE agrees to pay the yearly ACCESS for ELLs costs as follows:

Testing Year	Base Price – Per Test Scored	Estimate Tested Population	Total Estimate Cost
2014-2015	$23 – ACCESS for ELLs	114,000	$2,622,000
2014-2015	$160- Braille ACCESS for ELLs	15	$2,400
TOTAL			**$2,624,400**

C. Paragraph X. shall be amended by deleting existing Paragraph X.D. (Disclosure Liability).

D. Paragraph X shall be amended by adding the following new Paragraphs X.D. through X.L.

D. Protection

If Contractor provides physical or logical storage, processing or transmission of confidential or sensitive State data, 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, upon reasonable notice, 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 State data, maintaining State systems, and evaluating physical and logical security control effectiveness. Contractor, if it retains, stores, or is given protected or confidential information, 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 protected or confidential information, shall comply and shall cause its Subcontractors to comply, with State and federal regulations and guidelines related to security, confidentiality and auditing, including but not limited to regulations and guidelines including but not limited to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and 34 C.F.R. Part 99. Contractor, if it retains, stores, or is given protected or confidential information 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 OIS. Neither Contractor nor its Subcontractors shall have any rights to use or access any OIT or other State agency data or information, except with the prior approval of 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, specifically its policies and procedures to ensure compliance with the data handling and disposal policy published therein.

Contractor schedules periodic vulnerability scans of all WCER servers connected to the University campus network. The vulnerability scans include selective probes of communication services, operating systems, and applications to identify system weaknesses that could be exploited by intruders to gain access to the network. Responsibility for taking follow-up action to correct vulnerabilities, e.g., applying security patches to operating systems, is assigned to Contractor Computer Services support staff.

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 provided under the 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 Breach Remediation

If Contractor becomes aware of a data security breach, it shall notify the State as soon as practicable within a 24 hour period 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 breach, Contractor shall be responsible for the cost of notifying each Colorado resident and residents of other states whose personal information have been compromised. 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 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 fifteen (15) days of notifying the State of the data security breach. The State reserves the right to recommend adjustments to this plan. 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. A breach of Personal Identity Information (PII) shall have occurred when there has been unauthorized acquisition of unencrypted PII data (electronic or otherwise) used in performance of the Contract, or any subcontract from the Contractor's or any Subcontractors possession which compromises security, confidentiality, or integrity of such PII. Contractor agrees to be liable for any unauthorized disclosure of PII in its possession or in the possession of its Subcontractors as if Contractor was the owner of the data. Contractor acknowledges that any breach of PII is a material breach of the Contract. Contractor shall notify the State as soon as practicable of any breach, but in no event later than 24 hours after Contractor learns of the breach. Contractor and State will discuss remediation procedures in the event of breach and agree upon final remediation.

F. Disclosure-Liability

Disclosure of State records or other confidential information 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. To the extent authorized by Wisconsin Statutes Sections 893.82 and 895.46(1), Contractor shall hold harmless the State, its employees and agents, against any and all claims, damages, liability and court awards, incurred as a result of any negligent act or omission by Contractor, or its employees, agents, Subcontractors, or assignees pursuant to this Section. The Work under the Contract may require the State to supply data to the Contractor that contains PII. The State, in its sole discretion may securely deliver such data directly to the facility where the data is used to perform the Work. The data 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 the data is not retained beyond timeframes established by the State.

G. 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 State data in XML format, 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 the personal data transferred, and the copies thereof to the State, or shall destroy all the personal data and certify to the State that it has done so.

H. Disposition of Data

The State reserves all right, title and interest, including all intellectual property and proprietary rights, in and to State system data and content.

I. 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. To the extent authorized by Wisconsin Statutes Sections 893.82 and 895.46(1), 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.

E. Exhibit D, WCER's Standard Security Policies and Procedures, referred to in Paragraph XI.D.5. shall be deleted and replaced with the updated Exhibit D, WCER's Standard Security Policies and Procedures, attached hereto and incorporated herein by reference.

F. Paragraph XVIII.C.3 shall be amended by replacing it in its entirety with the following:

WIDA English Language Development Standards and Resource Guide ("WIDA ELD Standards"), including Essential Actions, WIDA Can Do Descriptors by grade level cluster, individual figures, tables and charts from the Resource Guide and future ELD Standards, Can Do Descriptors and Resource Guide editions;

G. Paragraph XVIII.C shall be amended by adding the following new Paragraph XVIII.C.7.

WIDA Early English Language Development Standards; WIDA Early Spanish Language Development Standards, in Spanish and English; WIDA Spanish Language Development Standards; and WIDA Spanish Language Arts Standards (collectively, "WIDA Language Standards");

H. Paragraph XVIII.D shall be amended by adding the following new Paragraph XVIII.D.7.

CDE's license to use the WIDA Language Standards is not subject to any fee and shall remain in effect as long as CDE and/or the Colorado State Board of Education elects to use the WIDA Language Standards as the State's language standards. For purpose of this license, CDE shall include any governmental agency of the State of Colorado. WCER will make the WIDA Language Standards available electronically in PDF format from the WIDA Consortium website. WCER will publically display and provide the WIDA Language Standards for download free of charge for personal and educational purposes. Educational purposes shall include the following: LEA, individual school/teacher, non-profit agency use within the State of Colorado. This license does not include the right for CDE, LEAs or non-profit agencies within the State of Colorado to copy and distribute the WIDA Language Standards beyond de minimis use (de minimis use is less than 100 copies per event, however, making copies for multiple planned events is not de minimis use). WCER will publish or license to publish full color bound copies of the WIDA Language Standards and make available to CDE, LEAs, non-profits and other educators within the State of Colorado at a lower WIDA Consortium member rate. The WIDA Language Standards shall not be modified or publically displayed for electronic storage and retrieval in any manner without express written permission from WCER or except in accordance with published guidelines issued by WIDA. However, linking to the WIDA Consortium website and stating the free availability of the WIDA Language Standards is encouraged. WCER will grant additional permissions upon request but CDE acknowledges that WCER may include additional reasonable restrictions for quality control purposes depending on the nature of the request.

I. Paragraph XVIII.E shall be amended by adding "and STATE Contractors (see below)" to the end of the last sentence.

J. Paragraph XVIII. shall be amended by adding the following new Paragraph XVIII.G.

CDE may contract with third parties ("CDE Contractors") to provide services to LEAs and other educational agencies within the State of Colorado or organizations operating under the authority of CDE that CDE would otherwise provide ("In-service Activities"). Contracts for In-service Activities shall be limited to a set geographic territory set by CDE ("In-service Area") and shall not authorize the provision of any WCER, WIDA or WIDA Consortium service, unless CDE receives prior written authorization from WCER to do so. CDE Contractors may charge a fee to cover the cost of providing In-service Activities. However, CDE Contractors are prohibited from charging a greater fee to LEAs and other educational agencies outside of their In-service Area, if their In-service Area is smaller than the whole state territory.

VII. START DATE

This Amendment shall take effect on the later of its Effective Date or October 1, 2014.

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
The Board of Regents of the University of Wisconsin System, on Behalf of the University of Wisconsin-Madison's Wisconsin Center for Education Research

By: William Barker
Name of Authorized Individual

Title: Director, OIP, UW-Madison, September 24, 2014
Official title of Authorized Individual

9/24/14
*Signature

STATE OF COLORADO

John W. Hickenlooper, GOVERNOR

Colorado Department of Education
Robert Hammond, Commissioner

By: Robert Hammond, Commissioner

Date: 9.29.14

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: 9-29-14

Exhibit D: WCER Standard Security Policies and Procedures

a) *Information Technology Asset Identification*

We uniquely identify each machine with physical asset numbers and maintain a database of the type and model of the device, the user to whom the machine was allocated, and the operating system. We scan machines that are attached to the School of Education domain during login and determine whether the machine requires security patches. Security patches are managed through a Windows System Update Service that runs on a centrally managed server. This allows us to identify machines at risk for attack based on the presence or absence of updates. All login activity is logged on the local machine as well as on the active directory domain server.

In addition to computer hardware, we also maintain a database to track all network hardware. This allows us to track down any failed device or compromised system and either repair it or isolate from the rest of the network. Our network topology map displays the departmental network hardware, e.g. hubs, switches, etc., and how the departmental network connects to the University networking backbone. We monitor this network in real time for outages. Network technicians are notified of outages by pager. We also maintain spares for all key hardware to minimize downtime from equipment failure.

b) *IT Security Policies and Procedures*

We have an overarching security policy for Wisconsin Center for Education Research that explicitly outlines the rights and responsibilities of users and makes clear the need for increased levels of security for research and administrative data. Users are also required to sign a form that acknowledges their understanding of the university's *IT Appropriate Use Policy*[1] as part of the procedure to create a network account. As a part of our user-level security policy, we require that users create and use complex passwords (at least 8 characters, no part of their names, mixed case, and including at least one number or punctuation mark). All passwords must be changed every 90 days and the systems do not allow passwords to be reused.

At the technical level, IT administrators have crafted access policies for users and devices in different organizational units within the School of Education. These policies are based on best practices for the various operating systems (as identified by third-party security organizations such as SANS or CIAC).

The WCER network operates behind a firewall with a default "deny all" policy. Specific ports may be opened to specific IP's to meet identified needs. Any remote access to any computer on the WCER network must be accomplished through VPN. User accounts and access rules are centrally managed through Active Directory.

[1] http://www.doit.wisc.edu/security/policies/ for general best practices as well as appropriate use, password, and networked device policies.

c) *Security Practices for Sensitive Data*
Depending on the sensitivity of the data and the requirements of the data provider, we implement additional security policies at the group (organizational unit) or sub-group level. These policies can be created to restrict access to particular machines or storage areas or can limit the access of particular individuals to meet narrow security requirements. We have supported a number of U.S. Department of Education-funded studies and are familiar with National Center for Education Statistics (NCES) security practices and audit procedures. We have never failed an NCES audit.

In many cases, when working with administrative and other individual student data, we follow NCES data security practices and create mapping tables for translating between sensitive identifiers (student or staff IDs, social security numbers, etc.) and internally created identifiers. The sensitive data is kept in encrypted tables and is only accessible by database administrators. These database administrators have no research duties and do not allow research access to the original data. The administrators only view encrypted versions of the original data using typical data management tools. Original media files or other data transport media are kept offline on optical or other media in a lock box in a fireproof tape safe. Only the database administrators have access to this lockbox.

d) *Use Anti-virus and Security Update Software*
We require that all systems attached to our network use anti-virus software and that they subscribe to appropriate auto-update services for critical security patches (depending on operating system). Scans are done periodically on all operating systems for which anti-virus software exists. We also remotely monitor the status of virus definitions on client machines that are attached to our domains to make sure that the update function is working.

e) *Transportation of Data.*
We normally only transport data in encrypted Zip archives on either tape or CD-ROM/DVD/Blu-Ray disk. Network file transmission is performed between secure ftp/ssh or secure socket link (SSL) http sites.

f) *Backups of Data*
We use Simpana as our enterprise backup system. The default policy keeps the last 6 versions of every file on the system. We also keep any deleted file for approximately (until backup tapes are reused) 90 days after it was deleted. In order to improve restore times, we cache the last 2 terabytes of backup on disk to speed restores of recently deleted or overwritten files. We keep a copy of all backup tapes in our online tape library to insure that all files will be readily retrievable. The servers themselves and the backup system are in a locked server

room in a secure facility. The original backup tapes are transferred on a daily basis to a large fire safe in a different building. Backups are tested quarterly to ensure the integrity of the data. An additional disaster recovery safeguard is that other units in the University Wisconsin System use Simpana to do its own backup and can provide backup personnel for WCER. Most of WCER servers are virtualized and we have a cooperative agreement in place with DOIT (UW System central technology group) to use their data as a remote recovery site for our virtual machines in the event of catastrophic loss.

g) *Ensure the Physical Security of IT Resources*
Logon to workstations is limited to named users. Logon to servers is restricted to named operators in the Technical Services unit. We have a backup generator that can provide power for all servers in the event of a power outage. The server room also has an emergency air conditioning system to ensure that servers and related support systems do not overheat in the event of a cooling failure. The server room has environmental sensors that can page appropriate personnel in the event of power and air conditioning, or water leaks. The server room is behind a series of locked doors in an alarmed space. Disposal policies ensure that all data is removed from machines and overwritten with random data before they are redeployed or disposed of.

h) *Perform Periodic Vulnerability Scanning*
WCER IT staff schedule periodic vulnerability scans of all WCER servers connected to the University campus network. The vulnerability scans include selective probes of communication services, operating systems, and applications to identify system weaknesses that could be exploited by intruders to gain access to the network. Responsibility for taking follow-up action to correct vulnerabilities, e.g., applying security patches to operating systems, is assigned to Computer Services support staff.

i) *Firewall Policy*
The School of Education has implemented a school-wide hardware firewall. Responsibility for maintaining the firewall, updated firewall policies, and periodically reviewing firewall logs is shared between the Dean's IT office and the senior administrators of WCER Technical Services. We currently do not require host-based (software) firewalls for remote machines. The network is segmented into multiple security zones with varying levels of trust and access. The server and network gear network segment has a default policy of *deny all unless specifically allowed*. We are able to create virtual networks between any given ports in the School of Education to ensure secure transmission between machines.