



**Francis Marion University
Request for Proposal
Amendment #1**

Solicitation Number **RFP-2278**
Date Issued **05/18/2017**
Purchasing Officer **Paul MacDonald**
Phone **(843) 661-1161**
E-Mail Address **pmacdonald@fmarion.edu**
Amendment Date **06/05/2017**

DESCRIPTION: **Provide Box Office Software for Francis Marion University**

The Term "Offer" Means Your "Bid" or "Proposal".

SUBMIT OFFER BY (Opening Date/Time): **06/21/2017 at 2:00 PM EST** See "Deadline For Submission Of Offer" provision

QUESTIONS MUST BE RECEIVED BY: **06/01/2017 at 2:00 PM EST** See "Questions From Offerors" provision

NUMBER OF COPIES TO BE SUBMITTED: **One (1) original in hard copy, three (3) copies in hard copy clearly marked "COPY," one Magnetic Media as Specified and One (1) Redacted Copy as Specified.**

SUBMIT YOUR OFFER TO ONE OF THE FOLLOWING ADDRESSES IN A SEALED PACKAGE.

MAILING ADDRESS: Francis Marion University Purchasing Office P.O. Box 100547 Florence, SC 29502-0547	EXPRESS SHIPPING ADDRESS: Francis Marion University Central Receiving 4822 E. Palmetto Street Florence, SC 29506	HAND-DELIVERY: Francis Marion University Purchasing Office (Room 102) Stokes Administration Building 4822 E. Palmetto Street Florence, SC 29506
--	--	---

CONFERENCE TYPE: **N/A**
DATE & TIME: **N/A**
As appropriate, see "Conferences - Pre-Bid/Proposal" & "Site Visit" provisions

LOCATION:
**Francis Marion University
Stokes Administration Building
Board Room
4822 East Palmetto Street
Florence, SC 29506**

AWARD & AMENDMENTS An **Award** will be posted at the Physical Address stated above on or around **06/28/2017**. The award, this solicitation, and any amendments will be posted at the following web address:
<http://www.fmarion.edu/about/solicitationsandawards>

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 thirty (30) calendar days after the Opening Date.

NAME OF OFFEROR (Full legal name of business submitting the offer)	OFFEROR'S TYPE OF ENTITY: (Check one) <input type="checkbox"/> Sole Proprietorship <input type="checkbox"/> Partnership <input type="checkbox"/> Corporation (tax-exempt) <input type="checkbox"/> Corporate entity (not tax-exempt) <input type="checkbox"/> Government entity (federal, state, or local) <input type="checkbox"/> Other _____
AUTHORIZED SIGNATURE (Person signing must be authorized to submit binding offer to enter contract on behalf of Offeror named above.)	
TITLE (Business title of person signing above)	
PRINTED NAME (Printed name of person signing above) DATE SIGNED	

(See "Signing Your Offer" provision.)

Instructions regarding Offeror's name: Any award issued will be issued to, and the contract will be formed with, the entity identified as the offeror above. An offer may be submitted by only one legal entity. The entity named as the offeror must be a single and distinct legal entity. Do not use the name of a branch office or a division of a larger entity if the branch or division is not a separate legal entity, *i.e.*, a separate corporation, partnership, sole proprietorship, etc.

STATE OF INCORPORATION (If Offeror is a corporation, identify the state of Incorporation.)

TAXPAYER IDENTIFICATION NO.

(See "Taxpayer Identification Number" provision)

PAGE TWO

(Return Page Two with Your Offer)

HOME OFFICE ADDRESS (Address for offeror's home office / principal place of business)	NOTICE ADDRESS (Address to which all procurement and contract related notices should be sent.) (See "Notice" clause)	
	_____ Address	
	_____ Area Code - Number - Extension	_____ Facsimile
	_____ E-mail Address	

PAYMENT ADDRESS (Address to which payments will be sent.) (See "Payment" clause)	ORDER ADDRESS (Address to which purchase orders will be sent) (See "Purchase Orders and "Contract Documents" clauses)
_____ Payment Address same as Home Office Address	_____ Order Address same as Home Office Address
_____ Payment Address same as Notice Address (check only one)	_____ Order Address same as Notice Address (check only one)

ACKNOWLEDGMENT OF AMENDMENTS							
Offerors acknowledges receipt of amendments by indicating amendment number and its date of issue. (See "Amendments to Solicitation" Provision)							
Amendment No.	Amendment Issue Date	Amendment No.	Amendment Issue Date	Amendment No.	Amendment Issue Date	Amendment No.	Amendment Issue Date

DISCOUNT FOR PROMPT PAYMENT (See "Discount for Prompt Payment" clause)	10 Calendar Days (%)	20 Calendar Days (%)	30 Calendar Days (%)	_____ Calendar Days (%)
---	----------------------	----------------------	----------------------	-------------------------

NOTE: A remote demonstration for each responsible and responsive Offeror (as determined by evaluating the Offeror's proposal) will be scheduled for 06/26/17 between 10:00am and 3:30pm EST and on 06/27/17 at times between 9:00am and 2:30pm EST daily. Each Offeror will be required to provide their remote demonstration on June 26 or June 27. No other dates will be available for remote demonstrations.

Amendment #1
RFP-2278 Provide Box Office Software Service

AMENDMENTS TO SOLICITATION

- (a) The Solicitation may be amended at any time prior to opening.
- (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.

Modifications

- 1. The following clause **replaces** the clause found on page 34 **INDEMNIFICATION -- THIRD PARTY CLAIMS (NOV 2011)**

INDEMNIFICATION -THIRD PARTY CLAIMS – DISCLOSURE OF INFORMATION (FEB 2015)

- (a) Without limitation, Contractor shall defend and hold harmless Indemnitees from and against any and all suits, claims, investigations, or fines (hereinafter “action”) of any character (and all related damages, settlement payments, attorneys' fees, costs, expenses, losses or liabilities) by a third party which arise out of or in connection with a disclosure of government information (as defined in the clause titled Information Security -Definitions) caused in whole or in part by any act or omission of contractor, its subcontractors at any tier, their employees, workmen, servants, agents, or anyone directly or indirectly employed by them or anyone for whose acts any of them may be liable, regardless of whether or not caused in part by an Indemnitee, and whether or not such action is brought by a third party or an Indemnitee, but only if the act or omission constituted a failure to perform some obligation imposed by the contract or the law.
- (b) Indemnitee must notify contractor in writing within a reasonable period of time after Indemnitee first receives written notice of any action. Indemnitee's failure to provide or delay in providing such notice will relieve contractor of its obligations under this clause only if and to the extent that such delay or failure materially prejudices contractor's ability to defend such action. Indemnitee must reasonably cooperate with contractor's defense of such actions (such cooperation does not require and is without waiver of an Indemnitee's attorney/client, work product, or other privilege) and, subject to Title 1, Chapter 7 of the South Carolina Code of Laws, allow contractor sole control of the defense, so long as the defense is diligently and capably prosecuted. Indemnitee may participate in contractor's defense of any action at its own expense. Contractor may not, without Indemnitee's prior written consent, settle, compromise, or consent to the entry of any judgment in any such commenced or threatened action unless such settlement, compromise or consent (i) includes an unconditional release of Indemnitee from all liability related to such commenced or threatened action, and (ii) is solely monetary in nature and does not include a statement as to, or an admission of fault, culpability or failure to act by or on behalf of, an Indemnitee or otherwise adversely affect an Indemnitee. Indemnitee's consent is necessary for any settlement that requires Indemnitee to part with any right or make any payment or subjects Indemnitee to any injunction.
- (c) Notwithstanding any other provision, contractor's obligations pursuant to this clause are without any limitation whatsoever. Contractor's obligations under this clause shall survive the termination, cancellation, rejection, or expiration of the contract. This provision shall be construed fairly and reasonably, neither strongly for nor against either party, and without regard to any clause regarding insurance.
- (d) "Indemnitee" means the State of South Carolina, its instrumentalities, agencies, departments, boards, political subdivisions and all their respective officers, agents and employees.

- 2. The following clauses are to be added to the document:

INDEMNIFICATION -INTELLECTUAL PROPERTY (JAN 2006)

- (a) Without limitation and notwithstanding any provision in this agreement, Contractor shall, upon receipt of notification, defend and indemnify the State, its instrumentalities, agencies, departments, boards, political subdivisions and all their respective officers, agents and employees against all actions, proceedings or claims of any nature (and all damages, settlement payments, attorneys' fees (including inside counsel), costs, expenses, losses or liabilities attributable thereto) by any third party asserting or involving an IP right related to an acquired item. State shall allow Contractor to defend such claim so long as the defense is diligently and capably prosecuted. State shall allow Contractor to settle such claim so long as (i) all settlement payments are made by Contractor, and (ii) the settlement imposes no non-monetary obligation upon State. State shall reasonably cooperate with Contractor's defense of such claim.(b)In the event an injunction or order shall be obtained against State's use of any acquired item, or if in Contractor's opinion, the acquired item is likely to become the subject of a claim of infringement or violation of an IP right, Contractor shall, without in any

way limiting the foregoing, and at its expense, either:

(1) procure for State the right to continue to use, or have used, the acquired item, or (2) replace or modify the acquired item so that it becomes non-infringing but only if the modification or replacement does not adversely affect the specifications for the acquired item or its use by State. If neither (1) nor (2), above, is practical, State may require that Contractor remove the acquired item from State, refund to State any charges paid by State therefor, and take all steps necessary to have State released from any further liability. (c) Contractor's obligations under this paragraph do not apply to a claim to the extent (i) that the claim is caused by Contractor's compliance with specifications furnished by the State unless Contractor knew its compliance with the State's specifications would infringe an IP right, or (ii) that the claim is caused by Contractor's compliance with specifications furnished by the State if the State knowingly relied on a third party's IP right to develop the specifications provided to Contractor and failed to identify such product to Contractor. (d) As used in this paragraph, these terms are defined as follows: "IP right(s)" means a patent, copyright, trademark, trade secret, or any other proprietary right. "Acquired item(s)" means the rights, goods, or services furnished under this agreement. "Specification(s)" means a detailed, exact statement of particulars such as a statement prescribing materials, dimensions, and quality of work. (e) Contractor's obligations under this clause shall survive the termination, cancellation, rejection, or expiration of this Agreement.

INFORMATION SECURITY -DEFINITIONS (FEB 2015)

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, the using governmental unit, 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 the Using Governmental Unit or a third party pursuant to or as a result of this contract.

Third party means any person or entity other than the Using Governmental Unit, 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 the using governmental unit 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 USE AND DISCLOSURE (FEB 2015)

Except to the extent necessary for performance of the work, citizens should not be required to share information with those engaged by the government in order to access services provided by the government and such information should be used by those engaged by the government only to the extent necessary to perform the work acquired; accordingly, this clause addresses basic requirements for the Contractor's use and disclosure of government information, which expressly includes, but is not limited to, information provided by or obtained from the citizens. Anonymizing information does not resolve the foregoing concern. This clause should be broadly interpreted to effectuate this intent. Every obligation in this clause is material. Absent express reference to this clause, this clause supersedes any other clause to the extent of any inconsistency unless and to the extent the other clause provides greater protection for government information.

(a) Definitions. The terms used in this clause shall have the same meaning as the terms defined in the clause titled Information

Security – Definitions.

(b) Legal mandates. Contractor shall be permitted to use, disclose, or retain government information to the limited extent necessary to comply with any requirement imposed on Contractor by law. If it is necessary for Contractor to use, disclose, or retain government information in order to comply with a law, Contractor shall provide using governmental unit with written notice, including a description of the circumstances and applicable law, in advance of such use, disclosure or retention except to the extent expressly prohibited by law.

(c) Flow down. Any reference in this clause to Contractor also includes any subcontractor at any tier. Contractor is responsible for, and shall impose by agreement the requirements of this clause on, any other person or entity that contractor authorizes to take action related to government information.

(d) Collecting Information. Contractor must gather and maintain government information only to the minimum extent necessary to accomplish the work.

(e) Rights, Disclosure and Use. Except as otherwise expressly provided in this solicitation, Contractor agrees NOT to either (1) use or disclose government information, or (2) retain government information after termination or expiration of this contract. Contractor acquires no rights in any government information except the limited rights to use, disclose and retain the government information in accordance with the terms of this solicitation. To the extent reasonably necessary to perform the work, Contractor may: (i) use (including access, process, transmit, and store) and maintain the government information itself; and (ii) disclose government information to persons having a need-to-know (e.g., subcontractors). Before disclosing government information to a subcontractor or third party, Contractor shall give the using governmental unit detailed written notice of both the reason for disclosure and the identity and location of the recipient. The notice shall be provided no later than fifteen (15) business days in advance of the disclosure.

(f) Return. Notwithstanding the using governmental unit's failure to perform or the pendency of a dispute, Contractor agrees to promptly deliver to the using governmental unit (or destroy, at the using governmental unit's option) all government information in its possession as and upon written request of using governmental unit (provided that, if the contract has not expired or been terminated, Contractor shall be excused from the performance of any work reasonably dependent on Contractor's further access to such government information).

(g) Privacy Policy & Applicable Laws. Without limiting any other legal or contractual obligations imposed by this contract or the law, Contractor shall (a) comply with its own privacy policies and written privacy statements relevant to the work, and

(b) comply with (1) all laws applicable to Contractor regarding government information, and (2) all laws and standards identified in the clause, if included, entitled Information Use and Disclosure – Standards.

(h) Actions Following Disclosure. Immediately upon discovery of a compromise or improper use of government information, Contractor shall take such action as may be necessary to preserve forensic evidence and eliminate the cause of the compromise or improper use. As soon as practicable, but no later than twenty-four hours after discovery, Contractor shall notify using governmental unit of the compromise or improper use, including a description of the circumstances of the use or compromise. As soon as practicable after discovery, Contractor shall undertake a thorough forensic investigation of any compromise or improper use and provide the using governmental unit all information necessary to enable the using governmental unit to fully understand the nature and extent of the compromise or improper use. With regard to any compromise or improper use of government information, Contractor shall: (1) provide any notification to third parties legally required to be provided such notice by Contractor, and if not (e.g., if legally required of the using governmental unit), Contractor shall reimburse using governmental unit for the cost of providing such notifications; (2) pay all costs and expenses for at least two years of identity theft monitoring services (including without limitation, credit monitoring) and identity theft restoration services for any such affected individuals receiving notice where such services are appropriate given the circumstances of the incident and the nature of the information compromised; (3) undertake any other measures that are customary and reasonable for an entity to take when experiencing a similar disclosure, (4) pay any related fines or penalties imposed on the using governmental unit, and (5) reimburse the Using Governmental Unit all costs reasonably incurred for communications and public relations services involved in responding to the compromise or improper use. Notwithstanding any other provision, contractor's obligations pursuant to this item (h) are without limitation.

(i) Survival & Remedy. All the obligations imposed by this paragraph are material. The obligations of this section shall survive termination or expiration of the contract. Without limiting any rights the using governmental unit may have, and notwithstanding any other term of this contract, Contractor agrees that using governmental unit may have no adequate remedy at law for a breach of Contractor's obligations under this clause and therefore the using governmental unit shall be entitled to pursue equitable remedies in the event of a breach of this clause.

INFORMATION USE AND DISCLOSURE – STANDARDS (FEB 2015)

To the extent applicable:

(a) Breach of security of state agency data; notification; rights and remedies of injured parties; penalties; notification of Consumer Protection Division, S.C. Code Ann. Section 1-11-490.

(b) South Carolina Financial Identity Fraud and Identity Theft Protection Act (FIFITPA), 2008 Act 190, as amended. Solely for purposes of Section 39-1-90 of the South Carolina Code of Laws, as amended, Contractor is deemed to be the owner of government information, as defined herein, and Contractor agrees that the Using Governmental Unit is not a licensee.

(c) The South Carolina Family Privacy Protection Act of 2002, S.C. Code Ann. Sections 30-2-10, et seq.

(d) Personal Identifying Information Privacy Protection, S.C. Code Ann. Sections 30-2-310 et seq.

(e) Data Breach Notification, 2014 Act No. 286, Section 117.117, as revised in any future annual appropriations act.

INFORMATION SECURITY -SAFEGUARDING REQUIREMENTS (FEB 2015)

(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, 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 shall 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/80088/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, antispayware.

(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.

INFORMATION SECURITY – LOCATION OF DATA (FEB 2015)

Notwithstanding any other provisions, contractor is prohibited from processing, storing, transmitting, or accessing government information, as defined in the clause titled Information Security –Definitions, outside the continental United States. For clarity, this obligation is a material requirement of this contract and applies to subcontractors at any tier.

LICENSES AND PERMITS (JAN 2006)

During the term of the contract, the Contractor shall be responsible for obtaining, and maintaining in good standing, all licenses (including professional licenses, if any), permits, inspections and related fees for each or any such licenses, permits and /or inspections required by the State, county, city or other government entity or unit to accomplish the work specified in this solicitation and the contract.

PRICING DATA --AUDIT --INSPECTION (JAN 2006)

[Clause Included Pursuant to Section 11-35-1830, -2210, & -2220] (a) Cost or Pricing Data. Upon Procurement Officer's request, you shall submit cost or pricing data, as defined by 48 C.F.R. Section 2.101 (2004), prior to either (1) any award to contractor pursuant to 11-35-1530 or 11-35-1560, if the total contract price exceeds \$500,000, or (2) execution of a change order or contract modification with contractor which exceeds \$100,000. Your price, including profit or fee, shall be adjusted to exclude any significant sums by which the state finds that such price was increased because you furnished cost or pricing data that was inaccurate, incomplete, or not current as of the date agreed upon between parties. (b) Records Retention. You shall maintain your records for three years from the date of final payment, or longer if requested by the chief Procurement Officer. The state may audit your records at reasonable times and places. As used in this subparagraph (b), the term "records" means any books or records that relate to cost or pricing data submitted pursuant to this clause. In addition to the obligation stated in this subparagraph (b), you shall retain all records and allow any audits provided for by 11-35-2220(2). (c) Inspection. At reasonable times, the state may inspect any part of your place of business which is related to performance of the work. (d) Instructions Certification. When you submit data pursuant to subparagraph (a), you shall (1) do so in accordance with the instructions appearing in Table 15-2 of 48 C.F.R. Section 15.408 (2004) (adapted as necessary for the state context), and (2) submit a Certificate of Current Cost or Pricing Data, as prescribed by 48 CFR Section 15.406-2(a) (adapted as necessary for the state context). (e) Subcontracts. You shall include the above text of this clause in all of your subcontracts. (f) Nothing in this clause limits any other rights of the state.

RESTRICTIONS ON PRESENTING TERMS OF USE OR OFFERING ADDITIONAL SERVICES (FEB 2015)

(a) Citizens, as well as public employees (acting in their individual capacity), should not be unnecessarily required to agree to or provide consent to policies or contractual terms in order to access services acquired by the government pursuant to this contract (hereinafter "applicable services") or, in the case of public employees, to perform their job duties; accordingly, in performing the work, contractor shall not require or invite any citizen or public employee to agree to or provide consent to any end user contract, privacy policy, or other terms of use (hereinafter "terms of use") not previously approved in writing by the procurement officer. Contractor agrees that any terms of use regarding applicable services are void and of no effect.

(b) Unless expressly provided in the solicitation, public contracts are not intended to provide contractors an opportunity to market additional products and services; accordingly, in performing the work, contractor shall not – for itself or on behalf of any third party – offer citizens or public employees (other than the procurement officer) any additional products or services not required by the contract.

(c) Any reference to contractor in items (a) or (b) also includes any subcontractor at any tier. Contractor is responsible for compliance with these obligations by any person or entity that contractor authorizes to take any action related to the work.

(d) Any violation of this clause is a material breach of contract. The parties acknowledge the difficulties inherent in determining the damage from any breach of these restrictions. Contractor shall pay the state liquidated damages of \$1,000 for each contact with a citizen or end user that violates this restriction.

SERVICE PROVIDER SECURITY REPRESENTATION (FEB 2015)

The following obligations are subordinate to any other contract clause to the extent the other clause specifically provides for enhanced safeguarding of government information, applicable information systems, or applicable organizations. Offeror (i) warrants that the work will be performed, and any applicable information system (as defined in the clause titled "Information Security -Definitions") will be established and maintained in substantial conformity with the information provided in Offeror's Response to SPSAQ; (ii) agrees to provide the Using Governmental Unit with prompt notice of any material variation in operations from that reflected in the Response to SPSAQ; and (iii) agrees to comply with all other obligations involving either information security or information use and disclosure imposed by the contract, notwithstanding any inconsistent statement in Offeror's Response to SPSAQ. To the extent Offeror's Response to SPSAQ does not conform to any other contractual requirements, the Using Agency's lack of objection does not constitute a waiver.

Questions

Vendor Questions and Answers

Question 1	How many different venue map layouts will be required (across all "reserved seat" venues)?
Answer	At present, a minimum of 3 for reserved seating and 2 (one for each theatre) for general admission events. Mainstage (849) seating with pit seats, Mainstage (849) seating without pit seats, Black Box (100 seats).
Question 2	How many seats are there in the LARGEST reserved seating venue?

Answer	At present, 849.
Question 3	How many seats are there in the SMALLEST reserved seating venue?
Answer	At present, 100.
Question 4	How many customer records are there in your ticketing system in total?
Answer	7,231 as of 6/1/17
Question 5	How many subscription packages are sold? How many different events do those packages consist of?
Answer	We offer subscription packages for our companies in residence. For 2016/2017 there were 204 subscription packages sold. This is for the season containing 5 to 6 shows.
Question 6	If applicable, please describe the benefits your subscribers get.
Answer	Subscribers get to reserve / renew their seats prior to the general public on sale dates, if bought as a subscription they get a per ticket discount, and special receptions for specified concerts.
Question 7	Average single ticket price?
Answer	Pricing is set up in 3 tiers with 4 discounts per tier. Average single ticket price at present is \$30.00
Question 8	Average subscription package price?
Answer	Subscriptions are set up in 3 tiers with 4 discounts per tier. Average subscription package price at present is \$110.00
Question 9	Do you have a membership program? If so, how many members do you have and what benefits do members receive?
Answer	We have a membership program with 21 members at present for the 2016-2017 season. This number varies from year to year. The members get a set number of complimentary tickets depending on their membership level, possible meet & greet opportunities, and advanced notice for buying tickets on selected shows.
Question 10	How many unique staff members will need access to the system?
Answer	At minimum 5 in any given year, but staff members will vary from year to year as bolunteers and student workers change over time in the department.
Question 11	Is there a need for the box office system to connect/integrate the University's fundraising/development system?
Answer	No
Question 12	How many email subscribers do you have in your email list?
Answer	At present, approximately 1,100.
Question 13	How many times per year are email campaigns sent to the entire list?
Answer	Approximately once per month.
Question 14	Please define: "Real time, online web ticketing for flex subscription/package sales"
Answer	Since we offer both flex and subscription packages frequently at the same times for different organizations or shows, the software therefore must be able to handle both types of packages and be set up to prevent double booking of seats.
Question 15	Please define: "Able to limit user privileges by event/organization"
Answer	We would like to be able to establish a "member" within the system, set their level and have the software manage their comp tickets as well as their bought tickets within the same sale. For instance, one of our resident companies has their own "memberships". With their members, each member presently can receive a set number of complimentary tickets depending on their membership level.
Question 16	Please define: "Email system has ability to use pre-designed templates, as well as customer generated templates"
Answer	We would like to have the capability to send out email blasts about upcoming shows that would be both easy to set up and that could be used again in future. Also, we seek the capability to email specific show information that would only be relevant to customers that bought tickets to a specific show.
Question 17	Please provide serial numbers for your Boca Lemur S Thermal ticket printers to confirm compatibility with our system.
Answer	Boca #1: 326506 ; Boca #2: 324881

Question 18	Our system has partnered with “X” company and “Y” company to provide PCI-DSS1 validated P2P Encryption for credit card transactions. Our clients are required to sign up with this partner for merchant service transactions and to receive credit card readers. Is FMU open and willing to changing credit card processors for this technology transition?
Answer	FMU is open to changing credit card processors for this transition, but only for use at the Performing Arts Center. The University will not be bound university wide to the use of a new credit card processor. Offeror must indicate in its proposal any expense associated with a change to the credit card processor. Offeror must also indicate in its proposal all per-use fees for all credit card transactions.
Question 19	Please explain: Can set true BOGO promotional offers that will force customers into the parameters of the BOGO
Answer	Any promotions that would involve “Buy one, get one free” or “discount for groups of 8 or more” are capable of being controlled by the ticketing software and not by a separate “honor program” in which we have to run reports to double check that patrons are not abusing the promotion.
Question 20	Please explain: Ability to tag accounts individually, or by including them in groups
Answer	We would like a system that can identify a member of a membership program at the time of purchase and guide them through their membership options that would be preset each season. At present we have two membership programs running the length of the season. The University desires the option for these membership programs to be separate from one another, even if the membership benefits for each of the programs are identical.
Question 21	Please explain: Lasso/Multi-seat selection tool
Answer	For group sales we would like to have short cuts in selecting large groups of seats without having to click on each seat individually.
Question 22	Please explain: Describe your secured method of data transport.
Answer	As part of your proposal, the University desires to know the Offeror’s specific methods for securing data at rest or in storage, in use, or when used or accessed, and in motion or during transmission.
Question 23	What ticketing platform are you using today?
Answer	Choice Ticketing (Classic System)
Question 24	Please explain your goals for this question? What are you hoping to share back and forth with the ticketing system. Can your system integrate with our Higher Education ERP system – Ellucian Colleague?
Answer	As part of your proposal, the University desires to know the Offeror’s specific proposed capability of integration to our Higher Education Enterprise Requirements Programming system. Detail any and all capability of integration with our ERP system.
Question 25	What are the fees currently charged by your ticketing provider and / or you to purchasers of tickets online, via telephone, and at the box office?
Answer	Our current provider charges a \$2.50 per ticket fee for tickets bought online; the current provider does not charge a fee for purchases made by telephone or at the box office.

Vendor: _____

Authorized Signature: _____
 (Same signature as individual who signed cover page of the solicitation)

Date: _____