Charleston County SCHOOL DISTRICT
excellence is our standard

Charleston County School District
Request for Proposals
AMENDMENT #2
Solicitation Number: P1803
Description: Medicaid Documentation and Claims Software for Charleston County School District
Date: November 2, 2017

SUBMIT OFFER BY: November 17, 2017 BY 2:00 PM ET

QUESTIONS MUST BE RECEIVED BY: October 19, 2017 by 2:00 PM ET

NUMBER OF COPIES TO BE SUBMITTED: One (1) Original Copy, Six (6) Hard Copies and One (1) USB Flash Drive (See page 2 for details)

PROCUREMENT OFFICIAL CONTACT:

Procurement Services
Attention: Debra Cannon, CPPO, CPPB
3999 Bridge View Drive
North Charleston, SC 29405
Phone: 843-566-1982
Email: debra_cannon@charleston.k12.sc.us

The term "Offer" means your "Bid" or "Proposal".
Offers must be submitted in a sealed package. Solicitation Number & Opening Date must appear on package exterior.

You must submit a signed copy of this form with your offer. By submitting a bid or proposal, You agree to be bound by the terms of the Solicitation. You agree to hold your offer open for a minimum of ninety (90) calendar days after the Opening date.		
Print Name of Offeror (Full legal name of business submitting the offer)		Date Signed
Authorized Signature (Person signing must be authorized to submit binding offer to enter contract on behalf of Offeror named above.)		Taxpayer Identification No.
Title (Business title of person signing above)		Telephone Number
Printed Name (of person signing above)		Facsimile Number
Company Address (Street, City, State & Zip Code)		
Contact Person(if different than authorized signature)		Email Address
Telephone Number	Facsimile Number	

Cover Page

The above numbered Request for Proposals is amended as set forth below. The Hour and Date specified for receipt of proposals has not been extended.
Bid Schedule has not been amended.

Reference and acknowledge this Addendum on the offer submitted. Failure to acknowledge addendum may result in rejection of your offer.
If by virtue of this addendum you desire to change an offer already submitted, such change may be made by submitting an amended bid prior to the closing date and hour specified.

AMENDMENTS TO SOLICITATION
(a)The Solicitation may be amended at any time prior to opening. All actual and prospective Offerors should monitor the following web site for the issuance of Amendments: http://academicdepartments.musc.edu/vpfa/finance/purchasingap/vendors/solicit-awards/bids.htm (b) Offerors shall acknowledge receipt of any amendment to this solicitation (1) by signing and returning the amendment, (2) by identifying the amendment number and date in the space provided for this purpose on Page Two, (3) by letter, or (4) by submitting a bid that indicates in some way that the bidder received the amendment. (c) If this solicitation is amended, then all terms and conditions which are not modified remain unchanged.

Insert the following clauses starting on Page 12 under terms and conditions:

OFFSHORE CONTRACTING PROHIBITED. No part of the resulting contract from this solicitation may be performed offshore of the United States by persons located offshore of the United State or by means, methods, or communications that, in whole or in part, take place offshore of the United States.

INFORMATION SECURITY - DEFINITIONS

The following definitions are used in those clauses that cross reference this clause.

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. Without limitation, the term “compromise” includes copying the data through covert network channels, or copying the data to unauthorized media, or disclosure of information in violation of any obligation imposed by this contract.

Data means a subset of information in an electronic format that allows it to be retrieved or transmitted.

Government information means information (i) provided to Contractor by, or generated by Contractor for, CCSD, or (ii) acquired or accessed by Contractor
as a result of performing the Work. Without limiting the foregoing, government information includes any information that Contractor acquires or accesses by software or web-based services, which includes, without limitation, any metadata or location data. Government information excludes unrestricted information.

Information means any communication or representation of knowledge such as facts, statistics, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Public information means any specific information, regardless of form or format, that the State has actively and intentionally disclosed, disseminated, or made available to the public. Information is not public information solely because it may be subject to inspection pursuant to an unfulfilled public records request.

Software means any computer program accessed or used by CCSD or a third party pursuant to or as a result of this contract.

Third party means any person or entity other than CCSD, the Contractor, or any subcontractors at any tier.

Unrestricted information means (1) public information acquired other than through performance of the work, (2) information acquired by Contractor prior to contract formation, (3) information incidental to your contract administration, such as financial, administrative, cost or pricing, or management information, and (4) any ideas, concepts, know-how, methodologies, processes, technologies, techniques which Contractor develops or learns in connection with Contractor's performance of the work.

Web-based service means a service accessed over the Internet and acquired, accessed, or used by CCSD or a third party pursuant to or as a result of this contract, including without limitation, cloud services, software-as-a-service, and hosted computer services.

INFORMATION SECURITY - SAFEGUARDING REQUIREMENTS

(a) *Definitions*. The terms used in this clause shall have the same meaning as the terms defined in the clause titled Information Security – Definitions. In addition, as used in this clause—

Clearing means removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods.

Intrusion means an unauthorized act of bypassing the security mechanisms of a system.

Media means physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, portable hard drives, "thumb" drives, large scale integration memory chips, and printouts (but not including display media, e.g., a computer monitor, cathode ray tube (CRT) or other (transient) visual output) onto which information is recorded, stored, or printed within an information system.

Safeguarding means measures or controls that are prescribed to protect information.

Voice means all oral information regardless of transmission protocol.

(b) *Safeguarding Information*. Without limiting any other legal or contractual obligations, contractor shall implement and maintain reasonable and appropriate administrative, physical, and technical safeguards (including without limitation written policies and procedures) for protection of the security, confidentiality and integrity of the government information in its possession. In addition, contractor stall apply security controls when the contractor reasonably determines that safeguarding requirements, in addition to those identified in paragraph (c) of this clause, may be required to provide adequate security, confidentiality and integrity in a dynamic environment based on an assessed risk or vulnerability.

(c) *Safeguarding requirements and procedures*. Contractor shall apply the following basic safeguarding requirements to protect government information from unauthorized access and disclosure:

(1) Protecting information on public computers or Web sites: Do not process government information on public computers (e.g., those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control. Government information shall not be posted on Web sites that are publicly available or have access limited only by domain/Internet Protocol restriction. Such information may be posted to web pages that control access by user ID/password, user certificates, or other technical means, and that provide protection via use of security technologies. Access control may be provided by the intranet (versus the Web site itself or the application it hosts).

(2) Transmitting electronic information. Transmit email, text messages, blogs, and similar communications that contain government information using technology and processes that provide the best level of security and privacy available, given facilities, conditions, and environment.

(3) Transmitting voice and fax information. Transmit government information via voice and fax only when the sender has a reasonable assurance that access is limited to authorized recipients.

(4) Physical and electronic barriers. Protect government information by at least one physical and one electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

(5) Sanitization. At a minimum, clear information on media that have been used to process government information before external release or disposal. Overwriting is an acceptable means of clearing media in accordance with National Institute of Standards and Technology 800–88, Guidelines for Media Sanitization, at http://csrc.nist.gov/ publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf.

(6) Intrusion protection. Provide at a minimum the following protections against intrusions and compromise:

(i) Current and regularly updated malware protection services, e.g., anti-virus, antispyware.

(ii) Prompt application of security-relevant software upgrades, e.g., patches, service packs, and hot fixes.

(7) Transfer limitations. Transfer government information only to those subcontractors that both require the information for purposes of contract performance and provide at least the same level of security as specified in this clause.

(d) *Subcontracts*. Any reference in this clause to Contractor also includes any subcontractor at any tier. Contractor is responsible for, and shall impose by agreement requirements at least as secure as those imposed by this clause on, any other person or entity that contractor authorizes to take action related to government information.

(e) *Other contractual requirements regarding the safeguarding of information*. This clause addresses basic requirements and is subordinate to any other contract clauses or requirements to the extent that it specifically provides for enhanced safeguarding of information or information systems.