Exhibit 3

FOURTH AMENDMENT TO THE SOFTWARE SUPPORT AND MAINTENANCE AGREEMENT BETWEEN BROWARD COUNTY AND SSI, INC.

This Fourth Amendment ("Fourth Amendment") to the Agreement (hereinafter defined) between Broward County, a political subdivision of the State of Florida ("County"), and SSI, Inc., an Arizona corporation authorized to do business in the State of Florida ("Provider") (collectively, the "Parties"), is entered into effective as of the date this Fourth Amendment is fully executed by the Parties.

RECITALS

A. The Parties entered into the Software Support and Maintenance Agreement dated April 20, 2015, for support and maintenance of the Provider's Hosted Interactive Learning System ("ILS"), simple course builder, and third party software (as amended, the "Agreement").

B. The Parties desire to amend the Agreement to extend the renewal option in this Agreement for up to three (3) additional one (1) year terms to provide continued support and maintenance of the ILS, simple course builder, and third party software, and to add and update security related provisions to the Agreement.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. The foregoing Recitals are true and correct, and are incorporated herein by reference.

2. Unless noted otherwise, amendments made to the Agreement by this Fourth Amendment are indicated by the use of strikethroughs to indicate deletions and underlining (except for headers) to indicate additions.

3. Section 4.2 of the Agreement is amended as follows:

    4.2 Extensions. County shall have the option to renew this Agreement for up to ~~two (2)~~ five (5) additional one (1) year terms by sending notice thereof to Provider at least thirty (30) days prior to the expiration of the then-current term. The Contract Administrator is authorized to exercise each extension option. In the event that unusual or exceptional circumstances, as determined in the sole discretion of the Purchasing Director, render the exercise of an extension not practicable or if no extension is available, and expiration of this Agreement would result in a gap in the provision of services necessary for the ongoing operations of the County, then this Agreement may be extended on the same terms and conditions by the Purchasing Director for period(s) not to exceed six (6) months in the aggregate, provided that any such extension is within the authority of the Purchasing Director or otherwise authorized by the Board.

4. Section 5.1 of the Agreement is amended as follows:

5.1 For the duration of the Agreement, County will pay Provider in accordance with Exhibit B up to the following maximum amount(s):

Services/Goods	Term	Not-To-Exceed Amount
Software Support and Maintenance Services	Effective Date until Final Acceptance of the SaaS System	$25,000.00
SaaS Services, and Support and Maintenance Services	Remainder of the Initial Term (until April 19, 2018)	$45,000.00
Each optional renewal term	Each 1 year renewal term (Total ~~2~~ 5 years)	$45,000.00 (~~2~~ 5 years: ~~$90,000.00~~ $225,000.00)
Optional Services	Duration of the Agreement (inclusive of any renewals)	~~$605,000.00~~ $470,000.00
TOTAL NOT TO EXCEED		$765,000.00

****

5. Section 8.5 of the Agreement is replaced in its entirety with the following (underlining omitted):

8.5 Security and Access. If Provider will have access to any aspect of County's network via an Active Directory Account, onsite access, remote access, or otherwise, Provider must:

a. comply at all times with all applicable County access and security standards, policies, and procedures related to County's network, as well as any other or additional restrictions or standards for which County provides written notice to Provider;

b. provide any and all information that County may reasonably request in order to determine appropriate security and network access restrictions and verify Provider's compliance with County security standards;

c. provide privacy and information security training to its employees with access to County's network upon hire and at least once annually; and

d. notify County of any terminations or separations of Provider's employees who had access to County's network.

In addition, for any remote access to County's network, Provider must:

Exhibit 3

a. utilize secure, strictly-controlled industry standards for encryption (e.g., virtual private networks) and passphrases and safeguard County data that resides in or transits through Provider's internal network from unauthorized access and disclosure;

b. ensure the remote host device used for access is not connected to any other network, including an unencrypted third party public WiFi network, while connected to County's network, with the exception of networks that are under Provider's complete control or under the complete control of a person or entity authorized in advance by County in writing;

c. enforce automatic disconnect of sessions for remote access technologies after a specific period of inactivity with regard to connectivity into County infrastructure;

d. utilize equipment that contains antivirus protection software, an updated operating system, firmware, and third party-application patches, and that is configured for least privileged access;

e. utilize, at a minimum, industry standard security measures, as determined in County's sole discretion, to safeguard County data that resides in or transits through Provider's internal network from unauthorized access and disclosure; and

f. activate remote access from Provider and its subproviders into the County network only to the extent necessary to perform services under this Agreement, deactivating such access immediately after use.

If at any point in time County, in the sole discretion of its Chief Information Officer ("CIO"), determines that Provider's access to any aspect of the County's network presents an unacceptable security risk, or if Provider exceeds the scope of access required to perform the required services under the Agreement, County may immediately suspend or terminate Provider's access and, if the risk is not promptly resolved to the reasonable satisfaction of the County's CIO, may terminate this Agreement or any applicable Work Authorization upon ten (10) business days' notice (including, without limitation, without restoring any access to the County network to Provider).

6. The Agreement is amended to create Sections 8.9 and 8.10, as follows (underlining omitted):

8.9 Managed or Professional Services. Provider shall immediately notify County of any terminations or separations of Provider's employees who performed services under the Agreement and who had access to County Confidential Information or County's network. If any unauthorized party is successful in accessing any information technology component related to Provider (including but not limited to servers or fail-over servers) where County data or files exist or are housed, Provider shall notify County within twenty-four (24) hours after becoming aware of such breach, unless an extension is granted by County's CIO. Provider shall provide County with a detailed incident report

Exhibit 3

within five (5) days after becoming aware of the breach, including remedial measures instituted and any law enforcement involvement. Provider shall fully cooperate with County on incident response, forensics, and investigations into Provider's infrastructure as it relates to any County data or County applications. Provider shall not release County data or copies of County data without the advance written consent of County. If Provider will be transmitting County data, Provider agrees that it will only transmit or exchange County data via a secure method, including HTTPS, SFTP, or another method approved by County's CIO. Provider shall ensure adequate background checks have been performed on any personnel having access to County Confidential Information. To the extent permitted by such checks, Provider shall not knowingly allow convicted felons or other persons deemed by Provider to be a security risk to access County data. Provider shall ensure the use of any open source or third-party software or hardware does not undermine the security posture of the Provider or County.

8.10 System and Organization Controls (SOC) Report. Provider must provide County with a copy of a current unqualified System and Organization Controls 2 Type II Report for Provider and for any third party that provides the applicable services comprising the system, inclusive of all five trust service principles (security, availability, processing integrity, confidentiality, and privacy), on request and at least annually, unless this requirement is waived in writing by the County's CIO or designee.

7. In the event of any conflict or ambiguity between this Fourth Amendment and the Agreement, the Parties agree that this Fourth Amendment shall control.

8. Capitalized terms not otherwise defined herein shall have the meanings set forth in the Agreement.

9. The Agreement, including as amended herein, incorporates and includes all prior negotiations, correspondence, conversations, agreements, and understandings applicable to the matters contained herein, and the Parties agree that there are no commitments, agreements, or understandings concerning the subject matter hereof that are not contained in the Agreement, including as amended in this Fourth Amendment. Accordingly, the Parties agree that no deviation from the terms hereof shall be predicated upon any prior representations or agreements, whether oral or written.

10. Preparation of this Fourth Amendment has been a joint effort of the Parties, and the resulting document shall not, solely as a matter of judicial construction, be construed more severely against one of the Parties than any other.

11. Except as modified herein, all terms and conditions of the Agreement shall remain in full force and effect.

12. This Fourth Amendment may be executed in multiple originals, and may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

Exhibit 3
Page 5 of 6

IN WITNESS WHEREOF, the Parties hereto have made and executed this Fourth Amendment: BROWARD COUNTY through its BOARD OF COUNTY COMMISSIONERS, signing by and through its Mayor or Vice-Mayor, authorized to execute same by Board action on the _____ day of _______________, 2020, and SSI, Inc., signing by and through its President, duly authorized to execute same.

COUNTY

ATTEST:

____
Broward County Administrator, as
ex officio Clerk of the Broward County
Board of County Commissioners

BROWARD COUNTY, by and through
its Board of County Commissioners

By ______________________________
Mayor

________ day of ____________________, 2020

Approved as to form by
Andrew J. Meyers
Broward County Attorney
Aviation Office
2200 SW 45th Street, Suite 101
Dania Beach, Florida 33312
Telephone: (954) 359-6100
Telecopier: (954) 359-1292

By ______________________ 03/18/2020
Yesenia Alfonso (Date)
Assistant County Attorney

By ______________________ 03/18/2020
Alexander J. Williams, Jr. (Date)
Senior Assistant County Attorney

Exhibit 3
Page 6 of 6

FOURTH AMENDMENT TO THE SOFTWARE SUPPORT AND MAINTENANCE AGREEMENT BETWEEN BROWARD COUNTY AND SSI, INC.

PROVIDER

WITNESSES:

Signature

AARON WRIGHT
Print Name of Witness above

Signature

Raiza Rodriguez
Print Name of Witness above

SSI, INC.

By: Lorena de Rodriguez
Authorized Signor

Lorena de Rodriguez, President
Print Name and Title

17 day of March, 2020

ATTEST:

Corporate Secretary or other person authorized to attest

(CORPORATE SEAL OR NOTARY)