## Addendum #4

RFP #653177

## Intelligent Bus System RFP

Please note that the **deadline** for further questions is **5:00 pm CST, Tuesday, October 17, 2017**.

The following revisions have been made to the RFP Specifications:

1. **Technical Requirements (This section provides some technical clarifications.)**
2. **Overall**

**14)** System must be in HTML5 on the web for access, as well as, compliance to WCAG 2.0 AA, Fed 508 and W3C for accessibility and code standards.

**19)** systems is replaced with implantations. Requirement now reads; Vendor must supply three proven implementations with AVL, APC, and AVA systems fully functioning that has been working for more than four years.

## Accessibility Language:

Do you incorporate best practices for building in accessibility as defined by Apple?

https://developer.apple.com/accessibility/ios/

Do you incorporate best practices for building in accessibility as defined by Google?

https://developer.android.com/guide/topics/ui/accessibility/index.html

## Security Language:

Information Privacy and Security and Personally Identifiable Information

1.0 The Vendor shall not use any Customer Data it receives for purposes other than carrying out the Product and shall not provide any subcontractor or other third party with access to Customer Data unless it has received prior written consent from Customer or such access is specifically allowed under this Agreement.

1.1 The Vendor agrees that, beginning on the effective date of this Agreement, and continuing as long as The Vendor controls, possesses, stores, transmits or processes Customer Data, The Vendor shall employ and maintain reasonable Security to: (i) ensure that all Customer Data is protected from unauthorized use, alteration, access or disclosure, and to protect and ensure the confidentiality, integrity and availability of Customer Data; (ii) prevent unauthorized access to and unauthorized use of, and ensure the availability of, The Vendor Systems; and (iii) prevent a security breach or Malicious Code infection of Customer systems. Such Security shall, without limitation, be consistent with all Privacy Laws and Regulations, comply with PII, FERPA and as applicable FISMA security standard, and at a minimum meet all relevant industry standards. Such Security shall include, but not be limited to, the following:

(i)            The Vendor shall implement reasonable restrictions regarding physical and electronic access to Customer Data and The Vendor Systems, including but not limited to physical access controls, secure user authentication protocols, secure access control methods, firewall protection, malware protection, and use of encryption for laptops, mobile devices and Customer Data being transmitted across the public Internet or wirelessly, and as otherwise required by Privacy Laws and Regulations;

(ii)           The Vendor shall implement a reasonable and appropriate written data security program that includes technological, physical, administrative and procedural controls to protect the confidentiality, integrity and availability of Customer Data and The Vendor Systems, that encompasses access, retention and transport of Customer Data, and that provides for disciplinary action (insert penalty relative to the contract) in the event of its violation;

(iii)          The Vendor shall prevent terminated employees from accessing Customer Data and The Vendor Systems by immediately terminating their physical and electronic access to such information and systems;

(iv)         The Vendor shall employ assessment, monitoring and auditing procedures to ensure internal compliance with these safeguards;

(v)          The Vendor shall conduct a complete assessment of these safeguards at least annually and, upon written request, provide a report on the results of this assessment, including but not limited to any discrepancies, to Customer.

1.2 **Security Reporting Aid Audits**. Upon prior written notice and at a mutually acceptable time, Customer personnel or its agents may audit or inspect The Vendor's information security program and facilities to assure Customer Data is adequately protected. Customer and

The Vendor will mutually agree to the scope of such audits, which may extend to other The Vendor resources used to support The Vendor Systems and Customer Data handling by The Vendor. The Vendor will inform Customer of any internal auditing capability it possesses and permit Customer's personnel to consult on a confidential basis such internal auditors at all reasonable times. The Vendor regularly and on special request will provide reasonable reports on implementation of its information security program and its information security plan for Customer.

The Vendor shall ensure that all subcontractors whose services are part of the Product or who have access to Customer Data have a written information security program and plan substantially equivalent to the program utilized by The Vendor.

The Vendor shall review the effectiveness of its information security program at least annually and shall revise its program considering any relevant changes in technology, the sensitivity, nature and quantity of the Customer Data it holds, internal or external threats to information and The Vendor's own changing business arrangements.

The Vendor shall establish and maintain contingency plans, recovery plans and proper risk controls to ensure The Vendor's continued performance under the Agreement. The Vendor shall provide copies of the plans to Customer upon request. If Customer objects in writing to any provision of such plans and controls, The Vendor shall respond in writing within thirty (30) calendar days, explaining, among other matters that The Vendor wishes to include in its response, the actions The Vendor intends to take to cure Customer's objection.

The Vendor shall maintain for a mutually agreed-upon length of time, and afford Customer reasonable access to, all system records and logs.

Customer may review and inspect any record of system activity or Customer Data. The Vendor acknowledges and agrees that records of system activity and of Customer Data handling may be evidence (subject to appropriate chain of custody procedures) in the event of a security breach or other inappropriate activity. Upon Customer's request, The Vendor shall deliver the original copies of such records to

Customer for use in any legal, investigatory or regulatory proceeding.

During the term, Customer or its third-party designee may, but is not obligated to, perform audits of the The Vendor Systems environment, including unannounced penetration and Security tests, relating to the receipt, maintenance, use or retention of Customer Data or other Customer owned data. The Vendor agrees to comply with all reasonable recommendations that result from such inspections, tests, or audits within reasonable timeframes, but in no event more than thirty (30) calendar days.

During each calendar year, The Vendor will provide to Customer, at The Vendor's cost, its AICPAService Organization Controls (SOC) 2 Type 2 reports for data centers from which the Work is provided to Customer. The Vendor will provide Customer and its external auditors with copies of all such reports upon issuance.

1.3 **Data Backup and Recovery**. The Vendor shall establish and maintain policies and procedures relevant to contingency plans, recovery plans and proper risk controls to ensure The Vendor's continued performance under the Contract. These policies and procedures shall include, but not be limited to, recovery strategy, documented recovery plans covering all areas of operations necessary to delivering The Vendor's Product pursuant to the Contract, vital records protection and testing plans. The plans shall provide, without limitation, for off-site backup of critical data files, Customer Data, Software, Documentation, forms and supplies, as well as alternative means of transmitting and processing Customer Data.

The recovery strategy shall provide for recovery after both short and long-term disruptions in facilities, environmental support and data processing equipment. Although short term outages can be protected with redundant resources and network diversity, the long-term strategy must be capable of addressing a total destruction of The Vendor's business operations for a period of six (6) months or longer.

The Vendor's recovery objectives (time to full restoration and amount of lost data tolerated) shall not exceed that of the Customer business unit for which the Work is rendered. Customer shall provide The Vendor with a copy of the relevant Customer business unit's business impact analysis that defines these recovery objectives and shall make reasonable efforts to notify The Vendor if these objectives change. In the event of a change, Customer shall consult with The Vendor to determine the date after which The Vendor shall match the new objectives if necessary.

The Vendor shall continue to provide the Product to Customer if Customer activates its contingency plan or moves to an interim site to conduct its business, including during tests of Customer's contingency operations plans.

The Vendor shall at all times maintain sufficient backup information on its system to restore all Customer Data. All backups must be encrypted.

To ensure that the Product will be continually available, The Vendor shall maintain a complete and current copy of The Vendor Systems and Customer Data on a server located at a remote location and with a different Internet connection than the primary The Vendor Systems. The Vendor shall also provide electrical power back up systems to ensure continuous power to the Work and related The Vendor Systems for at least twenty-four (24) hours after any disruption in the primary electric power supply. In the event that the Work is interrupted, the remote server shall be immediately activated so that availability of the Work may continue uninterrupted.

All Personally Identifiable Information ("PII"), and all confidential or proprietary information identified in Customer's "Data Classification and Control Standard", which is stored, transferred or transported to or from The Vendor or The Vendor Personnel must be encrypted using a valid encryption process consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. This includes The Vendor or The Vendor Personnel laptops and removable storage devices.

1.4 **Security Breaches**. The Vendor shall maintain policies and procedures for responding to security breaches, including without limitation, assigning and training an individual to serve as security coordinator and training The Vendor's personnel with access to Customer Data to recognize security breaches and to escalate and notify the security coordinator of the foregoing. In the event of a security breach, The Vendor will use best efforts and take all necessary actions to prevent, contain, and mitigate the impact of, such security breach. The Vendor will immediately provide notice to the Customer designated point of contact on the cover sheet, to Customer's IT Security representative, and any other person designated by Customer; such notice shall, in any event, be provided within six (6) hours after the The Vendor discovered or reasonably suspected the security breach. If time is critical, corrective action shall not be delayed until the contact can be reached, provided that The Vendor shall not take any actions that result in the destruction of evidence relating to such security breach. In addition, The Vendor shall:

(a)           Immediately conduct a reasonable investigation of the reasons for and circumstances surrounding such security breach;

(b)          collect and preserve all evidence concerning the discovery, cause, vulnerability, remedial actions and impact related to such security breach, which shall meet reasonable expectations of forensic admissibility;

( c)          document the incident response and remedial actions taken in detail, which shall meet reasonable expectations of forensic admissibility;

(d)          if requested by Customer, provide notice to individuals or entities whose information was or may have been affected in a manner and format specified by Customer; and

(e)          promptly, and in no event more than two (2) business days after the date The Vendor discovered or reasonably suspected a security breach, provide a written report to Customer concerning such security breach.

1.5 **Storage and Processing of Customer Data**. All Customer Data must be stored in a physically and logically secure environment that protects it from unauthorized access, modification, theft, misuse or destruction. In addition to the standards set forth above, The Vendor shall maintain a reasonable and appropriate level of physical security controls over its facilities and The Vendor Systems including, but not limited to, appropriate alarm systems, fire suppression, and access controls (including off-hour controls), which may include visitor access procedures, security guard force, video surveillance, and staff egress searches. Further, The Vendor will maintain a reasonable and appropriate level of data security controls for its facilities and The Vendor Systems, including, but not limited to, logical access controls (including user sign-on identification and authentication), data access controls (including password protection of applications, data files and libraries), accountability tracking, anti-virus software, secured printers, restricted download to disk capability and provision for system back up.

The Vendor Systems shall be located in the United States. The Vendor and its subcontractors with access to Customer Data shall store, process and transmit Customer Data only on computers located in the United States, unless The Vendor has received Customer's prior written consent. In the event The Vendor discovers or reasonably believes that any Customer Data has been or is being stored, processed or transmitted in any other country other than the United States, The Vendor shall provide prompt notice to Customer, and in all events shall provide such notice within forty-eight (48) hours of such discovery.

The Vendor agrees that, beginning on the effective date of this Agreement, and continuing as long as The Vendor controls, possesses, stores, transmits or processes Customer Data, The Vendor shall: (a) comply with the requirements of Customer's information security program, and any documents, policies and procedures related thereto; and (b) employ and maintain the same Security reflected in Customer's information security program and any documents, policies and procedures related thereto. In order to comply with the requirements of this section, The Vendor shall periodically and regularly review Customer's information security program and the documents, policies and procedures related thereto.

In the event of any conflict between or among The Vendor's obligation to employ and maintain reasonable Security, its obligation to meet relevant industry standards for Security, its obligation to comply with the ISO 27002 security standard, and/or any obligation of The Vendor under this Information Privacy and Security section, The Vendor shall comply with the obligation that provides the most protection for the confidentiality, integrity or availability of Customer Data.

The Vendor agrees to reasonably cooperate and coordinate with Customer concerning: (a) Customer's investigation, enforcement, monitoring, document preparation, notification requirements and reporting concerning security breaches and The Vendor's and Customer's compliance with Privacy Laws and Regulations; and (b) and any other activities or duties set forth under this Agreement for which cooperation between Customer and The Vendor may be reasonably required.

2.0 **Personally Identifiable Information**. Customer shall provide The Vendor with Personally Identifiable Information ("Pll") only to the extent necessary for each party to reform their obligations hereunder. The Vendor shall implements appropriate measures to ensure the confidentiality and security of PII transmitted to The Vendor, and to protect against any unanticipated access or disclosure of information, and prevent any other action that could result in substantial harm to Customer or any individual identified by the data. In the event of a breach of any of the The Vendor’s obligations regarding Pll hereunder. The Vendor agrees to notify Customer immediately and assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless, and defend Customer and its employees from and against any and all claims, damages, or causes of action related to the breach.