



RFP No. 720-1904 Event Management Software

Status: Posted

Solicitation ID: 720-1904

Response Due Date: 10/30/2018

Response Due Time: 2:30 PM

Agency Number: 720

Days Solicited: 21+ Days for Solicitation Notice

Solicitation Posting Date: 10/5/2018

Last Modified: 10/5/2018 1:03 pm

Solicitation Description: Event Management Software

Class/Item Code: 92014-*Applications Software (For Minicomputer Systems)

Attachments

#	Name	Description
1	ESBD_File_145330_RFP 720-1904 Event Management Software.docx	RFP document
2	ESBD_File_145330_RFP 720-1904 APPENDIX TWO. Event Management Software.docx	APPENDIX TWO - Sample agreement



Texas Comptroller of Public Accounts
Glenn Hegar

- Home (<http://comptroller.texas.gov/>)
- Contact Us (<http://comptroller.texas.gov/about/contact/>)

POLICIES

- Privacy and Security Policy (<https://comptroller.texas.gov/about/policies/privacy.php>)
- Accessibility Policy (<https://comptroller.texas.gov/about/policies/accessibility.php>)
- Link Policy (<https://comptroller.texas.gov/about/policies/links.php>)
- Texas.gov (<http://texas.gov>)
- Search from the Texas State Library (<https://www.tsl.texas.gov/trail/index.html>)
- Texas Homeland Security (<http://www.dhs.gov/geography/texas>)
- Texas Veterans Portal (<https://veterans.portal.texas.gov/>)
- Public Information Act (<https://comptroller.texas.gov/about/policies/public-information-act.php>)
- Texas Secretary of State (<http://www.sos.state.tx.us/>)
- HB855 Browser Statement

OTHER STATE SITES

- [texas.gov](https://www.texas.gov/) (https://www.texas.gov/)
- Texas Records and Information Locator (TRAIL) (<http://www.tsl.state.tx.us/trail/>)
- State Link Policy
(<http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/State%20Website%20Linking%20and%20Privacy%20Policy.pdf>)
- Texas Veterans Portal (<http://veterans.portal.texas.gov>)



REQUEST FOR PROPOSAL

RFP No. 720-1904 Event Management Software

Proposal Submittal Deadline: Tuesday, October 30th, 2018 at 2:30 PM CST

The University of Texas System
Multiple Departments

Prepared By:
Darya Vienne
The University of Texas System
210 West 7th Street
Austin, Texas 78701-2982
dvienne@utsystem.edu
October 5th, 2018

REQUEST FOR PROPOSAL

TABLE OF CONTENTS

SECTION 1: INTRODUCTION 1

SECTION 2: NOTICE TO PROPOSER..... 3

SECTION 3: SUBMISSION OF PROPOSAL..... 7

SECTION 4: GENERAL TERMS AND CONDITIONS 9

SECTION 5: SPECIFICATIONS AND ADDITIONAL QUESTIONS 10

SECTION 6: PRICING AND DELIVERY SCHEDULE 16

Attachments:

- APPENDIX ONE: PROPOSAL REQUIREMENTS
- APPENDIX TWO: SAMPLE AGREEMENT
- APPENDIX THREE: ACCESS BY INDIVIDUALS WITH DISABILITIES
- APPENDIX FOUR: HIGHER EDUCATION VENDOR ASSESSMENT TOOL (HECVAT)

SECTION 1

INTRODUCTION

1.1 Description of The University of Texas System

For more than 130 years, The University of Texas System has been committed to improving the lives of Texans and people all over the world through education, research and health care.

The University of Texas System is one of the nation's largest systems of higher education, with [14 institutions](#) that educate more than 230,000 students. Each year, UT institutions award more than one-third of all undergraduate degrees in Texas and almost two-thirds of all health professional degrees. With about 20,000 faculty – including Nobel laureates – and more than 80,000 health care professionals, researchers, student advisors and support staff, the UT System is one of the largest employers in the state.

Life-changing research and invention of new technologies at UT institutions places the UT System among the [top 10 “World’s Most Innovative Universities,”](#) according to Reuters. The UT System [ranks eighth in the nation in patent applications](#), and because of the high caliber of scientific research conducted at UT institutions, the UT System is ranked No. 1 in Texas and No. 3 in the nation in federal research expenditures.

In addition, the UT System is home to three of the nation's National Cancer Institute Cancer Centers – UT MD Anderson, UT Southwestern and UT Health Science Center-San Antonio – which must meet rigorous criteria for world-class programs in cancer research. And the UT System is the only System in the country to have four Clinical and Translational Science Awards (CTSA) from the National Institutes of Health.

Transformational initiatives implemented over the past several years have cemented UT as a national leader in higher education, including the expansion of educational opportunities in South Texas with the opening of The University of Texas Rio Grande Valley in 2015. And UT was the only system of higher education in the nation that established not one, but two new medical schools in 2016 at The University of Texas at Austin and UT Rio Grande Valley.

University of Texas institutions are setting the standard for excellence in higher education and will continue to do so thanks to our generous donors and the leadership of the [Chancellor](#), [Board of Regents](#) and [UT presidents](#).

1.2 Background and Special Circumstances

The purpose of this Request for Proposal (RFP) is to identify the vendor to provide an online Events Management Software (EMS). The EMS would allow for the creation and support of online events, receipting, and reporting for these events. This system would serve UT System events, such as conference and training planning. At present, there is no intent to offer this service to any of the 14 UT System campuses.

This RFP does not include merchant and banking services. Each Proposer should be able to support one or more merchant processing companies using industry standard payment processing gateways. If Proposer requires the use of a proprietary / specific payment gateway or merchant processor, please clearly indicate.

Note: Please exclude any industry standard merchant processing and interchange fees, card / network acceptance fees and banking fees ("Merchant and Banking Fees") from Proposer's pricing / fee schedule. If Merchant and Banking Fees cannot be excluded from the pricing, please clearly identify all pricing that may have embedded Merchant and Banking Fees.

1.3 Objective of Request for Proposal

The University of Texas System is soliciting proposals in response to this Request for Proposal No.720-1904 (this "RFP"), from qualified vendors to provide Event Management Software (the "**Software**") more specifically described in **Section 5** of this RFP.

1.4 Group Purchase Authority

Texas law authorizes institutions of higher education (defined by [§61.003, Education Code](#)) to use the group purchasing procurement method (ref. §§[51.9335](#), [73.115](#), and [74.008](#), *Education Code*). Additional Texas institutions of higher education may therefore elect to enter into a contract with the successful Proposer under this RFP. In particular, Proposer should note that University is part of The University of Texas System (**UT System**), which is comprised of fourteen institutions described at <http://www.utsystem.edu/institutions>. UT System institutions routinely evaluate whether a contract resulting from a procurement conducted by one of the institutions might be suitable for use by another, and if so, this RFP could give rise to additional purchase volumes. As a result, in submitting its proposal, Proposer should consider proposing a pricing model and other commercial terms that take into account the higher volumes and other expanded opportunities that could result from the eventual inclusion of other institutions in the purchase contemplated by this RFP. Any purchases made by other institutions based on this RFP will be the sole responsibility of those institutions.

SECTION 2

NOTICE TO PROPOSER

2.1 Submittal Deadline

University will accept proposals submitted in response to this RFP until 2:30 p.m., Central Standard Time (“**CST**”) on Tuesday, October 30th, 2018 (the “**Submittal Deadline**”).

2.2 University Contact Person

Proposers will direct all questions or concerns regarding this RFP to the following University contact (“**University Contact**”):

Darya Vienne
Email: dvienne@utsystem.edu

University specifically instructs all interested parties to restrict all contact and questions regarding this RFP to written communications delivered to (i) University Contact, or (ii) if questions relate to Historically Underutilized Businesses, to HUB Coordinator (ref. **Section 2.5** of this RFP). *University Contact must receive all questions or concerns no later than 2:30 p.m. CST on Tuesday, October 16th, 2018.* University will have a reasonable amount of time to respond to questions or concerns. It is University’s intent to respond to all appropriate questions and concerns; however, University reserves the right to decline to respond to any question or concern.

2.3 Criteria for Selection

The successful Proposer, if any, selected by University through this RFP will be the Proposer that submits a proposal on or before the Submittal Deadline that is the most advantageous to University. The successful Proposer is referred to as “**Contractor**.”

Proposer is encouraged to propose terms and conditions offering the maximum benefit to University in terms of (1) service, (2) total overall cost, and (3) project management expertise.

The evaluation of proposals and the selection of Contractor will be based on the information provided in the proposal. University may consider additional information if University determines the information is relevant.

Criteria to be considered by University in evaluating proposals and selecting Contractor, will be these factors:

2.3.1 Threshold Criteria Not Scored

- A. Ability of University to comply with laws regarding Historically Underutilized Businesses; and
- B. Ability of University to comply with laws regarding purchases from persons with disabilities.

2.3.2 Scored Criteria

- A. Cost (30%);
- B. Types of Services Offered by Proposer (20%);
- C. Vendor Experience (10%);
- D. Platform Technology, Security and Functionality (20%);
- E. Account Management (20%).

2.4 Key Events Schedule

Issuance of RFP	Friday, October 5 th , 2018
Pre-Proposal Conference Call (ref. Section 2.6 of this RFP)	3 p.m. CST on Monday, October 15 th , 2018
Deadline for Questions / Concerns (ref. Section 2.2 of this RFP)	2:30 p.m. CST on Tuesday, October 16 th , 2018
Submittal Deadline (ref. Section 2.1 of this RFP)	2:30 p.m. CST on Tuesday, October 30 th , 2018

2.5 Historically Underutilized Businesses

- 2.5.1 All agencies of the State of Texas are required to make a good faith effort to assist historically underutilized businesses (each a “**HUB**”) in receiving contract awards. The goal of the HUB program is to promote full and equal business opportunity for all businesses in contracting with state agencies. Pursuant to the HUB program, if under the terms of any agreement or contractual arrangement resulting from this RFP, Contractor subcontracts any of the Services, then Contractor must make a good faith effort to utilize HUBs certified by the Procurement and Support Services Division of the Texas Comptroller of Public Accounts. Proposals that fail to comply with the requirements contained in this **Section 2.5** will constitute a material failure to comply with advertised specifications and will be rejected by University as non-responsive. Additionally, compliance with good faith effort guidelines is a condition precedent to awarding any agreement or contractual arrangement resulting from this RFP. Proposer acknowledges that, if selected by University, its obligation to make a good faith effort to utilize HUBs when subcontracting any of the Services will continue throughout the term of all agreements and contractual arrangements resulting from this RFP. Furthermore, any subcontracting of the Services by Proposer is subject to review by University to ensure compliance with the HUB program.
- 2.5.2 University has reviewed this RFP in accordance with [Title 34, Texas Administrative Code, Section 20.285](#), and has determined that subcontracting opportunities (HUB **and / or** Non-HUB) are probable under this RFP. The HUB participation goal for this RFP is **26%**.
- 2.5.3 A HUB Subcontracting Plan (“**HSP**”) is required as part of, *but submitted separately from*, Proposer’s proposal. The HSP will be developed and administered in accordance with University’s Policy on Utilization of Historically Underutilized Businesses and incorporated for all purposes.

*Each Proposer, **whether self-performing or planning to subcontract**, must complete and return the HSP in accordance with the terms and conditions of this RFP. Proposers that fail to do so will be considered non-responsive to this RFP in accordance with [§2161.252, Government Code](#).*

Questions regarding the HSP may be directed to:

Contact: Kyle Hayes
HUB Coordinator
Phone: 512-322-3745
Email: khayes@utsystem.edu

Contractor will not be permitted to change its HSP after the deadline submittal date unless: (1) Contractor completes a new HSP, setting forth all modifications requested by Contractor, (2) Contractor provides the modified HSP to University, (3) University HUB Program Office approves the modified HSP in writing, and (4) all agreements resulting from this RFP are amended in writing to conform to the modified HSP.

- 2.5.4 Proposer must submit, **via email**, one (1) HSP in PDF format to University no later than Tuesday, October 30th, 2018 at 2:30 p.m. CST (ref. **Section 3.2** of this RFP) to the email address below:

HSP Submittal Email: utadminHSP@utsystem.edu

Proposer must include the following information in the email submission:

Subject Line: *RFP 720-1904, Event Management Software, Tuesday, October 30th, HUB Subcontracting Plan*

Body: Proposer company name and the name and contact information of the person who prepared the HSP.

Instructions on completing an HSP

Proposer must visit <https://www.utsystem.edu/offices/historically-underutilized-business/hub-forms> to download the most appropriate HUB Subcontracting Plan (HSP) / Exhibit H form for use with this Request for Proposal. Proposer will find, on the HUB Forms webpage, a link to “[Guide to Selecting the Appropriate HSP Option](#)”. **Please click on this link and read the Guide first before selecting an HSP Option.** Proposer shall select, from the four (4) Options available, the Option that is most applicable to Proposer’s subcontracting intentions. These forms are in **fillable** PDF format and must be downloaded and opened with *Adobe Acrobat/ Reader* to utilize the fillable function. If Proposer has any questions regarding which Option to use, Proposer shall contact the HUB Coordinator listed in 2.5.3.

Proposer must complete the HSP, then print, sign and scan *all pages* of the HSP Option selected, with additional support documentation*, **to the submittal email address noted above**. NOTE: signatures must be “wet” signatures. Digital signatures are not acceptable.

Any proposal submitted in response to this RFP that does not have a corresponding HSP meeting the above requirements may be rejected by University and returned to Proposer unopened as non-responsive due to material failure to comply with advertised specifications.

University will send an email confirmation to each Proposer upon receipt of the Proposer’s HSP. Each Proposer’s HSP will be evaluated for completeness and compliance prior to opening the proposal to confirm Proposer compliance with HSP rules and standards. Proposer’s failure to submit one (1) completed and signed HUB Subcontracting Plan **to the email address noted above** may result in University’s rejection of the proposal as non-responsive due to material failure to comply with advertised specifications; such a proposal *may* be returned to the Proposer unopened (ref. **Section 1.5** of **APPENDIX ONE** to this RFP). **Note:** *The requirement that Proposer provide one (1) completed and signed pdf of the HSP under this **Section 2.5.4** is separate from, and does not affect, Proposer’s obligation to provide University with the number of copies of its proposal as specified in **Section 3.1** of this RFP.*

***If Proposer's submitted HSP refers to specific page(s) / Sections(s) of Proposer's proposal that explain how Proposer will perform entire contract with its own equipment, supplies, materials and/or employees, Proposer must submit copies of those pages with the HSP sent to the HSP Submittal email address noted above. In addition, all solicitation emails to potential subcontractors must be included as backup documentation to the Proposer's HSP to demonstrate Good Faith Effort. Failure to do so will slow the evaluation process and may result in DISQUALIFICATION.**

2.6 Pre-Proposal Conference Call

University will hold a pre-proposal conference call at **3 p.m. Central Time on Monday, October 15th, 2018**. The pre-proposal conference call will allow all Proposers an opportunity to ask University's representatives relevant questions and clarify provisions of this RFP.

Call-in number: (877)226-9790

Participant Code: 6269693#

SECTION 3

SUBMISSION OF PROPOSAL

3.1 Number of Copies

- A. One (1) complete paper copy of its *entire* proposal.

The paper copy of the proposal should contain the mark “original” on the front cover of the proposal. An original signature by an authorized officer of Proposer must appear on the Execution of Offer (ref. Section 2 of APPENDIX ONE) of the submitted paper copy of the proposal.

University does not consider electronic signatures to be valid therefore the original signature must be a “wet signature.”

- B. One (1) complete electronic copy of its entire proposal in a single .pdf file on USB Flash Drive. USB Flash Drive must include a protective cover and be labeled with Proposer’s name and RFP number. In addition, Proposer must submit one (1) complete electronic copy of the proposal on the same USB Flash Drive on which all proposed pricing information, provided in response to **Section 6**, has been removed.

3.2 Submission

Proposals must be received by University on or before the Submittal Deadline (ref. **Section 2.1** of this RFP) and should be delivered to:

The University of Texas System Administration
210 West 7th Street
Austin, Texas 78701-2982
Attn: Darya Vienne

NOTE: Show the Request for Proposal number and submittal date in the lower left-hand corner of sealed bid envelope (box / container).

Proposals must be typed on letter-size (8-1/2” x 11”) paper, and must be submitted in a 3-ring binder. Preprinted material should be referenced in the proposal and included as labeled attachments. Sections within a proposal should be divided by tabs for ease of reference.

3.3 Proposal Validity Period

Each proposal must state that it will remain valid for University’s acceptance for a minimum of one hundred and twenty (120) days after the Submittal Deadline, to allow time for evaluation, selection, and any unforeseen delays.

3.4 Terms and Conditions

- 3.4.1 Proposer must comply with the requirements and specifications contained in this RFP, including the Agreement (ref. **APPENDIX TWO**), the Notice to Proposer (ref. **Section 2** of this RFP), Proposal Requirements (ref. **APPENDIX ONE**) and the Specifications and Additional Questions (ref. **Section 5** of this RFP). If there is a conflict among the provisions in this RFP, the provision requiring Proposer to supply the better quality or greater quantity of services will prevail, or if such conflict

does not involve quality or quantity, then interpretation will be in the following order of precedence:

- 3.4.1.1. Specifications and Additional Questions (ref. **Section 5** of this RFP);
- 3.4.1.2. Redlined Sample Agreement (ref. **Section 4** and **APPENDIX TWO**);
- 3.4.1.3. Proposal Requirements (ref. **APPENDIX ONE**);
- 3.4.1.4. Notice to Proposers (ref. **Section 2** of this RFP).

3.5 Submittal Checklist

Proposer is instructed to complete, sign, and return the following documents as a part of its proposal. If Proposer fails to return each of the following items with its proposal, then University may reject the proposal:

- 3.5.1 Signed and Completed Execution of Offer (ref. **Section 2** of **APPENDIX ONE**)
- 3.5.2 Signed and Completed Pricing and Delivery Schedule (ref. **Section 6** of this RFP)
- 3.5.3 Responses to Proposer's General Questionnaire (ref. **Section 3** of **APPENDIX ONE**)
- 3.5.4 Signed and Completed Addenda Checklist (ref. **Section 4** of **APPENDIX ONE**)
- 3.5.5 Responses to questions and requests for information in the Specifications and Additional Questions Section (ref. **Section 5** of this RFP)
- 3.5.6 Completed Voluntary Product Accessibility Template (VPAT) (ref. **Section 5.2.2** of this RFP).
- 3.5.7 Completed Higher Education Vendor Assessment Tool (HECVAT) (ref. **APPENDIX FOUR** of this RFP).

SECTION 4

GENERAL TERMS AND CONDITIONS

The terms and conditions contained in the attached Agreement (ref. **APPENDIX TWO**) or, in the sole discretion of University, terms and conditions substantially similar to those contained in the Agreement, will constitute and govern any agreement that results from this RFP. If Proposer takes exception to any terms or conditions set forth in the Agreement, Proposer will submit redlined **APPENDIX TWO** as part of its proposal in accordance with **Section 5.2.1** of this RFP.

Additionally, Proposer must submit as part of its Proposal all terms and conditions that it proposes to include in any contract or agreement resulting from this RFP (such as software license terms and conditions) in accordance with **Section 5.2.1** of this RFP. Proposer bears all risk and responsibility for its failure to include such terms and conditions in its Proposal. The University will not be bound by or required to accept or agree to any terms and conditions that a Proposer includes (or fails to include) in its Proposal.

Proposer's exceptions and proposed terms and conditions will be reviewed by University and may result in disqualification of Proposer's proposal as non-responsive to this RFP. If Proposer's exceptions do not result in disqualification of Proposer's proposal, then University may consider Proposer's exceptions when University evaluates the Proposer's proposal.

SECTION 5

SPECIFICATIONS AND ADDITIONAL QUESTIONS

5.1 General

The minimum requirements and the specifications for the Services, as well as certain requests for information to be provided by Proposer as part of its proposal, are set forth below. As indicated in **Section 2.3** of this RFP, the successful Proposer is referred to as the “**Contractor.**”

Contract Term: University intends to enter into an agreement with the Contractor to perform the Services for a six (6) years base term.

Disclosure of Existing Agreement: Various University departments have existing event management system agreements with Cvent, which are scheduled to expire in 2019, 2020 and 2021.

5.2 Additional Questions Specific to this RFP

Proposer must submit the following information as part of Proposer’s proposal:

5.2.1 If Proposer takes exception to any terms or conditions set forth in the Agreement (ref. **APPENDIX TWO**), Proposer must redline APPENDIX TWO and include **APPENDIX TWO** as part of its Proposal. If Proposer agrees with terms or conditions set forth in the **APPENDIX TWO**, Proposer will submit a written statement acknowledging it.

5.2.2 In its proposal, Proposer must indicate whether it will consent to include in the Agreement the “Access by Individuals with Disabilities” language that is set forth in **APPENDIX THREE, Access by Individuals with Disabilities**. If Proposer objects to the inclusion of the “Access by Individuals with Disabilities” language in the Agreement, Proposer must, as part of its proposal, specifically identify and describe in detail all of the reasons for Proposer’s objection. NOTE THAT A GENERAL OBJECTION IS NOT AN ACCEPTABLE RESPONSE TO THIS QUESTION. NOTE THAT PROPOSER IS REQUIRED TO SUBMIT COMPLETED VPAT (VOLUNTARY PRODUCT ACCESSIBILITY TEMPLATE) WITH PROPOSAL. VPAT document to complete is located at the following website: <https://www.itic.org/dotAsset/d432b9da-3696-47fe-a521-7d0458d48202.doc>

5.2.3 In its proposal, Proposer must respond to each item listed in **APPENDIX FOUR**, Higher Education Vendor Assessment Tool (HECVAT).

5.3 Scope of Work

As part of the RFP submission package, Proposers must complete *Types of Services Offered by Proposer* document, which can be found in **Section 5.4** of this RFP. The specifications listed in **Section 5.3** of the RFP document and the items found in **Section 5.4** are identical.

The University of Texas System has identified Business, Tracking and Reporting, Technical, Operations & Support specifications for a Software, which are outlined below. **Note that these Specifications are not limited to the list provided. Proposers are invited to submit their proposal if they do not meet all of the Specifications outlined below;** suitability of Proposal will be determined during the evaluation stage of the RFP process.

1. Business Specifications

- a. Program content management, including event creation, event registration, ecommerce, and activity reporting, with customization for event;
- b. Integrated email system that supports html message creation and constituent database integration;
- c. Financial management and budgeting;
- d. Venue sourcing;
- e. Administration / Communication;
- f. Overall registration management, including online registration services;
- g. Social media integration;
- h. Mobile application availability;
- i. Registration software and database, including ability to import legacy data;
- j. Ability to enter batches of offline donations and registrations;
- k. Payment gateway;
- l. Vendor management;
- m. Exhibition management;
- n. Accommodation and conference / event lodging tie-ins (e.g., Passkey);
- o. Survey / Evaluation functionality;
- p. Ability to maintain separate departmental instances to limit the visibility of events and data;
- q. Ability to allow administrators to define and assign different user levels with variable levels of access to the system (role-based security).

2. Tracking and Reporting Specifications

- a. Ability to import / export files and reports to / from Microsoft Office;
- b. Ability to export data from the proposed system to CRM system and/or financial software system;
- c. User dashboards;
- d. Ability to generate reports;
- e. Ability to easily build custom reports;
- f. Creates audit trail of every action taken on a submission / project.

3. Technical Specifications

- a. Cloud-based solution (SaaS);
- b. Compliance with all state electronic information resources accessibility requirements;
- c. Must be compliant with Payment Card Industry (PCI) standards (have an attestation of compliance for service providers);
- d. Ability to scale to meet increased demand without downtime;
- e. Support Android and iPhone mobile devices;
- f. All website content must be clearly visible and functional in Internet Explorer, Safari, Microsoft Edge, Firefox, and Google Chrome browsers;
- g. The log-on page must not allow the browser to store the information entered in the cache. The auto-complete feature must be turned off for every form;
- h. The font must be easy to read, no smaller than 10px; and
- i. All web content and downloadable documents, including Adobe Portable Document Format (PDF) files, must be made accessible to persons with disabilities, in accordance with APPENDICES (TBD) and (TBD) of this RFP document;
- j. Support integration with existing customer relationship management and financial support services software via web services or application programming interface (API);
- k. Secure access using at minimum SSL/HTTPS to access application and web services;
- l. Integrate with UT System's single-sign on technology (SAML, Shibboleth, etc.);
- m. Archive of data to be kept for ten (10) years.

4. Operations and Support

- a. Provide 24/7/365 technical and end-user web-based and telephone support;
- b. Have a history of reasonable response times associated with service-related incidents;
- c. Offer a dedicated account manager;
- d. Provide training and detailed software, database, and process manuals;
- e. Adhere to appropriate communications for all scheduled maintenance, changes, and upgrades.

5. Usage at UT System Administration

Refer to the table below to analyze UT System’s existent usage under the existing agreement.

	Total
Number of licenses (user logins/admins)	13
Number of events per year (odd/even years)	21
Number of registrations processed per year	3,975

5.4 Types of Services Offered by Proposer (20%)

Indicate if the Specifications below are provided in Proposer’s Software Current Version, Future Version (mark the expected release date), as Custom Enhancement (provide additional cost information in **Section 6** of this RFP) or are Not Supported.

Business Specifications	In Current Version (10 points)	As a Custom Enhancement (5 points)	In Future Version (1 point)	Not Supported (0 points)
a. Program content management, including event creation, event registration, ecommerce, and activity reporting, with customization for event				
b. Integrated email system that supports html message creation and constituent database integration				
c. Financial management and budgeting				
d. Venue sourcing				
e. Administration / Communication				
f. Overall registration management, including online registration services				
g. Social media integration				
h. Mobile application availability				

i. Registration software and database, including ability to import legacy data				
j. Ability to enter batches of offline donations and registrations				
k. Payment gateway				
l. Vendor management				
m. Exhibition management				
n. Accommodation and conference/event lodging tie-ins (e.g., Passkey)				
o. Survey/Evaluation functionality				
p. Ability to maintain separate departmental instances to limit the visibility of events and data				
q. Ability to allow administrators to define and assign different user levels with variable levels of access to the system (role-based security)				
Tracking and Reporting Specifications	In Current Version (10 points)	As a Custom Enhancement (5 points)	In Future Version (1 point)	Not Supported (0 points)
a. Ability to import / export files and reports to / from Microsoft Office				
b. Ability to export data from the proposed system to CRM system and/or financial software system;				
c. User dashboards;				
d. Ability to generate reports;				
e. Ability to easily build custom reports;				
f. Creates audit trail of every action taken on a submission / project.				
Technical Specifications	In Current Version (10 points)	As a Custom Enhancement (5 points)	In Future Version (1 point)	Not Supported (0 points)
a. Cloud-based solution (SaaS);				
b. Compliance with all state electronic information resources accessibility requirements;				
c. Must be compliant with Payment Card Industry (PCI) standards (have an attestation of compliance for service providers);				
d. Ability to scale to meet increased demand without downtime;				
e. Support Android and iPhone mobile devices;				
f. All website content must be clearly visible and functional in Internet Explorer, Safari, Microsoft Edge, Firefox, and Google Chrome browsers;				
g. The log-on page must not allow the browser to store the information entered in the cache. The				

auto-complete feature must be turned off for every form;				
h. The font must be easy to read, no smaller than 10px; and				
i. All web content and downloadable documents, including Adobe Portable Document Format (PDF) files, must be made accessible to persons with disabilities, in accordance with APPENDIX THREE of this RFP document;				
j. Support integration with existing customer relationship management and financial support services software via web services or application programming interface (API);				
k. Secure access using at minimum SSL/HTTPS to access application and web services;				
l. Integrate with UT System's single-sign on technology (SAML, Shibboleth, etc.);				
m. Archive of data to be kept for ten (10) years.				
Operations and Support	Available (10 points)	Available for additional fee (5 points)	Not available (0 points)	
a. Provide 24/7/365 technical and end-user web-based and telephone support;				
b. Have a history of reasonable response times associated with service-related incidents;				
c. Offer a dedicated account manager;				
d. Provide training and detailed software, database, and process manuals;				
e. Adhere to appropriate communications for all scheduled maintenance, changes, and upgrades.				

5.5 Additional Questions Specific to this RFP

Proposer must submit the following information as part of Proposer's proposal:

Vendor Experience (10%)

1. Provide references from three (3) of Proposer's customers from the past five (5) years for services that are similar in scope, size, and complexity to the Services described in this RFP.

Provide the following information for each customer:

- Customer name and address;
 - Contact name with email address and phone number;
 - Time period in which work was performed;
 - Short description of work performed.
2. Has Proposer worked with University institutions in the past five (5) years? If "yes," state University Institution name, department name, department contact, and provide a brief description of work performed.

3. Describe the history and background of Proposer's company.
4. Describe Proposer's core product and service lines, and any optional services Proposer provides.
5. Describe Proposer's experience in providing event management services to large, public-sector organizations.

Platform Technology, Security and Functionality (20%)

6. Can Proposer's web site and mobile app be presented in non-English languages? Describe what languages are available.
7. Describe the user experience of Proposer's platform, including mobile application capabilities, for participants and administrative users.
8. How often is maintenance performed and how is this communicated to clients? Does maintenance require downtime? For how long?
9. Explain how Proposer manages system enhancements. How often is Proposer's platform upgraded?

Account Management (20%)

10. Briefly outline Proposer's account management philosophy.
11. Detail Proposer's account manager / executive turn-over rate for the last twelve (12) months.
12. What are the response metrics from customer support, specifically:
 - What is the expected response time for the account management team when responding to UT System staff?
 - What is the expected response time for escalated customer service team members to members of the University staff?
13. Detail any additional functionalities not listed in the SOW. Provide the pricing structure for additional functionalities in **Section 6.3** of this RFP.
14. Provide temporary access to the software to perform a quality and requirements review of software features, including mobile application(s), as a part of the RFP process. If available, provide links to the demos readily available online for viewing.
15. Describe the efforts Proposer intends to take to ensure compliance with the General Data Protection Regulation (GDPR) for data that comes from an individual located in a European Union member state. Include any statements, consent language or forms used by Proposer to engage with a customer when GDPR compliance may be required.

SECTION 6

PRICING AND DELIVERY SCHEDULE

Proposal of: _____
(Proposer Company Name)

To: The University of Texas System

RFP No.: 720-1904 Event management Software

Ladies and Gentlemen:

Having carefully examined all the specifications and requirements of this RFP and any attachments thereto, the undersigned proposes to furnish the required pursuant to the above-referenced Request for Proposal upon the terms quoted (firm fixed price) below. The University will not accept proposals which include assumptions or exceptions to the work identified in this RFP.

6.1 Service Package Scenarios

Proposers must provide total cost for the three (3) scenarios listed below that will be used for scoring purposes. The total cost for each scenario (Scenario A, Scenario B and Scenario C) must be submitted in **Section 6.2**, Pricing for Services Offered of this RFP.

Assumption: Proposer should assume that the agreement between parties is for six (6) years total with no renewals.

Note: The three (3) scenarios are only examples. For each scenario Proposer must explain how the fees were calculated (e.g. per registrant, per license, per year, etc.).

Scenario A

One (1) event per year
Three hundred (300) registrations per year
Two (2) administrative users
Six (6) year agreement with no extensions

Scenario B

One (1) event every two (2) years
Five hundred (500) registrations every two (2) years
Five (5) administrative users
Six (6) year agreement with no extensions

Scenario C

Twelve (12) events per year
1,200 registrations per year
Three (3) administrative users
Six (6) year agreement with no extensions

6.2 Pricing for Services Offered

Proposers must provide the total cost for all three (3) scenarios listed in **Section 6.1** of this RFP.

1. Total Cost for Scenario A (10%) \$ _____
2. Total Cost for Scenario B (10%) \$ _____
3. Total Cost for Scenario C (10%) \$ _____

6.3 Pricing for Additional Functionalities

5.4. Provide pricing for additional functionalities (if offered by Proposer), not listed in **Sections 5.3 &**

6.4 Discounts

Describe all discounts that may be available to University, including, educational, federal, state and local discounts.

6.5 Delivery Schedule of Events and Time Periods

Indicate number of calendar days needed to commence the Services from the execution of the services agreement:

_____ Calendar Days

6.6 Payment Terms

University’s standard payment terms are “net 30 days” as mandated by the *Texas Prompt Payment Act* (ref. [Chapter 2251, Government Code](#)).

Indicate below the prompt payment discount that Proposer offers:

Prompt Payment Discount: _____% _____ days / net 30 days.

[Section 51.012, Education Code](#), authorizes University to make payments through electronic funds transfer methods. Proposer agrees to accept payments from University through those methods, including the automated clearing house system (“ACH”). Proposer agrees to provide Proposer’s banking information to University in writing on Proposer letterhead signed by an authorized representative of Proposer. Prior to the first payment, University will confirm Proposer’s banking information. Changes to Proposer’s bank information must be communicated to University in writing at least thirty (30) days before the effective date of the change and must include an [IRS Form W-9](#) signed by an authorized representative of Proposer.

University, an agency of the State of Texas, is exempt from Texas Sales & Use Tax on goods and services in accordance with [§151.309, Tax Code](#), and [Title 34 TAC §3.322](#). Pursuant to [34 TAC §3.322\(c\)\(4\)](#), University is not required to provide a tax exemption certificate to establish its tax exempt status.

Respectfully submitted,

Proposer: _____

By: _____
(Authorized Signature for Proposer)

Name: _____

Title: _____

Date: _____

**APPENDIX ONE
PROPOSAL REQUIREMENTS**

TABLE OF CONTENTS

SECTION 1: GENERAL INFORMATION..... 1

SECTION 2: EXECUTION OF OFFER 4

SECTION 3: PROPOSER'S GENERAL QUESTIONNAIRE 7

SECTION 4: ADDENDA CHECKLIST 9

SECTION 1

GENERAL INFORMATION

1.1 Purpose

University is soliciting competitive sealed proposals from Proposers having suitable qualifications and experience providing services in accordance with the terms, conditions and requirements set forth in this RFP. This RFP provides sufficient information for interested parties to prepare and submit proposals for consideration by University.

By submitting a proposal, Proposer certifies that it understands this RFP and has full knowledge of the scope, nature, quality, and quantity of the services to be performed, the detailed requirements of the services to be provided, and the conditions under which such services are to be performed. Proposer also certifies that it understands that all costs relating to preparing a response to this RFP will be the sole responsibility of the Proposer.

PROPOSER IS CAUTIONED TO READ THE INFORMATION CONTAINED IN THIS RFP CAREFULLY AND TO SUBMIT A COMPLETE RESPONSE TO ALL REQUIREMENTS AND QUESTIONS AS DIRECTED.

1.2 Inquiries and Interpretations

University may in its sole discretion respond in writing to written inquiries concerning this RFP and mail its response as an Addendum to all parties recorded by University as having received a copy of this RFP. Only University's responses that are made by formal written Addenda will be binding on University. Any verbal responses, written interpretations or clarifications other than Addenda to this RFP will be without legal effect. All Addenda issued by University prior to the Submittal Deadline will be and are hereby incorporated as a part of this RFP for all purposes.

Proposers are required to acknowledge receipt of each Addendum as specified in this Section. The Proposer must acknowledge all Addenda by completing, signing and returning the Addenda Checklist (ref. **Section 4** of **APPENDIX ONE**). The Addenda Checklist must be received by University prior to the Submittal Deadline and should accompany the Proposer's proposal.

Any interested party that receives this RFP by means other than directly from University is responsible for notifying University that it has received an RFP package, and should provide its name, address, telephone and facsimile (**FAX**) numbers, and email address, to University, so that if University issues Addenda to this RFP or provides written answers to questions, that information can be provided to that party.

1.3 Public Information

Proposer is hereby notified that University strictly adheres to all statutes, court decisions and the opinions of the Texas Attorney General with respect to disclosure of public information.

University may seek to protect from disclosure all information submitted in response to this RFP until such time as a final agreement is executed.

Upon execution of a final agreement, University will consider all information, documentation, and other materials requested to be submitted in response to this RFP, to be of a non-confidential and non-proprietary nature and, therefore, subject to public disclosure under the *Texas Public Information Act* (ref. [Chapter 552, Government Code](#)). Proposer will be advised of a request for public information that implicates their materials and will have the opportunity to raise any objections to disclosure to the Texas Attorney General. Certain information may be protected from release under §§[552.101](#), [552.104](#), [552.110](#), [552.113](#), and [552.131](#), *Government Code*.

1.4 Type of Agreement

Contractor, if any, will be required to enter into a contract with University in a form substantially similar to the between University and Contractor (the "**Agreement**") attached to this RFP as **APPENDIX TWO** and incorporated for all purposes.

1.5 Proposal Evaluation Process

University will select Contractor by using the competitive sealed proposal process described in this Section. Any proposals that are not submitted by the Submittal Deadline or that are not accompanied by required number of completed and signed originals of the HSP will be rejected by University as non-responsive due to material failure to comply with this RFP (ref. **Section 2.5.4** of this RFP). Upon completion of the initial review and evaluation of proposals, University may invite one or more selected Proposers to participate in oral presentations. University will use commercially reasonable efforts to avoid public disclosure of the contents of a proposal prior to selection of Contractor.

University may make the selection of Contractor on the basis of the proposals initially submitted, without discussion, clarification or modification. In the alternative, University may make the selection of Contractor on the basis of negotiation with any of the Proposers. In conducting negotiations, University will use commercially reasonable efforts to avoid disclosing the contents of competing proposals.

University may discuss and negotiate all elements of proposals submitted by Proposers within a specified competitive range. For purposes of negotiation, University may establish, after an initial review of the proposals, a competitive range of acceptable or potentially acceptable proposals composed of the highest rated proposal(s). In that event, University may defer further action on proposals not included within the competitive range pending the selection of Contractor; provided, however, University reserves the right to include additional proposals in the competitive range if deemed to be in the best interest of University.

After the Submittal Deadline but before final selection of Contractor, University may permit Proposer to revise its proposal in order to obtain the Proposer's best and final offer. In that event, representations made by Proposer in its revised proposal, including price and fee quotes, will be binding on Proposer. University will provide each Proposer within the competitive range with an equal opportunity for discussion and revision of its proposal. University is not obligated to select the Proposer offering the most attractive economic terms if that Proposer is not the most advantageous to University overall, as determined by University.

University reserves the right to (a) enter into an agreement for all or any portion of the requirements and specifications set forth in this RFP with one or more Proposers, (b) reject any and all proposals and re-solicit proposals, or (c) reject any and all proposals and temporarily or permanently abandon this selection process, if deemed to be in the best interests of University. Proposer is hereby notified that University will maintain in its files concerning this RFP a written record of the basis upon which a selection, if any, is made by University.

1.6 Proposer's Acceptance of RFP Terms

Proposer (1) accepts [a] Proposal Evaluation Process (ref. **Section 1.5** of **APPENDIX ONE**), [b] Criteria for Selection (ref. **2.3** of this RFP), [c] Specifications and Additional Questions (ref. **Section 5** of this RFP), [d] terms and conditions of the Agreement (ref. **APPENDIX TWO**), and [e] all other requirements and specifications set forth in this RFP; and (2) acknowledges that some subjective judgments must be made by University during this RFP process.

1.7 Solicitation for Proposal and Proposal Preparation Costs

Proposer understands and agrees that (1) this RFP is a solicitation for proposals and University has made no representation written or oral that one or more agreements with University will be awarded under this RFP; (2) University issues this RFP predicated on University's anticipated requirements for the Services, and University has made no representation, written or oral, that any particular scope of services will actually be required by University; and (3) Proposer will bear, as its sole risk and responsibility, any cost that arises from Proposer's preparation of a proposal in response to this RFP.

1.8 Proposal Requirements and General Instructions

- 1.8.1 Proposer should carefully read the information contained herein and submit a complete proposal in response to all requirements and questions as directed.
- 1.8.2 Proposals and any other information submitted by Proposer in response to this RFP will become the property of University.
- 1.8.3 University will not provide compensation to Proposer for any expenses incurred by the Proposer for proposal preparation or for demonstrations or oral presentations that may be made by Proposer. Proposer submits its proposal at its own risk and expense.
- 1.8.4 Proposals that (i) are qualified with conditional clauses; (ii) alter, modify, or revise this RFP in any way; or (iii) contain irregularities of any kind, are subject to disqualification by University, at University's sole discretion.
- 1.8.5 Proposals should be prepared simply and economically, providing a straightforward, concise description of Proposer's ability to meet the requirements and specifications of this RFP. Emphasis should be on completeness, clarity of content, and responsiveness to the requirements and specifications of this RFP.
- 1.8.6 University makes no warranty or guarantee that an award will be made as a result of this RFP. University reserves the right to accept or reject any or all proposals, waive any formalities, procedural requirements, or minor technical inconsistencies, and delete any requirement or specification from this RFP or the Agreement when deemed to be in University's best interest. University reserves the right to seek clarification from any Proposer concerning any item contained in its proposal prior to final selection. Such clarification may be provided by telephone conference or personal meeting with or writing to University, at University's sole discretion. Representations made by Proposer within its proposal will be binding on Proposer.
- 1.8.7 Any proposal that fails to comply with the requirements contained in this RFP may be rejected by University, in University's sole discretion.

1.9 Preparation and Submittal Instructions

1.9.1 Specifications and Additional Questions

Proposals must include responses to the questions in Specifications and Additional Questions (ref. **Section 5** of this RFP). Proposer should reference the item number and repeat the question in its response. In cases where a question does not apply or if unable to respond, Proposer should refer to the item number, repeat the question, and indicate N / A (Not Applicable) or N / R (No Response), as appropriate. Proposer should explain the reason when responding N / A or N / R.

1.9.2 Execution of Offer

Proposer must complete, sign and return the attached Execution of Offer (ref. **Section 2** of **APPENDIX ONE**) as part of its proposal. The Execution of Offer must be signed by a representative of Proposer duly authorized to bind the Proposer to its proposal. Any proposal received without a completed and signed Execution of Offer may be rejected by University, in its sole discretion.

1.9.3 Pricing and Delivery Schedule

Proposer must complete and return the Pricing and Delivery Schedule (ref. **Section 6** of this RFP), as part of its proposal. In the Pricing and Delivery Schedule, the Proposer should describe in detail (a) the total fees for the entire scope of the Services; and (b) the method by which the fees are calculated. The fees must be inclusive of all associated costs for delivery, labor, insurance, taxes, overhead, and profit.

University will not recognize or accept any charges or fees to perform the Services that are not specifically stated in the Pricing and Delivery Schedule.

In the Pricing and Delivery Schedule, Proposer should describe each significant phase in the process of providing the Services to University, and the time period within which Proposer proposes to be able to complete each such phase.

1.9.4 Proposer's General Questionnaire

Proposals must include responses to the questions in Proposer's General Questionnaire (ref. **Section 3** of **APPENDIX ONE**). Proposer should reference the item number and repeat the question in its response. In cases where a question does not apply or if unable to respond, Proposer should refer to the item number, repeat the question, and indicate N / A (Not Applicable) or N / R (No Response), as appropriate. Proposer should explain the reason when responding N / A or N / R.

1.9.5 Addenda Checklist

Proposer should acknowledge all Addenda to this RFP (if any) by completing, signing and returning the Addenda Checklist (ref. **Section 4** of **APPENDIX ONE**) as part of its proposal. Any proposal received without a completed and signed Addenda Checklist may be rejected by University, in its sole discretion.

1.9.6 Submission

*Proposer should submit all proposal materials as instructed in **Section 3** of this RFP. RFP No. (ref. **Title Page** of this RFP) and Submittal Deadline (ref. **Section 2.1** of this RFP) should be clearly shown (1) in the Subject line of any email transmitting the proposal, and (2) in the lower left-hand corner on the top surface of any envelope or package containing the proposal. In addition, the name and the return address of the Proposer should be clearly visible in any email or on any envelope or package.*

University will not under any circumstances consider a proposal that is received after the Submittal Deadline or which is not accompanied by the HSP as required by **Section 2.5** of this RFP. University will not accept proposals submitted by email, telephone or FAX transmission.

Except as otherwise provided in this RFP, no proposal may be changed, amended, or modified after it has been submitted to University. However, a proposal may be withdrawn and resubmitted at any time prior to the Submittal Deadline. No proposal may be withdrawn after the Submittal Deadline without University's consent, which will be based on Proposer's written request explaining and documenting the reason for withdrawal, which is acceptable to University.

SECTION 2

EXECUTION OF OFFER

THIS EXECUTION OF OFFER MUST BE COMPLETED, SIGNED AND RETURNED WITH PROPOSER'S PROPOSAL. FAILURE TO COMPLETE, SIGN AND RETURN THIS EXECUTION OF OFFER WITH THE PROPOSER'S PROPOSAL MAY RESULT IN THE REJECTION OF THE PROPOSAL.

- 2.1 Representations and Warranties.** Proposer represents, warrants, certifies, acknowledges, and agrees as follows:
- 2.1.1 Proposer will furnish the Services to University and comply with all terms, conditions, requirements and specifications set forth in this RFP and any resulting Agreement.
 - 2.1.2 This RFP is a solicitation for a proposal and is not a contract or an offer to contract. Submission of a proposal by Proposer in response to this RFP will not create a contract between University and Proposer. University has made no representation or warranty, written or oral, that one or more contracts with University will be awarded under this RFP. Proposer will bear, as its sole risk and responsibility, any cost arising from Proposer's preparation of a response to this RFP.
 - 2.1.3 Proposer is a reputable company that is lawfully and regularly engaged in providing the Services.
 - 2.1.4 Proposer has the necessary experience, knowledge, abilities, skills, and resources to perform the Services.
 - 2.1.5 Proposer is aware of, is fully informed about, and is in full compliance with all applicable federal, state and local laws, rules, regulations and ordinances relating to performance of the Services.
 - 2.1.6 Proposer understands (i) the requirements and specifications set forth in this RFP and (ii) the terms and conditions set forth in the Agreement under which Proposer will be required to operate.
 - 2.1.7 Proposer will not delegate any of its duties or responsibilities under this RFP or the Agreement to any sub-contractor, except as expressly provided in the Agreement.
 - 2.1.8 Proposer will maintain any insurance coverage required by the Agreement during the entire term.
 - 2.1.9 All statements, information and representations prepared and submitted in response to this RFP are current, complete, true and accurate. University will rely on such statements, information and representations in selecting Contractor. If selected by University, Proposer will notify University immediately of any material change in any matters with regard to which Proposer has made a statement or representation or provided information.
 - 2.1.10 PROPOSER WILL DEFEND WITH COUNSEL APPROVED BY UNIVERSITY, INDEMNIFY, AND HOLD HARMLESS UNIVERSITY, THE STATE OF TEXAS, AND ALL OF THEIR REGENTS, OFFICERS, AGENTS AND EMPLOYEES, FROM AND AGAINST ALL ACTIONS, SUITS, DEMANDS, COSTS, DAMAGES, LIABILITIES AND OTHER CLAIMS OF ANY NATURE, KIND OR DESCRIPTION, INCLUDING REASONABLE ATTORNEYS' FEES INCURRED IN INVESTIGATING, DEFENDING OR SETTling ANY OF THE FOREGOING, ARISING OUT OF, CONNECTED WITH, OR RESULTING FROM ANY NEGLIGENT ACTS OR OMISSIONS OR WILLFUL MISCONDUCT OF PROPOSER OR ANY AGENT, EMPLOYEE, SUBCONTRACTOR, OR SUPPLIER OF PROPOSER IN THE EXECUTION OR PERFORMANCE OF ANY CONTRACT OR AGREEMENT RESULTING FROM THIS RFP.
 - 2.1.11 Pursuant to §§[2107.008](#) and [2252.903](#), *Government Code*, any payments owing to Proposer under the Agreement may be applied directly to any debt or delinquency that Proposer owes the State of Texas or any agency of the State of Texas, regardless of when it arises, until such debt or delinquency is paid in full.
 - 2.1.12 Any terms, conditions, or documents attached to or referenced in Proposer's proposal are applicable to this procurement only to the extent that they (a) do not conflict with the laws of the State of Texas or this RFP, and (b) do not place any requirements on University that are not set forth in this RFP. Submission of a proposal is Proposer's good faith intent to enter into the Agreement with University as specified in this RFP and that Proposer's intent is not contingent upon University's acceptance or execution of any terms, conditions, or other documents attached to or referenced in Proposer's proposal.
 - 2.1.13 Pursuant to [Chapter 2270, Government Code](#), Proposer certifies Proposer (1) does not currently boycott Israel; and (2) will not boycott Israel during the Term of the Agreement. Proposer acknowledges the Agreement may be terminated and payment withheld if this certification is inaccurate.
 - 2.1.14 Pursuant to [Subchapter F, Chapter 2252, Government Code](#), Proposer certifies Proposer is not engaged in business with Iran, Sudan, or a foreign terrorist organization. Proposer acknowledges the Agreement may be terminated and payment withheld if this certification is inaccurate.
- 2.2 No Benefit to Public Servants.** Proposer has not given or offered to give, nor does Proposer intend to give at any time hereafter, any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor or service to a public servant in connection with its proposal. Failure to sign this Execution of Offer, or signing with a false statement, may void the submitted proposal or any resulting Agreement, and Proposer may be removed from all proposer lists at University.
- 2.3 Tax Certification.** Proposer is not currently delinquent in the payment of any taxes due under [Chapter 171, Tax Code](#), or Proposer is exempt from the payment of those taxes, or Proposer is an out-of-state taxable entity that is not subject to those taxes, whichever is applicable. A false certification will be deemed a material breach of any resulting contract or agreement and, at University's option, may result in termination of any resulting Agreement.

- 2.4 Antitrust Certification.** Neither Proposer nor any firm, corporation, partnership or institution represented by Proposer, nor anyone acting for such firm, corporation or institution, has violated the antitrust laws of the State of Texas, codified in [§15.01 et seq., Business and Commerce Code](#), or the Federal antitrust laws, nor communicated directly or indirectly the proposal made to any competitor or any other person engaged in such line of business.
- 2.5 Authority Certification.** The individual signing this document and the documents made a part of this RFP, is authorized to sign the documents on behalf of Proposer and to bind Proposer under any resulting Agreement.
- 2.6 Child Support Certification.** Under [§231.006, Family Code](#), relating to child support, the individual or business entity named in Proposer's proposal is not ineligible to receive award of the Agreement, and any Agreements resulting from this RFP may be terminated if this certification is inaccurate.
- 2.7 Relationship Certifications.**
- No relationship, whether by blood, marriage, business association, capital funding agreement or by any other such kinship or connection exists between the owner of any Proposer that is a sole proprietorship, the officers or directors of any Proposer that is a corporation, the partners of any Proposer that is a partnership, the joint venturers of any Proposer that is a joint venture, or the members or managers of any Proposer that is a limited liability company, on one hand, and an employee of any member institution of University, on the other hand, other than the relationships which have been previously disclosed to University in writing.
 - Proposer has not been an employee of any member institution of University within the immediate twelve (12) months prior to the Submittal Deadline.
 - No person who, in the past four (4) years served as an executive of a state agency was involved with or has any interest in Proposer's proposal or any contract resulting from this RFP (ref. [§669.003, Government Code](#)).
 - All disclosures by Proposer in connection with this certification will be subject to administrative review and approval before University enters into any Agreement resulting from this RFP with Proposer.
- 2.8 Compliance with Equal Employment Opportunity Laws.** Proposer is in compliance with all federal laws and regulations pertaining to Equal Employment Opportunities and Affirmative Action.
- 2.9 Compliance with Safety Standards.** All products and services offered by Proposer to University in response to this RFP meet or exceed the safety standards established and promulgated under the Federal Occupational Safety and Health Law ([Public Law 91-596](#)) and the *Texas Hazard Communication Act*, [Chapter 502, Health and Safety Code](#), and all related regulations in effect or proposed as of the date of this RFP.
- 2.10 Exceptions to Certifications.** Proposer will and has disclosed, as part of its proposal, any exceptions to the information stated in this Execution of Offer. All information will be subject to administrative review and approval prior to the time University makes an award or enters into any Agreement with Proposer.
- 2.11 Manufacturer Responsibility and Consumer Convenience Computer Equipment Collection and Recovery Act Certification.** If Proposer will sell or lease computer equipment to University under any Agreement resulting from this RFP then, pursuant to [§361.965\(c\), Health & Safety Code](#), Proposer is in compliance with the Manufacturer Responsibility and Consumer Convenience Computer Equipment Collection and Recovery Act set forth in [Chapter 361, Subchapter Y, Health & Safety Code](#), and the rules adopted by the Texas Commission on Environmental Quality under that Act as set forth in [30 TAC Chapter 328, §361.952\(2\), Health & Safety Code](#), states that, for purposes of the Manufacturer Responsibility and Consumer Convenience Computer Equipment Collection and Recovery Act, the term "computer equipment" means a desktop or notebook computer and includes a computer monitor or other display device that does not contain a tuner.
- 2.12 Conflict of Interest Certification.**
- Proposer is not a debarred vendor or the principal of a debarred vendor (i.e. owner, proprietor, sole or majority shareholder, director, president, managing partner, etc.) either at the state or federal level.
 - Proposer's provision of services or other performance under any Agreement resulting from this RFP will not constitute an actual or potential conflict of interest.
 - Proposer has disclosed any personnel who are related to any current or former employees of University.
 - Proposer has not given, nor does Proposer intend to give, at any time hereafter, any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor or service to an officer or employee of University in connection with this RFP.
- 2.13 Proposer should complete the following information:**

If Proposer is a Corporation, then State of Incorporation: _____

If Proposer is a Corporation, then Proposer's Corporate Charter Number: _____

RFP No.: 720-1904 Event Management Software

NOTICE: WITH FEW EXCEPTIONS, INDIVIDUALS ARE ENTITLED ON REQUEST TO BE INFORMED ABOUT THE INFORMATION THAT GOVERNMENTAL BODIES OF THE STATE OF TEXAS COLLECT ABOUT SUCH INDIVIDUALS. UNDER §§[552.021](#) AND [552.023](#), GOVERNMENT CODE, INDIVIDUALS ARE ENTITLED TO RECEIVE AND REVIEW SUCH INFORMATION. UNDER [§559.004, GOVERNMENT CODE](#), INDIVIDUALS ARE ENTITLED TO HAVE GOVERNMENTAL BODIES OF THE STATE OF TEXAS CORRECT INFORMATION ABOUT SUCH INDIVIDUALS THAT IS INCORRECT.

Submitted and Certified By:

(Proposer Institution's Name)

(Signature of Duly Authorized Representative)

(Printed Name / Title)

(Date Signed)

(Proposer's Street Address)

(City, State, Zip Code)

(Telephone Number)

(FAX Number)

(Email Address)

SECTION 3

PROPOSER'S GENERAL QUESTIONNAIRE

NOTICE: WITH FEW EXCEPTIONS, INDIVIDUALS ARE ENTITLED ON REQUEST TO BE INFORMED ABOUT THE INFORMATION THAT GOVERNMENTAL BODIES OF THE STATE OF TEXAS COLLECT ABOUT SUCH INDIVIDUALS. UNDER §§552.021 AND 552.023, GOVERNMENT CODE, INDIVIDUALS ARE ENTITLED TO RECEIVE AND REVIEW SUCH INFORMATION. UNDER §559.004, GOVERNMENT CODE, INDIVIDUALS ARE ENTITLED TO HAVE GOVERNMENTAL BODIES OF THE STATE OF TEXAS CORRECT INFORMATION ABOUT SUCH INDIVIDUALS THAT IS INCORRECT.

Proposals must include responses to the questions contained in this Proposer's General Questionnaire. Proposer should reference the item number and repeat the question in its response. In cases where a question does not apply or if unable to respond, Proposer should refer to the item number, repeat the question, and indicate N / A (Not Applicable) or N / R (No Response), as appropriate. Proposer will explain the reason when responding N / A or N / R.

3.1 Proposer Profile

3.1.1 Legal name of Proposer company:

Address of principal place of business:

Address of office that would be providing service under the Agreement:

Number of years in Business: _____

State of incorporation: _____

Number of Employees: _____

Annual Revenues Volume: _____

Name of Parent Corporation, if any _____

NOTE: If Proposer is a subsidiary, University prefers to enter into a contract or agreement with the Parent Corporation or to receive assurances of performance from the Parent Corporation.

3.1.2 State whether Proposer will provide a copy of its financial statements for the past two (2) years, if requested by University.

3.1.3 Proposer will provide a financial rating of the Proposer entity and any related documentation (such as a Dunn and Bradstreet analysis) that indicates the financial stability of Proposer.

3.1.4 Is Proposer currently for sale or involved in any transaction to expand or to become acquired by another business entity? If yes, Proposer will explain the expected impact, both in organizational and directional terms.

3.1.5 Proposer will provide any details of all past or pending litigation or claims filed against Proposer that would affect its performance under the Agreement with University (if any).

3.1.6 Is Proposer currently in default on any loan agreement or financing agreement with any bank, financial institution, or other entity? If yes, Proposer will specify the pertinent date(s), details, circumstances, and describe the current prospects for resolution.

3.1.7 Proposer will provide a customer reference list of no less than three (3) organizations with which Proposer currently has contracts and / or to which Proposer has previously provided services (within the past five (5) years) of a type and scope similar to those required by University's RFP. Proposer will include in its customer reference list the customer's company name, contact person, telephone number, project description, length of business relationship, and background of services provided by Proposer.

- 3.1.8 Does any relationship exist (whether by family kinship, business association, capital funding agreement, or any other such relationship) between Proposer and any employee of University? If yes, Proposer will explain.
- 3.1.9 Proposer will provide the name and Social Security Number for each person having at least 25% ownership interest in Proposer. This disclosure is mandatory pursuant to [§231.006, Family Code](#), and will be used for the purpose of determining whether an owner of Proposer with an ownership interest of at least 25% is more than 30 days delinquent in paying child support. Further disclosure of this information is governed by the *Texas Public Information Act* (ref. [Chapter 552, Government Code](#)), and other applicable law.

3.2 Approach to Project Services

- 3.2.1 Proposer will provide a statement of the Proposer's service approach and will describe any unique benefits to University from doing business with Proposer. Proposer will briefly describe its approach for each of the required services identified in **Section 5.3** Scope of Work of this RFP.
- 3.2.2 Proposer will provide an estimate of the earliest starting date for services following execution of the Agreement.
- 3.2.3 Proposer will submit a work plan with key dates and milestones. The work plan should include:
- 3.2.3.1 Identification of tasks to be performed;
 - 3.2.3.2 Time frames to perform the identified tasks;
 - 3.2.3.3 Project management methodology;
 - 3.2.3.4 Implementation strategy; and
 - 3.2.3.5 The expected time frame in which the services would be implemented.
- 3.2.4 Proposer will describe the types of reports or other written documents Proposer will provide (if any) and the frequency of reporting, if more frequent than required in this RFP. Proposer will include samples of reports and documents if appropriate.

3.3 General Requirements

- 3.3.1 Proposer will provide summary resumes for its proposed key personnel who will be providing services under the Agreement with University, including their specific experiences with similar service projects, and number of years of employment with Proposer.
- 3.3.2 Proposer will describe any difficulties it anticipates in performing its duties under the Agreement with University and how Proposer plans to manage these difficulties. Proposer will describe the assistance it will require from University.

3.4 Service Support

Proposer will describe its service support philosophy, how it is implemented, and how Proposer measures its success in maintaining this philosophy.

3.5 Quality Assurance

Proposer will describe its quality assurance program, its quality requirements, and how they are measured.

3.6 Miscellaneous

- 3.6.1 Proposer will provide a list of any additional services or benefits not otherwise identified in this RFP that Proposer would propose to provide to University. Additional services or benefits must be directly related to the goods and services solicited under this RFP.
- 3.6.2 Proposer will provide details describing any unique or special services or benefits offered or advantages to be gained by University from doing business with Proposer. Additional services or benefits must be directly related to the goods and services solicited under this RFP.
- 3.6.3 Does Proposer have a contingency plan or disaster recovery plan in the event of a disaster? If so, then Proposer will provide a copy of the plan.

SECTION 4

ADDENDA CHECKLIST

Proposal of: _____
(Proposer Company Name)

To: The University of Texas System

Ref.: Event Management Software

RFP No.: 720-1904

Ladies and Gentlemen:

The undersigned Proposer hereby acknowledges receipt of the following Addenda to the captioned RFP (initial if applicable).

Note: If there was only one (1) Addendum, initial just the first blank after No. 1, not all five (5) blanks below.

No. 1 _____ No. 2 _____ No. 3 _____ No. 4 _____ No. 5 _____

Respectfully submitted,

Proposer: _____

By: _____
(Authorized Signature for Proposer)

Name: _____

Title: _____

Date: _____

APPENDIX TWO
SAMPLE AGREEMENT
(INCLUDED AS SEPARATE ATTACHMENT)

APPENDIX THREE

ACCESS BY INDIVIDUALS WITH DISABILITIES

Contractor represents and warrants (**EIR Accessibility Warranty**) the electronic and information resources and all associated information, documentation, and support Contractor provides to University under this Agreement (**EIRs**) comply with applicable requirements set forth in [1 TAC Chapter 213](#), and [1 TAC §206.70](#) (ref. [Subchapter M, Chapter 2054, Government Code](#).) To the extent Contractor becomes aware that EIRs, or any portion thereof, do not comply with the EIR Accessibility Warranty, then Contractor represents and warrants it will, at no cost to University, either (1) perform all necessary remediation to make EIRs satisfy the EIR Accessibility Warranty or (2) replace EIRs with new EIRs that satisfy the EIR Accessibility Warranty. If Contractor fails or is unable to do so, University may terminate this Agreement and, within thirty (30) days after termination, Contractor will refund to University all amounts University paid under this Agreement.

APPENDIX FOUR
HIGHER EDUCATION VENDOR ASSESSMENT TOOL (HECVAT)
(INCLUDED AS SEPARATE ATTACHMENT)

AGREEMENT BETWEEN UNIVERSITY AND CONTRACTOR

This Agreement between University and Contractor (**Agreement**) is made and entered into effective as of _____, 20____ (**Effective Date**), by and between **The University of Texas** _____, an agency and institution of higher education established under the laws of the State of Texas (**University**), and _____, a _____ (**Contractor**), Federal Tax Identification Number.

University and Contractor hereby agree as follows:

1. **Scope of Work.**

- 1.1 Contractor will perform the scope of the work (**Work**) in **Exhibit A**, Scope of Work, to the satisfaction of University and in accordance with the schedule (**Schedule**) for Work in **Exhibit B**, Schedule. Time is of the essence in connection with this Agreement. University will have no obligation to accept late performance or waive timely performance by Contractor.
- 1.2 Contractor will obtain, at its own cost, any and all approvals, licenses, filings, registrations and permits required by federal, state or local, laws, statutes, regulations and ordinances (collectively, **Applicable Laws**), for the performance of Work.

2. **The Project.**

The Work will be provided in connection with event management software and all other related, necessary and appropriate services (**Project**).

3. **Time for Commencement and Completion.**

The term (**Initial Term**) of this Agreement will begin on the Effective Date and expire on _____, 20____. University will have the option to renew this Agreement for _____ (____) additional _____ (____) year terms (each a **Renewal Term**). The Initial Term and each Renewal Term are collectively referred to as the **Term**.

4. **Contractor's Obligations.**

- 4.1 Contractor will perform Work in compliance with (a) all Applicable Laws, and (b) the Board of Regents of The University of Texas System *Rules and Regulations* (<http://www.utsystem.edu/offices/board-regents/regents-rules-and-regulations>) and the policies of The University of Texas System (<http://www.utsystem.edu/board-of-regents/policy-library>) (collectively, **University Rules**). Contractor represents and warrants that neither Contractor nor any firm, corporation or institution represented by Contractor, or anyone acting for the firm, corporation or institution, (1) has violated the antitrust laws of the State of Texas, [Chapter 15, Texas Business and Commerce Code](#), or federal antitrust laws, or (2) has communicated directly or indirectly the content of Contractor's response to University's procurement solicitation to any competitor or any other person engaged in a similar line of business during the procurement process for this Agreement.
- 4.2 Contractor represents and warrants that (a) it will use commercially reasonable efforts to perform Work in a good and workmanlike manner and in accordance with commercially reasonable standards of Contractor's profession or business, and (b) all Work to be performed will be of the quality that prevails among similar businesses engaged in providing similar services in major United States urban areas under the same or similar circumstances.

- 4.3 Contractor will call to University's attention in writing all information in any materials supplied to Contractor (by University or any other party) that Contractor regards as unsuitable, improper or inaccurate in connection with the purposes for which the material is furnished.
- 4.4 University at all times is relying on Contractor's skill and knowledge in performing Work. Contractor represents and warrants that Work will be accurate and free from any material defects. Contractor's duties and obligations under this Agreement will not be in any way diminished by reason of any approval by University. Contractor will not be released from any liability by reason of any approval by University.
- 4.5 Contractor will, at its own cost, correct all material defects in Work as soon as practical after Contractor becomes aware of the defects. If Contractor fails to correct material defects in Work within a reasonable time, then University may correct the defective Work at Contractor's expense. This remedy is in addition to, and not in substitution for, any other remedy for defective Work that University may have at law or in equity.
- 4.6 Contractor will maintain a staff of properly trained and experienced personnel to ensure satisfactory performance under this Agreement. Contractor will cause all persons connected with Contractor directly in charge of Work to be duly registered and licensed under all Applicable Laws. Contractor will assign to the Project a designated representative who will be responsible for administration and coordination of Work. Contractor will furnish efficient business administration and coordination and perform Work in an expeditious and economical manner consistent with the interests of University.
- 4.7 Contractor represents and warrants it is duly organized, validly existing and in good standing under the laws of the state of its organization; it is duly authorized and in good standing to conduct business in the State of Texas; it has all necessary power and has received all necessary approvals to execute and deliver this Agreement; and the individual executing this Agreement on behalf of Contractor has been duly authorized to act for and bind Contractor.
- 4.8 Contractor represents and warrants that neither the execution and delivery of this Agreement by Contractor nor the performance of its duties and obligations under this Agreement will (a) result in the violation of any provision of its organizational documents; (b) result in the violation of any provision of any agreement by which it is bound; or (c) conflict with any order or decree of any court or other body or authority having jurisdiction.
- 4.9 Contractor represents and warrants that all of Contractor's Personnel contributing to Work Material (ref. **Section 7**) under this Agreement will be required to (i) acknowledge in writing the ownership of Contractor (for the benefit of University) of Work Material produced by Personnel while performing services pursuant to this Agreement, and (ii) make all assignments necessary to effectuate such ownership. **Personnel** means any and all persons associated with Contractor who provide any work or work product pursuant to this Agreement, including officers, managers, supervisors, full-time employees, part-time employees, and independent contractors.
- 4.10 Contractor represents and warrants that: (i) Work will be performed solely by Contractor, its full-time or part-time employees during the course of their employment, or independent contractors who have assigned in writing all right, title and interest in their work to Contractor (for the benefit of University); (ii) University will receive free, good and clear title to all Work Material developed under this Agreement; (iii) Work Material and the intellectual property rights protecting Work Material are free and clear of all encumbrances, including security interests, licenses, liens, charges and other restrictions; (iv) Work Material will not infringe upon or violate any patent, copyright, trade secret, trademark, service mark or other property right of any former employer, independent contractor, client or other third party; and (v) the

use, reproduction, distribution, or modification of Work Material will not violate the rights of any third parties in Work Material, including trade secret, publicity, privacy, copyright, trademark, service mark and patent rights.

5. **The Contract Amount.**

- 5.1 University will pay Contractor for the performance of Work in accordance with **Exhibit C**, Payment for Services.
- 5.2 The Contract Amount includes all applicable federal, state or local sales or use taxes payable as a result of the execution or performance of this Agreement.
- 5.3 University (a State agency) is exempt from Texas Sales & Use Tax on Work in accordance with [§151.309, Texas Tax Code](#) and [34 Texas Administrative Code \(TAC\) §3.322](#). Pursuant to 34 TAC §§3.322(c)(4) and (g)(3), this Agreement is sufficient proof of University's tax exempt status and University is not required to provide further evidence of its exempt status.

6. **Payment Terms.**

- 6.1 At least ten (10) days before the end of each month during the Term, Contractor will submit to University an invoice covering Work performed for University to that date, in compliance with **Exhibit C**, Payment for Services. Each invoice will be accompanied by documentation that University may reasonably request to support the invoice amount.
- 6.2 Within ten (10) days after final completion and acceptance of Work by University or as soon thereafter as possible, Contractor will submit a final invoice (**Final Invoice**) setting forth all amounts due and remaining unpaid to Contractor. Upon approval of the Final Invoice by University, University will pay (**Final Payment**) to Contractor the amount due under the Final Invoice.
- 6.3 Notwithstanding any provision of this Agreement to the contrary, University will not be obligated to make any payment (whether a Progress Payment or Final Payment) to Contractor if Contractor is in default under this Agreement.
- 6.4 The cumulative amount of all Progress Payments and the Final Payment (defined below) will not exceed the Contract Amount in **Exhibit C**, Payment for Services.
- 6.5 No payment made by University will (a) be construed to be final acceptance or approval of that part of the Work to which the payment relates, or (b) relieve Contractor of any of its duties or obligations under this Agreement.
- 6.6 The acceptance of Final Payment by Contractor will constitute a waiver of all claims by Contractor except those previously made in writing and identified by Contractor as unsettled at the time of the Final Invoice for payment.
- 6.7 University will have the right to verify the details in Contractor's invoices and supporting documentation, either before or after payment, by (a) inspecting the books and records of Contractor at mutually convenient times; (b) examining any reports with respect to the Project; and (c) other reasonable action.
- 6.8 [Section 51.012, Texas Education Code](#), authorizes University to make payments through electronic funds transfer methods. Contractor agrees to accept payments from University through those methods, including the automated clearing house system (ACH). Contractor agrees to provide Contractor's banking information to University in writing on Contractor

letterhead signed by an authorized representative of Contractor. Prior to the first payment, University will confirm Contractor's banking information. Changes to Contractor's bank information must be communicated to University in accordance with **Section 12.14** in writing at least thirty (30) days before the effective date of the change and must include an [IRS Form W-9](#) signed by an authorized representative of Contractor.

- 6.9 **[Option (Include if University is entitled to a prompt payment discount.):** Notwithstanding any other provision of this Agreement, University is entitled to a discount of % (**Prompt Payment Discount**) off of each payment that University submits within days after University's receipt of Contractor's invoice for that payment.]

7. Ownership and Use of Work Material.

- 7.1 All tools, software, programs drawings, specifications, plans, computations, sketches, data, photographs, tapes, renderings, models, publications, statements, accounts, reports, studies, and other materials prepared by Contractor or any subcontractors in connection with the Work (collectively, "**Work Material**"), whether or not accepted or rejected by University, are the sole property of University and for its exclusive use and re-use at any time without further compensation and without any restrictions.
- 7.2 Contractor grants and assigns to University all rights and claims of whatever nature and whether now or hereafter arising in and to the Work Material and will cooperate fully with University in any steps University may take to obtain or enforce patent, copyright, trademark or like protections with respect to the Work Material.
- 7.3 Contractor will deliver all Work Material to University upon expiration or termination of this Agreement. University will have the right to use the Work Material for the completion of the Work or otherwise. University may, at all times, retain the originals of the Work Material. The Work Material will not be used by any person other than University on other projects unless expressly authorized by University in writing.
- 7.4 The Work Material will not be used or published by Contractor or any other party unless expressly authorized by University in writing. Contractor will treat all Work Material as confidential.
- 7.5 All title and interest in the Work Material will vest in University and will be deemed to be a work made for hire and made in the course of the Work rendered under this Agreement. To the extent that title to any Work Material may not, by operation of law, vest in University or Work Material may not be considered works made for hire, Contractor hereby irrevocably assigns, conveys and transfers to University and its successors, licensees and assigns, all rights, title and interest worldwide in and to the Work Material and all proprietary rights therein, including all copyrights, trademarks, service marks, patents, trade secrets, moral rights, all contract and licensing rights and all claims and causes of action with respect to any of the foregoing, whether now known or hereafter to become known. In the event Contractor has any rights in the Work Material which cannot be assigned, Contractor agrees to waive enforcement worldwide of the rights against University, its successors, licensees, assigns, distributors and customers or, if necessary, to exclusively license the rights, worldwide to University with the right to sublicense. These rights are assignable by University.
- 7.6 "**Contractor IP**" means, collectively, all tools software and/or programs owned by Contractor, or which have been licensed to Contractor by a third party that either: 1) existed prior to the effective date of this Agreement and the commencement of Work; 2) are not related to the Work or to Contractor's services in connection with the Work; or 3) were created by the Contractor (or its licensor) totally separate from the Work or Contractor's services in connection with the Work. Contractor IP is the sole property of Contractor (or its licensor)

and Contractor (or its licensor) will at all times retain sole and exclusive title to and ownership to Contractor IP. Contractor hereby grants to University a non-exclusive, worldwide, perpetual, irrevocable, sub-licensable, royalty-free license to use the Contractor IP in connection with the Work and with Contractor's services in connection with the Work.

- 7.7 To the extent that particular Work Product comprises an improvement, enhancement or modification to preexisting Contractor IP, *whether or not patentable, copyrightable as a derivative work, or otherwise protectable as intellectual property* (hereafter "**Work Product Improvements to Contractor IP**"), University grants to Contractor a non-exclusive, worldwide, perpetual, irrevocable, sub-licensable, royalty-free license to the Work Product Improvements to Contractor IP

8. Default and Termination

- 8.1 In the event of a material failure by a party to this Agreement to perform in accordance with its terms (**default**), the other party may terminate this Agreement upon fifteen (15) days' written notice of termination setting forth the nature of the material failure; provided, that, the material failure is through no fault of the terminating party. The termination will not be effective if the material failure is fully cured prior to the end of the fifteen-day (15-day) period.
- 8.2 University may, without cause, terminate this Agreement at any time upon giving seven (7) days' advance written notice to Contractor. Upon termination pursuant to this Section, Contractor will be entitled to payment of an amount that will compensate Contractor for Work satisfactorily performed from the time of the last payment date to the termination date in accordance with this Agreement; provided, that, Contractor has delivered all Work Material to University. Notwithstanding any provision in this Agreement to the contrary, University will not be required to pay or reimburse Contractor for any services performed or for expenses incurred by Contractor after the date of the termination notice, that could have been avoided or mitigated by Contractor.
- 8.3 Termination under **Sections 8.1** or **8.2** will not relieve Contractor from liability for any default or breach under this Agreement or any other act or omission of Contractor.
- 8.4 If Contractor fails to cure any default within fifteen (15) days after receiving written notice of the default, University will be entitled (but will not be obligated) to cure the default and will have the right to offset against all amounts due to Contractor under this Agreement, any and all reasonable expenses incurred in connection with University's curative actions.
- 8.5 In the event that this Agreement is terminated, then within thirty (30) days after termination, Contractor will reimburse University for all fees paid by University to Contractor that were (a) not earned by Contractor prior to termination, or (b) for goods or services that University did not receive from Contractor prior to termination.

9. Indemnification

9.1 TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS, CONTRACTOR WILL AND DOES HEREBY AGREE TO INDEMNIFY, PROTECT, DEFEND WITH COUNSEL APPROVED BY UNIVERSITY, AND HOLD HARMLESS UNIVERSITY AND ITS RESPECTIVE AFFILIATED ENTERPRISES, REGENTS, OFFICERS, DIRECTORS, ATTORNEYS, EMPLOYEES, REPRESENTATIVES AND AGENTS (COLLECTIVELY, **INDEMNITEES**) FROM AND AGAINST ALL DAMAGES, LOSSES, LIENS, CAUSES OF ACTION, SUITS, JUDGMENTS, EXPENSES, AND OTHER CLAIMS OF ANY NATURE, KIND, OR DESCRIPTION, INCLUDING REASONABLE ATTORNEYS' FEES INCURRED IN INVESTIGATING, DEFENDING OR SETTLING ANY OF THE FOREGOING (COLLECTIVELY, **CLAIMS**) BY ANY PERSON OR ENTITY, ARISING OUT OF, CAUSED BY, OR RESULTING FROM CONTRACTOR'S PERFORMANCE UNDER OR BREACH OF THIS AGREEMENT AND THAT ARE CAUSED IN WHOLE OR IN PART BY ANY NEGLIGENT ACT, NEGLIGENT OMISSION OR WILLFUL MISCONDUCT OF CONTRACTOR, ANYONE DIRECTLY EMPLOYED BY CONTRACTOR OR ANYONE FOR WHOSE ACTS CONTRACTOR MAY BE LIABLE. THE PROVISIONS OF THIS SECTION WILL NOT BE CONSTRUED TO ELIMINATE OR REDUCE ANY OTHER INDEMNIFICATION OR RIGHT WHICH ANY INDEMNITEE HAS BY LAW OR EQUITY. ALL PARTIES WILL BE ENTITLED TO BE REPRESENTED BY COUNSEL AT THEIR OWN EXPENSE.

9.2 IN ADDITION, CONTRACTOR WILL AND DOES HEREBY AGREE TO INDEMNIFY, PROTECT, DEFEND WITH COUNSEL APPROVED BY UNIVERSITY, AND HOLD HARMLESS INDEMNITEES FROM AND AGAINST ALL CLAIMS ARISING FROM INFRINGEMENT OR ALLEGED INFRINGEMENT OF ANY PATENT, COPYRIGHT, TRADEMARK OR OTHER PROPRIETARY INTEREST ARISING BY OR OUT OF THE PERFORMANCE OF SERVICES OR THE PROVISION OF GOODS BY CONTRACTOR, OR THE USE BY INDEMNITEES, AT THE DIRECTION OF CONTRACTOR, OF ANY ARTICLE OR MATERIAL; PROVIDED, THAT, UPON BECOMING AWARE OF A SUIT OR THREAT OF SUIT FOR INFRINGEMENT, UNIVERSITY WILL PROMPTLY NOTIFY CONTRACTOR AND CONTRACTOR WILL BE GIVEN THE OPPORTUNITY TO NEGOTIATE A SETTLEMENT. IN THE EVENT OF LITIGATION, UNIVERSITY AGREES TO REASONABLY COOPERATE WITH CONTRACTOR. ALL PARTIES WILL BE ENTITLED TO BE REPRESENTED BY COUNSEL AT THEIR OWN EXPENSE.

10. Relationship of the Parties.

For all purposes of this Agreement and notwithstanding any provision of this Agreement to the contrary, Contractor is an independent contractor and is not a state employee, partner, joint venturer, or agent of University. Contractor will not bind nor attempt to bind University to any agreement or contract. As an independent contractor, Contractor is solely responsible for all taxes, withholdings, and other statutory or contractual obligations of any sort, including workers' compensation insurance.

11. Insurance.

11.1 Contractor, consistent with its status as an independent contractor will carry and will cause its subcontractors to carry, at least the following insurance, with companies authorized to do insurance business in the State of Texas or eligible surplus lines insurers operating in accordance with the [Texas Insurance Code](#), having an A.M. Best Rating of A-:VII or better, and in amounts not less than the following minimum limits of coverage:

11.1.1 Workers' Compensation Insurance with statutory limits, and Employer's Liability Insurance with limits of not less than \$1,000,000:

Employers Liability - Each Accident	\$1,000,000
Employers Liability - Each Employee	\$1,000,000
Employers Liability - Policy Limit	\$1,000,000

Workers' Compensation policy must include under Item 3.A. on the information page of the Workers' Compensation policy the state in which Work is to be performed for University.

11.1.2 Commercial General Liability Insurance with limits of not less than:

Each Occurrence Limit	\$1,000,000
Damage to Rented Premises	\$ 300,000
Personal & Advertising Injury	\$1,000,000
General Aggregate	\$2,000,000
Products - Completed Operations Aggregate	\$2,000,000

The required Commercial General Liability policy will be issued on a form that insures Contractor's and subcontractor's liability for bodily injury (including death), property damage, personal, and advertising injury assumed under the terms of this Agreement.

11.1.3 Business Auto Liability Insurance covering all owned, non-owned or hired automobiles, with limits of not less than \$1,000,000 single limit of liability per accident for Bodily Injury and Property Damage;

If a separate Business Auto Liability policy is not available, coverage for hired and non-owned auto liability may be endorsed on the Commercial General Liability policy.

11.1.4 Umbrella/Excess Liability Insurance with limits of not less than \$2,000,000 per occurrence and aggregate with a deductible of no more than \$10,000. The Umbrella/Excess Liability policy will be excess over and at least as broad as the underlying coverage as required under sections 11.1.1 Employer's Liability; 11.1.2 Commercial General Liability; and 11.1.3 Business Auto Liability. Inception and expiration dates will be the same as the underlying policies. Drop down coverage will be provided for reduction or exhaustion of underlying aggregate limits and will provide a duty to defend for any insured.

11.1.5 Professional Liability (Errors & Omissions) Insurance with limits of not less than \$1,000,000 each occurrence, \$3,000,000 aggregate. Such insurance will cover all Work performed by or on behalf of Contractor and its subcontractors under this Agreement. Renewal policies written on a claims-made basis will maintain the same retroactive date as in effect at the inception of this Agreement. If coverage is written on a claims-made basis, Contractor agrees to purchase an Extended Reporting Period Endorsement, effective twenty-four (24) months after the expiration or cancellation of the policy. No Professional Liability policy written on an occurrence form will include a sunset or similar clause that limits coverage unless such clause provides coverage for at least twenty-four (24) months after the expiration or termination of this Agreement for any reason.

11.1.6 Cyber Liability Insurance with limits of not less than \$10,000,000 for each wrongful act. This policy must cover:

- Liability for network security failures or privacy breaches, including loss or unauthorized access, use or disclosure of University data, whether by Contractor or any of subcontractor or cloud service provider used by Contractor;
- Costs associated with a privacy breach, including notification of affected individuals, customer support, forensics, crises management / public relations

consulting, legal services of a privacy attorney, credit monitoring and identity fraud resolution services for affected individuals;

- Expenses related to regulatory compliance, government investigations, fines, fees assessments and penalties;
- Liability for technological products and services;
- PCI fines, fees, penalties and assessments;
- Cyber extortion payment and response costs;
- First and Third Party Business Interruption Loss resulting from a network security failure;
- Liability for technological products and services;
- Costs of restoring, updating or replacing data; and
- Liability losses connected to network security, privacy, and media liability.

If this policy is written on a claims-made basis, (a) the “retroactive date” must be prior to the commencement of Work under this Agreement; and (b) if this policy is cancelled, terminated or non-renewed at any time during the Term, Contractor will purchase an “extended reporting period” for at least.

11.2 Contractor will deliver to University:

11.2.1 After the execution and delivery of this Agreement and prior to the performance of any Work by Contractor, evidence of insurance on a Texas Department of Insurance (TDI) approved certificate form (the Acord form is a TDI-approved form) verifying the existence and actual limits of all required insurance policies; and, if the coverage period shown on the current certificate form ends during the Term, then prior to the end of the coverage period, a new certificate form verifying the continued existence of all required insurance policies.

11.2.1.1 **All insurance policies** (with the exception of workers’ compensation, employer’s liability and professional liability) will be endorsed and name the Board of Regents of The University of Texas System and University as Additional Insureds for liability caused in whole or in part by Contractor’s acts or omissions with respect to its on-going and completed operations up to the actual liability limits of the required insurance policies maintained by Contractor. Commercial General Liability Additional Insured endorsement including ongoing and completed operations coverage will be submitted with the Certificates of Insurance. Commercial General Liability and Business Auto Liability will be endorsed to provide primary and non-contributory coverage.

11.2.1.2 Contractor hereby waives all rights of subrogation against the Board of Regents of The University of Texas System and University. **All insurance policies** will be endorsed to provide a waiver of subrogation in favor of the Board of Regents of The University of Texas System and University. No policy will be canceled until after thirty (30) days’ unconditional written notice to University. **All insurance policies** will be endorsed to require the insurance carrier providing coverage to send notice to University thirty (30) days prior to any cancellation, material change, or non-renewal relating to any insurance policy required in this **Section 11**.

11.2.1.3 Contractor will pay any deductible or self-insured retention for any loss. Any self-insured retention must be declared to and approved by University prior to the performance of any Work by Contractor under this

Agreement. All deductibles and self-insured retentions will be shown on the Certificates of Insurance.

11.2.1.4 Certificates of Insurance and Additional Insured Endorsements as required by this Agreement will be mailed, faxed, or emailed to the following University contact:

Name:
Address:
Facsimile Number:
Email Address:

11.3 Contractor's or subcontractor's insurance will be primary to any insurance carried or self-insurance program established by University. Contractor's or subcontractor's insurance will be kept in force until all Work has been fully performed and accepted by University in writing.

11.3.1 Professional Liability Insurance coverage written on a claims-made basis requires Contractor to purchase an Extended Reporting Period Endorsement, effective for twenty-four (24) months after the expiration or cancellation of the policy.

12. Miscellaneous.

- 12.1 **Assignment and Subcontracting.** Except as specifically provided in **Exhibit D**, Historically Underutilized Business Subcontracting Plan, Contractor's interest in this Agreement (including Contractor's duties and obligations under this Agreement, and the fees due to Contractor under this Agreement) may not be subcontracted, assigned, delegated, or otherwise transferred to a third party, in whole or in part, and any attempt to do so will (a) not be binding on University; and (b) be a breach of this Agreement for which Contractor will be subject to all remedial actions provided by Applicable Laws, including [Chapter 2161, Texas Government Code](#), and [34 TAC §§20.285\(g\)\(5\), 20.585 and 20.586](#). The benefits and burdens of this Agreement are assignable by University.
- 12.2 **Texas Family Code Child Support Certification.** Pursuant to [§231.006, Texas Family Code](#), Contractor certifies it is not ineligible to receive the award of or payments under this Agreement, and acknowledges this Agreement may be terminated and payment withheld if this certification is inaccurate.
- 12.3 **Tax Certification.** If Contractor is a taxable entity as defined by [Chapter 171, Texas Tax Code](#), then Contractor certifies it is not currently delinquent in the payment of any taxes due under Chapter 171, Contractor is exempt from the payment of those taxes, or Contractor is an out-of-state taxable entity that is not subject to those taxes, whichever is applicable.
- 12.4 **Payment of Debt or Delinquency to the State.** Pursuant to [§§2107.008 and 2252.903, Texas Government Code](#), Contractor agrees any payments owing to Contractor under this Agreement may be applied directly toward any debt or delinquency Contractor owes the State of Texas or any agency of the State of Texas, regardless of when it arises, until paid in full.
- 12.5 **Loss of Funding.** Performance by University under this Agreement may be dependent upon the appropriation and allotment of funds by the Texas State Legislature (**Legislature**) and/or allocation of funds by the Board of Regents of The University of Texas System (**Board**). If Legislature fails to appropriate or allot necessary funds, or Board fails to allocate necessary funds, then University will issue written notice to Contractor and University may

terminate this Agreement without further duty or obligation. Contractor acknowledges that appropriation, allotment, and allocation of funds are beyond University's control.

- 12.6 **Entire Agreement; Modifications.** This Agreement (including all exhibits, schedules, supplements and other attachments (collectively, **Exhibits**)) supersedes all prior agreements, written or oral, between Contractor and University and will constitute the entire agreement and understanding between the parties with respect to its subject matter. This Agreement and each of its provisions will be binding upon the parties, and may not be waived, modified, amended or altered, except by a writing signed by University and Contractor. All Exhibits are attached to this Agreement and incorporated for all purposes.
- 12.7 **Force Majeure.** Neither party hereto will be liable or responsible to the other for any loss or damage or for any delays or failure to perform due to causes beyond its reasonable control including acts of God, strikes, epidemics, war, riots, flood, fire, sabotage, or any other circumstances of like character (**force majeure occurrence**). Provided, however, in the event of a force majeure occurrence, Contractor agrees to use its best efforts to mitigate the impact of the occurrence so that University may continue to provide during the occurrence.
- 12.8 **Captions.** The captions of sections and subsections in this Agreement are for convenience only and will not be considered or referred to in resolving questions of interpretation or construction.
- 12.9 **Venue; Governing Law.** Travis County, Texas, will be the proper place of venue for suit on or in respect of this Agreement. This Agreement, all of its terms and conditions, all rights and obligations of the parties, and all claims arising out of or relating to this Agreement, will be construed, interpreted and applied in accordance with, governed by and enforced under, the laws of the State of Texas.
- 12.10 **Waivers.** No delay or omission in exercising any right accruing upon a default in performance of this Agreement will impair any right or be construed to be a waiver of any right. A waiver of any default under this Agreement will not be construed to be a waiver of any subsequent default under this Agreement.
- 12.11 **Confidentiality and Safeguarding of University Records; Press Releases; Public Information.** Under this Agreement, Contractor may (1) create, (2) receive from or on behalf of University, or (3) have access to, records or record systems (collectively, **University Records**). However, it is expressly agreed that University will not provide to Contractor, and Contractor will never seek to access, any University Records that contain personally identifiable information regarding any individual that is not available to any requestor under the *Texas Public Information Act*, [Chapter 552, Texas Government Code](#), including "directory information" of any student who has opted to prohibit the release of their "directory information" as that term is defined under the *Family Educational Rights and Privacy Act*, [20 USC §1232g \(FERPA\)](#) and its implementing regulations. Contractor represents, warrants, and agrees that it will: (1) hold University Records in strict confidence and will not use or disclose University Records except as (a) permitted or required by this Agreement, (b) required by Applicable Laws, or (c) otherwise authorized by University in writing; (2) safeguard University Records according to reasonable administrative, physical and technical standards (such as standards established by the National Institute of Standards and Technology and the Center for Internet Security, as well as the Payment Card Industry Data Security Standards) that are no less rigorous than the standards by which Contractor protects its own confidential information; (3) continually monitor its operations and take any action necessary to assure that University Records are safeguarded and the confidentiality of University Records is maintained in accordance with all Applicable Laws and the terms of this Agreement; and (4) comply with University Rules regarding access to and use of University's computer systems, including UTS 165 at

<http://www.utsystem.edu/board-of-regents/policy-library/policies/uts165-information-resources-use-and-security-policy>. At the request of University, Contractor agrees to provide University with a written summary of the procedures Contractor uses to safeguard and maintain the confidentiality of University Records.

- 12.11.1 **Notice of Impermissible Use.** If an impermissible use or disclosure of any University Records occurs, Contractor will provide written notice to University within one (1) business day after Contractor's discovery of that use or disclosure. Contractor will promptly provide University with all information requested by University regarding the impermissible use or disclosure.
- 12.11.2 **Return of University Records.** Contractor agrees that within thirty (30) days after the expiration or termination of this Agreement, for any reason, all University Records created or received from or on behalf of University will be (1) returned to University, with no copies retained by Contractor; or (2) if return is not feasible, destroyed. Twenty (20) days before destruction of any University Records, Contractor will provide University with written notice of Contractor's intent to destroy University Records. Within five (5) days after destruction, Contractor will confirm to University in writing the destruction of University Records.
- 12.11.3 **Disclosure.** If Contractor discloses any University Records to a subcontractor or agent, Contractor will require the subcontractor or agent to comply with the same restrictions and obligations as are imposed on Contractor by this **Section 12.11**.
- 12.11.4 **Press Releases.** Except when defined as part of Work, Contractor will not make any press releases, public statements, or advertisement referring to the Project or the engagement of Contractor as an independent contractor of University in connection with the Project, or release any information relative to the Project for publication, advertisement or any other purpose without the prior written approval of University.
- 12.11.5 **Public Information.** University strictly adheres to all statutes, court decisions and the opinions of the Texas Attorney General with respect to disclosure of public information under the *Texas Public Information Act (TPIA)*, [Chapter 552, Texas Government Code](#). In accordance with §§[552.002](#) and [2252.907](#), *Texas Government Code*, and at no additional charge to University, Contractor will make any information created or exchanged with University pursuant to this Agreement (and not otherwise exempt from disclosure under TPIA) available in a format reasonably requested by University that is accessible by the public.
- 12.11.6 **Termination.** In addition to any other termination rights in this Agreement and any other rights at law or equity, if University reasonably determines that Contractor has breached any of the restrictions or obligations in this Section, University may immediately terminate this Agreement without notice or opportunity to cure.
- 12.11.7 **Duration.** The restrictions and obligations under this Section will survive expiration or termination of this Agreement for any reason.
- 12.12 **Binding Effect.** This Agreement will be binding upon and inure to the benefit of the parties hereto and their respective permitted assigns and successors.
- 12.13 **Records.** Records of Contractor's costs, reimbursable expenses pertaining to the Project and payments will be available to University or its authorized representative during business hours and will be retained for four (4) years after final Payment or abandonment of the Project, unless University otherwise instructs Contractor in writing.

12.14 **Notices.** Except as otherwise provided by this Section, notices, consents, approvals, demands, requests or other communications required or permitted under this Agreement, will be in writing and sent via certified mail, hand delivery, overnight courier, facsimile transmission (to the extent a facsimile number is provided below), or email (to the extent an email address is provided below) as indicated below, and notice will be deemed given (i) if delivered by certified mail, when deposited, postage prepaid, in the United States mail, or (ii) if delivered by hand, overnight courier, facsimile (to the extent a facsimile number is provided below) or email (to the extent an email address is provided below), when received:

If to University: _____

Fax: _____
Email: _____
Attention: _____

with copy to: _____

Fax: _____
Email: _____
Attention: _____

If to Contractor: _____

Fax: _____
Email: _____
Attention: _____

or other person or address as may be given in writing by either party to the other in accordance with this Section.

12.15 **Severability.** In case any provision of this Agreement will, for any reason, be held invalid or unenforceable in any respect, the invalidity or unenforceability will not affect any other provision of this Agreement, and this Agreement will be construed as if the invalid or unenforceable provision had not been included.

12.16 **State Auditor's Office.** Contractor understands acceptance of funds under this Agreement constitutes acceptance of authority of the Texas State Auditor's Office or any successor agency (**Auditor**), to conduct an audit or investigation in connection with those funds (ref. §§[51.9335\(c\)](#), [73.115\(c\)](#) and [74.008\(c\)](#), *Texas Education Code*). Contractor agrees to cooperate with Auditor in the conduct of the audit or investigation, including providing all records requested. Contractor will include this provision in all contracts with permitted subcontractors.

12.17 **Limitation of Liability.** EXCEPT FOR UNIVERSITY'S OBLIGATION (IF ANY) TO PAY CONTRACTOR CERTAIN FEES AND EXPENSES UNIVERSITY WILL HAVE NO LIABILITY TO CONTRACTOR OR TO ANYONE CLAIMING THROUGH OR UNDER CONTRACTOR BY REASON OF THE EXECUTION OR PERFORMANCE OF THIS AGREEMENT. NOTWITHSTANDING ANY DUTY OR OBLIGATION OF UNIVERSITY TO CONTRACTOR OR TO ANYONE CLAIMING THROUGH OR UNDER CONTRACTOR, NO PRESENT OR FUTURE AFFILIATED ENTERPRISE, SUBCONTRACTOR, AGENT, OFFICER, DIRECTOR, EMPLOYEE, REPRESENTATIVE,

ATTORNEY OR REGENT OF UNIVERSITY, OR THE UNIVERSITY OF TEXAS SYSTEM, OR ANYONE CLAIMING UNDER UNIVERSITY HAS OR WILL HAVE ANY PERSONAL LIABILITY TO CONTRACTOR OR TO ANYONE CLAIMING THROUGH OR UNDER CONTRACTOR BY REASON OF THE EXECUTION OR PERFORMANCE OF THIS AGREEMENT.

12.18 **Survival of Provisions.** No expiration or termination of this Agreement will relieve either party of any obligations under this Agreement that by their nature survive expiration or termination, including **Sections 6.7, 9, 12.5, 12.9, 12.10, 12.11, 12.13, 12.16, 12.17, 12.19** and **12.21**.

12.19 **Breach of Contract Claims.**

12.19.1 To the extent that [Chapter 2260, Texas Government Code](#), as it may be amended from time to time (**Chapter 2260**), is applicable to this Agreement and is not preempted by other Applicable Laws, the dispute resolution process provided for in [Chapter 2260](#) will be used, as further described herein, by University and Contractor to attempt to resolve any claim for breach of contract made by Contractor:

12.19.1.1 Contractor's claims for breach of this Agreement that the parties cannot resolve pursuant to other provisions of this Agreement or in the ordinary course of business will be submitted to the negotiation process provided in [subchapter B](#) of Chapter 2260. To initiate the process, Contractor will submit written notice, as required by [subchapter B](#) of Chapter 2260, to University in accordance with the notice provisions in this Agreement. Contractor's notice will specifically state that the provisions of [subchapter B](#) of Chapter 2260 are being invoked, the date and nature of the event giving rise to the claim, the specific contract provision that University allegedly breached, the amount of damages Contractor seeks, and the method used to calculate the damages. Compliance by Contractor with [subchapter B](#) of Chapter 2260 is a required prerequisite to Contractor's filing of a contested case proceeding under [subchapter C](#) of Chapter 2260. The chief business officer of University, or another officer of University as may be designated from time to time by University by written notice to Contractor in accordance with the notice provisions in this Agreement, will examine Contractor's claim and any counterclaim and negotiate with Contractor in an effort to resolve the claims.

12.19.1.2 If the parties are unable to resolve their disputes under **Section 12.19.1.1**, the contested case process provided in [subchapter C](#) of Chapter 2260 is Contractor's sole and exclusive process for seeking a remedy for any and all of Contractor's claims for breach of this Agreement by University.

12.19.1.3 Compliance with the contested case process provided in [subchapter C](#) of Chapter 2260 is a required prerequisite to seeking consent to sue from the Legislature under [Chapter 107, Texas Civil Practices and Remedies Code](#). The parties hereto specifically agree that (i) neither the execution of this Agreement by University nor any other conduct, action or inaction of any representative of University relating to this Agreement constitutes or is intended to constitute a waiver of University's or the state's

sovereign immunity to suit and (ii) University has not waived its right to seek redress in the courts.

- 12.19.2 The submission, processing and resolution of Contractor's claim is governed by the published rules adopted by the Texas Attorney General pursuant to [Chapter 2260](#), as currently effective, thereafter enacted or subsequently amended.
- 12.19.3 University and Contractor agree that any periods provided in this Agreement for notice and cure of defaults are not waived.
- 12.20 **Undocumented Workers.** The *Immigration and Nationality Act* ([8 USC §1324a](#)) (**Immigration Act**) makes it unlawful for an employer to hire or continue employment of undocumented workers. The United States Immigration and Customs Enforcement Service has established the [Form I-9 Employment Eligibility Verification Form \(I-9 Form\)](#) as the document to be used for employment eligibility verification ([8 CFR §274a](#)). Among other things, Contractor is required to: (1) have all employees complete and sign the I-9 Form certifying that they are eligible for employment; (2) examine verification documents required by the I-9 Form to be presented by the employee and ensure the documents appear to be genuine and related to the individual; (3) record information about the documents on the I-9 Form, and complete the certification portion of the I-9 Form; and (4) retain the I-9 Form as required by Applicable Laws. It is illegal to discriminate against any individual (other than a citizen of another country who is not authorized to work in the United States) in hiring, discharging, or recruiting because of that individual's national origin or citizenship status. If Contractor employs unauthorized workers during performance of this Agreement in violation of the Immigration Act then, in addition to other remedies or penalties prescribed by Applicable Laws, University may terminate this Agreement in accordance with **Section 8**. Contractor represents and warrants that it is in compliance with and agrees that it will remain in compliance with the provisions of the Immigration Act.
- 12.21 **Limitations.** THE PARTIES ARE AWARE THERE ARE CONSTITUTIONAL AND STATUTORY LIMITATIONS (**LIMITATIONS**) ON THE AUTHORITY OF UNIVERSITY (A STATE AGENCY) TO ENTER INTO CERTAIN TERMS AND CONDITIONS THAT MAY BE PART OF THIS AGREEMENT, INCLUDING TERMS AND CONDITIONS RELATING TO LIENS ON UNIVERSITY'S PROPERTY; DISCLAIMERS AND LIMITATIONS OF WARRANTIES; DISCLAIMERS AND LIMITATIONS OF LIABILITY FOR DAMAGES; WAIVERS, DISCLAIMERS AND LIMITATIONS OF LEGAL RIGHTS, REMEDIES, REQUIREMENTS AND PROCESSES; LIMITATIONS OF PERIODS TO BRING LEGAL ACTION; GRANTING CONTROL OF LITIGATION OR SETTLEMENT TO ANOTHER PARTY; LIABILITY FOR ACTS OR OMISSIONS OF THIRD PARTIES; PAYMENT OF ATTORNEYS' FEES; DISPUTE RESOLUTION; INDEMNITIES; AND CONFIDENTIALITY, AND TERMS AND CONDITIONS RELATED TO LIMITATIONS WILL NOT BE BINDING ON UNIVERSITY EXCEPT TO THE EXTENT AUTHORIZED BY THE LAWS AND CONSTITUTION OF THE STATE OF TEXAS.
- 12.22 **Ethics Matters; No Financial Interest.** Contractor and its employees, agents, representatives and subcontractors have read and understand University's Conflicts of Interest Policy at <http://www.utsystem.edu/board-of-regents/policy-library/policies/int180-conflicts-interest-conflicts-commitment-and-outside->, University's Standards of Conduct Guide at <https://www.utsystem.edu/documents/docs/policies-rules/ut-system-administration-standards-conduct-guide>, and applicable state ethics laws and rules at <https://www.utsystem.edu/offices/systemwide-compliance/ethics>. Neither Contractor nor its employees, agents, representatives or subcontractors will assist or cause University employees to violate University's Conflicts of Interest Policy, University's Standards of Conduct Guide, or applicable state ethics laws or rules. Contractor represents and warrants that no member of the Board has a direct or indirect financial interest in the transaction that is the subject of this Agreement.

- 12.23. Contractor agrees and acknowledges that University is entering into this Agreement in reliance on Contractor's special and unique knowledge and abilities with respect to performing Work. Contractor's services provide a peculiar value to University. University cannot be reasonably or adequately compensated in damages for the loss of Contractor's services. Accordingly, Contractor acknowledges and agrees that a breach by Contractor of the provisions of this Agreement will cause University irreparable injury and damage. Contractor, therefore, expressly agrees that University will be entitled to injunctive and/or other equitable relief in any court of competent jurisdiction to prevent or otherwise restrain a breach of this Agreement.
- 12.24 **Access by Individuals with Disabilities.** Contractor represents and warrants (**EIR Accessibility Warranty**) the electronic and information resources and all associated information, documentation, and support Contractor provides to University under this Agreement (**EIRs**) comply with applicable requirements in [1 TAC Chapter 213](#) and [1 TAC §206.70](#) (ref. [Subchapter M, Chapter 2054, Texas Government Code](#)). To the extent Contractor becomes aware the EIRs, or any portion thereof, do not comply with the EIR Accessibility Warranty, then Contractor represents and warrants it will, at no cost to University, either (1) perform all necessary remediation to make the EIRs satisfy the EIR Accessibility Warranty or (2) replace the EIRs with new EIRs that satisfy the EIR Accessibility Warranty. If Contractor fails or is unable to do so, University may terminate this Agreement and, within thirty (30) days after termination, Contractor will refund to University all amounts University paid under this Agreement.
- 12.25 **Historically Underutilized Business Subcontracting Plan.** Contractor agrees to use good faith efforts to subcontract Work in accordance with the Historically Underutilized Business Subcontracting Plan (**HSP**) (ref. **Exhibit D**). Contractor agrees to maintain business records documenting its compliance with the HSP and to submit a monthly compliance report to University in the format required by the Statewide Procurement and Statewide Support Services Division of the Texas Comptroller of Public Accounts or successor entity (collectively, **SPSS**). Submission of compliance reports will be required as a condition for payment under this Agreement. If University determines that Contractor has failed to subcontract as set out in the HSP, University will notify Contractor of any deficiencies and give Contractor an opportunity to submit documentation and explain why the failure to comply with the HSP should not be attributed to a lack of good faith effort by Contractor. If University determines that Contractor failed to implement the HSP in good faith, University, in addition to any other remedies, may report nonperformance to the SPSS in accordance with [34 TAC §§20.285\(g\)\(5\)](#), [20.585](#) and [20.586](#). University may also revoke this Agreement for breach and make a claim against Contractor.
- 12.25.1 **Changes to the HSP.** If at any time during the Term, Contractor desires to change the HSP, before the proposed changes become effective (a) Contractor must comply with [34 TAC §20.285](#); (b) the changes must be reviewed and approved by University; and (c) if University approves changes to the HSP, this Agreement must be amended in accordance with **Section 12.6** to replace the HSP with the revised subcontracting plan.
- 12.25.2 **Expansion of Work.** If University expands the scope of Work through a change order or any other amendment, University will determine if the additional Work contains probable subcontracting opportunities *not* identified in the initial solicitation for Work. If University determines additional probable subcontracting opportunities exist, Contractor will submit an amended subcontracting plan covering those opportunities. The amended subcontracting plan must comply with the provisions of [34 TAC §20.285](#) before (a) this Agreement may be amended to include the additional Work; or (b) Contractor may perform the additional Work. If Contractor subcontracts any of the additional subcontracting opportunities identified by University without prior

authorization and without complying with [34 TAC §20.285](#), Contractor will be deemed to be in breach of this Agreement under **Section 8** and will be subject to any remedial actions provided by Applicable Laws, including [Chapter 2161, Texas Government Code](#), and [34 TAC §20.285](#). University may report nonperformance under this Agreement to the SPSS in accordance with [34 TAC §§20.285\(g\)\(5\), 20.585](#) and [20.586](#).

- 12.26 Each individual who is assigned to perform Work under this Agreement will be an employee of Contractor or an employee of a subcontractor engaged by Contractor. Contractor is responsible for the performance of all individuals performing Work under this Agreement. Prior to commencing Work, Contractor will (1) provide University with a list (**List**) of all individuals who may be assigned to perform Work on University's premises and (2) have an appropriate criminal background screening performed on all the individuals on the List. Contractor will determine on a case-by-case basis whether each individual assigned to perform Work is qualified to provide the services. Contractor will not knowingly assign any individual to provide services on University's premises who has a history of criminal conduct unacceptable for a university campus or healthcare center, including violent or sexual offenses. Contractor will update the List each time there is a change in the individuals assigned to perform Work on University's premises.

Prior to commencing performance of Work under this Agreement, Contractor will provide University a letter signed by an authorized representative of Contractor certifying compliance with this Section. Contractor will provide University an updated certification letter each time there is a change in the individuals on the List.

- 12.27 **External Terms.** This Agreement completely supplants, replaces, and overrides all other terms and conditions or agreements, written or oral, concerning Contractor's performance or provision of goods or services under this Agreement (**External Terms**). External Terms are null and void and will have no effect under this Agreement, even if University or its employees, contractors, or agents express assent or agreement to External Terms. External Terms include any shrinkwrap, clickwrap, browsewrap, web-based terms and conditions of use, and any other terms and conditions displayed in any format that University or its employees, contractors, or agents are required to accept or agree to before or in the course of accessing or using any goods or services provided by Contractor.
- 12.28 **Contractor Certification regarding Boycotting Israel.** Pursuant to [Chapter 2270, Texas Government Code](#), Contractor certifies Contractor (1) does not currently boycott Israel; and (2) will not boycott Israel during the Term of this Agreement. Contractor acknowledges this Agreement may be terminated and payment withheld if this certification is inaccurate.
- 12.29 **Contractor Certification regarding Business with Certain Countries and Organizations.** Pursuant to [Subchapter F, Chapter 2252, Texas Government Code](#), Contractor certifies Contractor is not engaged in business with Iran, Sudan, or a foreign terrorist organization. Contractor acknowledges this Agreement may be terminated and payment withheld if this certification is inaccurate.

University and Contractor have executed and delivered this Agreement to be effective as of the Effective Date.

UNIVERSITY:

CONTRACTOR:

THE UNIVERSITY OF TEXAS SYSTEM

By: _____
Name: _____
Title: _____

By: _____
Name: _____
Title: _____

Attach:

EXHIBIT A – Scope of Work

EXHIBIT B – Schedule

EXHIBIT C – Payment for Services

EXHIBIT D – HUB Subcontracting Plan

EXHIBIT A

SCOPE OF WORK

EXHIBIT B

SCHEDULE

(TO BE COMPLETED WHEN THE CONTRACTOR IS SELECTED)

EXHIBIT C

PAYMENT FOR SERVICES

(TO BE COMPLETED WHEN THE CONTRACTOR IS SELECTED)

SERVICE FEES:

Notwithstanding the foregoing, the cumulative amount of Service Fees remitted by University to Contractor will not exceed \$_____ (**Fee Cap**) without the prior written approval of University. In addition, total fees for each Phase of Work will not exceed the following specified amounts without the prior written approval of University:

If University submits, in advance, a written request for additional services not contemplated or reasonably inferred by this Agreement, Contractor will be paid for actual hours incurred by Contractor's personnel directly and solely in support of the additional services at the Rates provided above.

EXHIBIT D

HUB SUBCONTRACTING PLAN

(TO BE COMPLETED WHEN THE CONTRACTOR IS SELECTED)

Shared Assessments Introduction

Campus IT environments are rapidly changing and the speed of cloud service adoption is increasing. Institutions looking for ways to do more with less see cloud services as a good way to save resources. As campuses deploy or identify cloud services, they must ensure the cloud services are appropriately assessed for managing the risks to the confidentiality, integrity and availability of sensitive institutional information and the PII of constituents. Many campuses have established cloud security assessment methodology and resources to review cloud services for privacy and security controls. Other campuses don't have sufficient resources to assess their cloud services in this manner. On the vendor side, many cloud services providers spend significant time responding to the individualized security assessment requests made by campus customers, often answering the same questions repeatedly. Both the provider and consumer of cloud services are wasting precious resources creating, responding, and reviewing such assessments.

The Higher Education Cloud Vendor Assessment Tool attempts to generalize higher education information security and data protection questions and issues for consistency and ease of use. While all institutions may have specific issues that must be addressed in addition to the general questions provided in this assessment. It is anticipated that this Higher Education Cloud Vendor Assessment Tool will be revised over time to account for changes in cloud services provisioning and the information security and data protection needs of higher education institutions.

The Higher Education Cloud Vendor Assessment Tool:

- Helps higher education institutions ensure that cloud services are appropriately assessed for security and privacy needs, including some that are unique to higher education
- Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs of cloud services without increasing risks
- Reduces the burden that cloud service providers face in responding to requests for security assessments from higher education institutions

This Higher Education Cloud Vendor Assessment Tool was created by the Higher Education Information Security Council Shared Assessments Working Group. Its purpose is to provide a starting point for the assessment of third-party provided cloud services and resources. Over time the Shared Assessments Working Group hopes to create a framework that will establish a resource where institutions and cloud services providers will share completed Higher Education Cloud Vendor Assessment Tool assessments.

<https://www.educause.edu/hecvat>

<https://www.ren-isac.net/hecvat>

(C) EDUCAUSE 2016

This work is licensed under a Creative Commons Attribution-Noncommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).

This Higher Education Cloud Vendor Assessment Tool is brought to you by the Higher Education Information Security Council

Information Security Council, and members from EDUCAUSE, Internet2, and the Research Education Networking Information Sharing and Analysis Center (REN-ISAC).

d way to
d services
lability of
ished a
' and
rvices in
sponding to
ring similar
ious time

tion
use. Some
estions
essment
e

for

rough

ity

1
de a
ver time,
community
ation Cloud

.0

1

1 and



By completing the Higher Education Cloud Vendor Assessment Tool - Lite, that the completed assessment may be shared among higher education in uses, permissions, and audiences are defined in the table below.

Item	Default Sharing Permission
Assessment template and discussion regarding the assessment process	OK to share
List of service providers assessed and contact information of service providers	OK to share
Completed Vendor Assessment Tool (vendor answers intact)	None, Opt-in by service provider only
Security report created by this Higher Education institution	None, Opt-in by service provider only

The REN-ISAC hosts the Cloud Broker Index (CBI), an up-to-date index of a populated HECVAT for any/all of their services. Vendors have the choice of providing a link(s) to the index, or having the REN-ISAC host their populated

The Cloud Broker Index can be found at: <https://www.ren-isac.net/hecva>

cloud service providers understand
stitutions. Anticipated sharing

Default Sharing Audience
Public
Higher education institutions only
None, unless opt-in. If a service provider opts-in, the sharing is within higher education institutions only
None, unless opt-in. If a service provider opts-in, the sharing is within higher education institutions only

of participating vendors that maintain
e to host their own HECVAT(s),
ated HECVAT(s).

it/cbi.html.

Higher Education Instructions

Target Audience

These instructions are for the worksheet should not be submitted. Robust security is required for Institution's assessment.

Document Layout

There are five main sections. For more detail, this document is provided. Once completed, it can be populated. Questions are nested and in the correct order will

General Information

Higher Education Shared Assessments Confirmation

Qualifiers

Documentation

Company Overview

Safeguards

In sections where vendors are listed, answers and additional information are provided. Sometimes C and D are down boxes and any supporting information is provided. For questions, check this column. Use the "Addit

Figure 1:

Optional Safeguards

Not all questions are relevant depending on the scope become optional have the

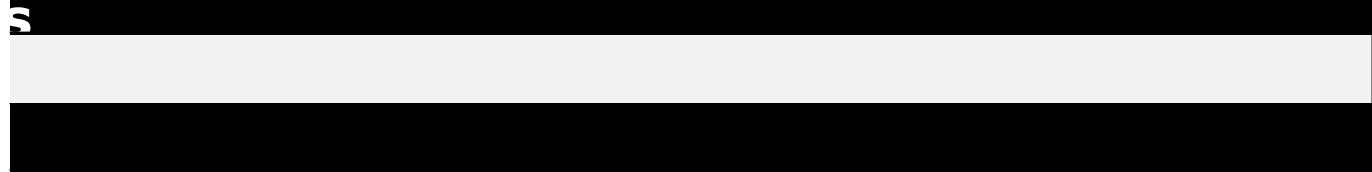
Figure 2:

BCP - Optional based on C

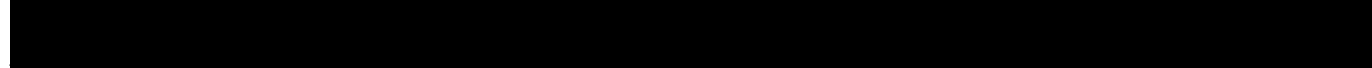
BCPL-01	Describe or provide a ref
---------	---------------------------

Proceed to the next t:

Higher Education Cloud Vendor Assessment Tool



For vendors interested in providing the Institution with a software and/or a service. This assessment is to be completed by a Institution entity. The purpose of this worksheet is for the vendor to provide information and safeguard information in regards to the product (software/service) being assessed in the assessment process.



Directions of the Higher Education Cloud Vendor Assessment Tool, all listed below and outlined in the document. The document is designed to have the first two sections populated first; after the Qualifiers section is populated in any order. Within each section, answer each question top-to-bottom. Some information may be blocked out via formatting based on previous answers. Populating this document ensure that questions are not answered unnecessarily.

This section is self-explanatory; product specifics and contact information. GNRL-01 through GNRL-06 should be populated by an institution entity. **GNRL-07 through GNRL-14 should be populated by the Vendor.** GNRL-15 and GNRL-16 are for Institution use only.

Answers to the statements in this section will determine how this assessment may be shared within the Higher Education community. Refer to the Sharing Read Me tab for further details.

Populate this section **completely** before continuing. Answers in this section can determine which sections will be required for this assessment. By answering "No" to Qualifiers, their matched sections become optional and are highlighted in orange.

Focused on external documentation, the Institution is interested in the frameworks that lead your security strategy and what has been done to certify these implementations.

This section is focused on company background, size, and business area experience.

The remainder of the document consists of various safeguards grouped generally by section.

For input is required there are only one or two columns that need modification, Vendor Information, columns C and D respectively (see Figure 1 below). You will see that separate and other times are merged. If they are separate, C will be a selectable, drop-down menu and information should be added to column D. If C and D are merged, the question is to be in narrative form. At the far right is a column titled "Guidance". After answering the question, the column to ensure you have submitted information/documentation to sufficiently answer the question. The "Additional Information" column to provide any requested details.

C	D	E
Vendor Answers	Additional Information	Guidance
No		Provide a brief description.

s Based on Qualifiers

evant to all vendors. Qualifiers are used to make whole sections optional to vendors of product usage and the data involved in the engagement being assessed. Sections that the section titles and questions highlighted in orange (see Figure 2).

QUALIFIER response.	Vendor Answers	Additional Information
ference to your Business Continuity Plan.		

ab, Cloud Vendor Assessment Tool, to begin.

Higher Education Cloud Vendor Assessment Tool

DATE-01	Date	<input type="checkbox"/> <input type="checkbox"/>
---------	-------------	---

General Information

In order to protect the Institution and its systems, vendors whose products and/or services will access and/or Throughout this tool, anywhere where the term data is used, this is an all-encompassing term including at least process will assist the institution in preventing breaches of protected information and comply with Institution p Assessment and should be completed by a vendor. Review the *Instructions* tab for further guidance.

GNRL-01 through GNRL-06; populated by Institution

GNRL-01	Institution Department	<i>The University of Texas</i>
GNRL-02	Institution Department Primary Campus	<i>System Administration</i>
GNRL-03	Institution Department Code	<i>NA</i>
GNRL-04	Institution Department Contact Name	<i>Institution Department Con</i>
GNRL-05	Institution Department Contact Email	<i>Institution Department Con</i>
GNRL-06	Institution Department Contact Phone Number	<i>555-555-5555</i>

GNRL-07 through GNRL-14; populated by Vendor

GNRL-07	Vendor Name	<i>Vendor Name</i>
GNRL-08	Product Name	<i>Product Name and Version .</i>
GNRL-09	Product Description	<i>Please include a brief descr</i>

GNRL-10	Web Link to Product Privacy Notice	<i>http://www.vendor.domain,</i>
GNRL-11	Vendor Contact Name	<i>Vendor Contact Name</i>
GNRL-12	Vendor Contact Title	<i>Vendor Contact Title</i>
GNRL-13	Vendor Contact Email	<i>Vendor Contact E-mail Addi</i>
GNRL-14	Vendor Contact Phone Number	<i>555-555-5555</i>
GNRL-15 and GNRL-16; populated by Institution Security Office		
GNRL-15	Institution Security Analyst/Engineer	<i>Institution Security Analyst,</i>
GNRL-16	Assessment Contact	<i>ticket#@yourdomain.edu</i>

Higher Education Shared Assessments Confirmation

Vendor Answers

By completing the Higher Education Cloud Vendor Assessment Tool, cloud service providers understand that the **following statements will determine how this assessment may be shared within the Higher Education**

HESA-01	I understand the goal of Higher Education Shared Assessments and that the completed Higher Education Cloud Vendor Assessment Tool may be shared with other higher education institutions, based on the following selections.	Yes
HESA-02	Add this completed assessment to a list of Higher Education assessed service providers, with contact information for service providers. No answers are shared; it is a list stating vendor, product, version, and service provider contact information.	Yes; OK to List
HESA-03	This completed Vendor Assessment Tool (with vendor answers intact) can be shared within Higher Education institutions through the Cloud Broker Index, https://www.ren-isac.net/hecvat/cbi.html .	Yes; OK to Share

HESA-04	The security report created by this Higher Education institution, after evaluating this assessment, can be shared within Higher Education institutions.	Yes; OK to Share
---------	---	------------------

Instructions

Step 1: Complete the *Qualifiers* section first. **Step 2:** Complete each section answering each set of questions completed Higher Education Cloud Vendor Assessment Tool (HECVAT) to the Institution according to institution

Qualifiers

Vendor Answers

The Institution conducts Third Party Security Assessments on a variety of third parties. As such, not all assess and allows for various parties to utilize this common documentation instrument. **Responses to the following**

QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	No
QUAL-02	Does the vended product host/support a mobile application? (e.g. app)	
QUAL-03	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)	
QUAL-04	Do you have a Business Continuity Plan (BCP)?	

QUAL-05	Do you have a Disaster Recovery Plan (DRP)?	
QUAL-06	Will data regulated by PCI DSS reside in the vended product?	Yes
QUAL-07	Is your company a consulting firm providing only consultation to the Institution?	No
Documentation		Vendor Answers
DOCU-01	Have you undergone a SSAE 16 audit?	
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Special Publication 800-53, ISO 27001, etc.)	
DOCU-05	Are you compliant with FISMA standards (indicate at what level)?	

DOCU-06	Does your organization have a data privacy policy?	
Company Overview		Vendor Answers
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	
COMP-02	Describe how long your organization has conducted business in this product area.	
COMP-03	How many higher education, commercial customers and government customers do you serve in North America? Please provide a higher education customer reference if available.	
COMP-04	Please explain in detail any involvement in business-related litigation in the last five years by your organization, its management, or the staff that will be providing the administrative services.	
COMP-05	Describe the structure and size of your Security Office and overall information security staff. (e.g. Admin, Engineering, QA/Compliance, etc.)	
COMP-06	Describe the structure and size of your Software and System Development teams. (e.g. Customer Support, Implementation, Product Management, etc.)	

COMP-07	Use this area to share information about your environment that will assist those who are evaluating you company data security safeguards.	
Third Parties		Vendor Answers
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.	
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?	

THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.	
Consulting - Optional based on QUALIFIER response.		Vendor Answers
CONS-01	Will the consulting take place on-premises or remotely?	
CONS-02	Will the consultant require access to Institution's network resources?	
CONS-03	Will the consultant require access to hardware in the Institution's data centers?	
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?	
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?	
CONS-06	Will any data be transferred to the consultant's possession?	

CONS-07	How long will it remain in their possession?	
CONS-08	Is it encrypted (at rest) while in the consultant's possession?	
CONS-09	Will the consultant need remote access to the Institution's network or systems?	
CONS-10	What software will be used to facilitate that access?	
CONS-11	Can we restrict that access based on source IP address?	

Application/Service Security		Vendor Answers
APPL-01	Does the application/service support being virtualized?	
APPL-02	Are the servers hosting institution data currently deployed in a virtualized environment?	
APPL-03	Can user access be customized to allow read-only access, update access, or no-access to specific types of records, record attributes, components, or functions?	
APPL-04	Describe or provide a reference to how user security administration is performed?	

APPL-05	Define the access control roles of employees that will have access to the data and in what capacity.	
APPL-06	Do you allow employees to remotely access data (i.e. work from home)?	
APPL-07	Define what controls are in place to secure their remote environment and connection to the institution's data.	
APPL-08	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?	
APPL-09	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?	
APPL-10	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.	

APPL-11	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.	
APPL-12	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)	
APPL-13	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).	
APPL-14	Describe or provide a reference to any OS and/or web-browser combinations that are not currently supported.	
APPL-15	Can your system take advantage of mobile and/or GPS enabled mobile devices?	
APPL-16	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.	
APPL-17	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)	

APPL-18	Does the system provide data input validation and error messages?	
APPL-19	Do you employ a single-tenant or multi-tenant strategy in the environment hosting Institution's data?	
APPL-20	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc...).	
Authentication, Authorization, and Accounting		Vendor Answers
AAAI-01	Can you enforce password/passphrase aging requirements?	
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?	
AAAI-03	What are the minimum and maximum password lengths supported, and what types of characters are supported?	
AAAI-04	Describe the current/default/supported password/passphrase reset procedures?	

AAAI-05	Describe or provide a reference to the types of authentication, including standards-based single-sign-on (SSO, InCommon), that are supported by the web-based interface?	
AAAI-06	Are there any passwords/passphrases "hard coded" into your systems or products?	
AAAI-07	Are user account passwords/passphrases visible in administration modules?	
AAAI-08	Are user account passwords/passphrases stored encrypted?	
AAAI-09	Describe or provide a reference to the algorithm/strategy that is used to encrypt stored passwords/passphrases?	
AAAI-10	Does your <i>application</i> and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	
AAAI-11	List all supported multi-factor authentication methods, technologies, and/or products and provide a brief summary of each.	
AAAI-12	Does your <i>application</i> support integration with other authentication and authorization systems such as Active Directory, Kerberos (what version) or another institution centralized authorization service?	

AAAI-13	Will any external authentication or authorization system be utilized by an application with access to the institution's data?	
AAAI-14	Does the <i>system</i> (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?	
AAAI-15	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?	
AAAI-16	Will any external authentication or authorization system be utilized by a system with access to institution data?	
AAAI-17	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	
AAAI-18	Describe or provide a reference to the system capability to log security/authorization changes as well as user and administrator security (physical or electronic) events (e.g., login failures, access denied, changes accepted), and all requirements necessary to implement logging and monitoring on the system. Include information about SIEM/log collector usage.	
AAAI-19	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).	

Business Continuity Plan		Vendor Answers
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).	
BCPL-02	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?	
BCPL-03	If possible, can the Institution review your BCP and supporting documentation?	
BCPL-04	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	
BCPL-05	Is there a documented communication plan in your BCP for impacted clients?	
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	
BCPL-07	Indicate the last time that the BCP was tested and provide a summary of the results.	
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?	

BCPL-09	Are specific crisis management roles and responsibilities defined and documented?	
BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?	
BCPL-11	Does your organization conduct an annual test of relocating to this alternate site for business recovery purposes?	
BCPL-12	Indicate the priority of service restoration for services utilized by the Institution compared to other applications/services the vendor provides.	
Change Management		Vendor Answers
CHNG-01	Do you have a documented and currently followed change management process (CMP)?	
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.	
CHNG-03	How and when will the Institution be notified of major changes to your environment that could impact the Institution's security posture?	

CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)	
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.	
CHNG-07	Describe, if applicable, your support for client customizations from one release to another.	
CHNG-08	How does your organization ensure that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?	
CHNG-09	Describe or provide a reference to your release schedule for product updates.	
CHNG-10	Describe or provide a reference to your technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed.	

CHNG-11	Describe or provide a reference to your expectation of client involvement with product updates?	
CHNG-12	Provide a brief summary of how critical patches are applied to all systems and applications.	
CHNG-13	Describe or provide a reference to how security risks are mitigated until patches can be applied.	
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	
Data		Vendor Answers
DATA-01	Describe the highest level of data classification that will be managed within your system(s) and/or application(s).	
DATA-02	Describe or provide a reference to how institution data is physically and logically separated from that of other customers.	

DATA-03	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, ...) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?	
DATA-04	Is sensitive data encrypted in transport?	
DATA-05	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?	
DATA-06	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?	
DATA-07	Describe or provide a reference to the encryption technology and strategy you employ for transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN).	
DATA-08	List all locations (i.e. city + datacenter name) where the institution's data will be stored?	
DATA-09	At the completion of this contract, will data be returned to the institution?	
DATA-10	How will data be returned to the institution and in what format?	
DATA-11	How long will the institution's data be available within the system at the completion of this contract?	

DATA-12	Can the institution extract a full backup of data?	
DATA-13	Are ownership rights to all data, inputs, outputs, and metadata retained by the Institution?	
DATA-14	Are these rights retained even through a provider acquisition or bankruptcy event?	
DATA-15	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?	
DATA-16	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.	
DATA-17	Are backup copies made according to pre-defined schedules and securely stored and protected?	
DATA-18	How long are data backups stored?	
DATA-19	Are data backups encrypted?	
DATA-20	Summarize the encryption algorithm/strategy you are using to secure the backups.	

DATA-21	Describe or provide a reference to your cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) of all system components (e.g. database, system, web, etc.).	
DATA-22	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	
DATA-23	Are you performing offsite backups? (i.e. digitally moved off site)	
DATA-24	Are physical backups taken off site? (i.e. physically moved off site)	
DATA-25	Do backups containing the institution's data ever leave the United States of America either physically or via network routing?	
DATA-26	Describe or provide a reference to your media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures.	
DATA-27	Does this process adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?	
DATA-28	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?	

DATA-29	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?	
DATA-30	Will you handle data in a FERPA compliant manner?	
DATA-31	Is any institution data visible in system administration modules/tools?	
Database		Vendor Answers
DBAS-01	Does the database support encryption of specified data elements in storage?	
DBAS-02	Do you currently use encryption in your database(s)?	
Datacenter		Vendor Answers
DCTR-01	Does your company own the physical data center where the Institution's data will reside?	
DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?	
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e 24x7x365)?	
DCTR-04	Do any of your servers reside in a co-located data center?	

DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?	
DCTR-06	Does the physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	
DCTR-07	Select the option that best describes the network segment that servers are connected to.	
DCTR-08	Does this data center operate outside of the United States?	
DCTR-09	Will any institution data leave the United States?	
DCTR-10	List all datacenters and their cities, states (provinces), and countries where the institution's data will be stored (including within the United States).	
DCTR-11	Are your primary and secondary data centers geographically diverse?	
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the United States?	
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?	
DCTR-14	Is the service hosted in a high availability environment?	

DCTR-15	Is redundant power available for all datacenters where institution data will reside?	
DCTR-16	How often are redundant power strategies tested?	
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.	
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.	
DCTR-19	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?	
Disaster Recovery Plan		Vendor Answers
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).	
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	
DRPL-03	If possible, can the Institution review your DRP and supporting documentation?	

DRPL-04	Are any disaster recovery locations outside the United States?	
DRPL-05	Does your organization have a Disaster Recovery site or a contracted Disaster Recovery provider?	
DRPL-06	What type of availability does your Disaster Recovery site provide?	
DRPL-07	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?	
DRPL-08	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	
DRPL-09	Is there a documented communication plan in your DRP for impacted clients?	
DRPL-10	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)	
DRPL-11	Indicate the last time that the Disaster Recovery Plan was tested and provide a summary of the results (including actual recovery time).	

DRPL-12	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?	
DRPL-13	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	
DRPL-14	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	
Firewalls, IDS, IPS, and Networking		Vendor Answers
FIDP-01	Are you utilizing a web application firewall (WAF)?	
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?	
FIDP-03	State and describe who has the authority to change firewall rules?	
FIDP-04	Do you have a documented policy for firewall change requests?	
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?	
FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?	
FIDP-07	Do you employ host-based intrusion detection?	

FIDP-08	Do you employ host-based intrusion prevention?	
FIDP-09	Describe or provide a reference to any other safeguards used to monitor for attacks?	
FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?	
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?	
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and/or IPS?	
Mobile Applications		Vendor Answers
MAPP-01	On which mobile operating systems is your software or service supported?	
MAPP-02	Describe or provide a reference to the application's architecture and functionality.	
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?	
MAPP-04	Does the application store, process, or transmit critical data?	

MAPP-05	Is Institution data encrypted in transport?	
MAPP-06	Is Institution data encrypted in storage? (e.g. disk encryption, at-rest)	
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?	
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?	
MAPP-09	Does the application adhere to secure coding practices?	
MAPP-10	Has the application been tested for vulnerabilities by a third party?	
MAPP-11	State the party that performed the test and the date it was conducted?	
Physical Security		Vendor Answers
PHYS-01	Describe or provide a reference to physical safeguards that are placed on facilities housing the institution's data (e.g., video monitoring, restricted access areas, man traps, card access controls, etc.)?	
PHYS-02	Are employees allowed to take home Institution's data in any form?	

PHYS-03	Are video monitoring feeds retained?	
PHYS-04	Is the video feed monitored by data center staff?	
PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?	
PHYS-06	What are the equipment removal procedures for the clients?	
Policies, Procedures, and Processes		Vendor Answers
PPPR-01	Briefly describe your security organization. Include the responsible party for your information security program and the size of your security staff?	
PPPR-02	Do you have a documented patch management process?	
PPPR-03	Can you accommodate encryption requirements using open standards?	
PPPR-04	Have your developers been trained in secure coding techniques?	
PPPR-05	Was your application developed using secure coding techniques?	

PPPR-06	Do you subject your code to Static Code Analysis and/or Static Application Security Testing prior to release? If so, what tool(s) do you use?"	
PPPR-07	Describe testing processes that are established and followed (e.g., development of test plans, personnel involved in the testing process, and authorized individual accountable for approval and certification of test results)?	
PPPR-08	Are information security principles designed into the product lifecycle?	
PPPR-09	Do you have a documented systems development life cycle (SDLC)?	
PPPR-10	Describe or provide a reference to your system development life cycle methodology including your environments, version control, and change management (if not already covered in the Change Management section).	
PPPR-11	Do you have a formal incident response plan?	
PPPR-12	Will you comply with applicable Breach Notification Laws?	
PPPR-13	Will you comply with the Institution's IT policies with regards to user privacy and data protection?	
PPPR-14	Is your company subject to US laws and regulations?	

PPPR-15	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	
PPPR-16	Do you require new employees to fill out agreements and review policies?	
PPPR-17	What agreements are required and policies reviewed? (i.e. confidentiality agreement, etc.)	
PPPR-18	Do you have a documented information security policy?	
PPPR-19	Do you have an information security awareness program?	
PPPR-20	Is the security awareness training mandatory for all employees?	
PPPR-21	How frequently are employees required to undergo the security awareness training?	
PPPR-22	Is a process documented, and currently followed, that requires a review and update of the access-list for privileged accounts?	
PPPR-23	Describe or provide a reference to your internal audit processes and procedures.	

Product Evaluation**Vendor Answers**

PROD-01	Do you incorporate customer feedback into security feature requests?	
PROD-02	Can you provide an evaluation site to the institution for testing?	

Quality Assurance**Vendor Answers**

QLAS-01	Provide a general summary of your Quality Assurance program.	
QLAS-02	Do you comply with ISO 9001?	
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?	
QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?	
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?	

Systems Management & Configuration**Vendor Answers**

SYST-01	Are systems that support this service managed via a separate management network?	
SYST-02	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)	
SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?	
SYST-04	Provide a general summary of your systems management and configuration strategy, including servers, appliances, and mobile devices (company and employee owned).	

Vulnerability Scanning		Vendor Answers
VULN-01	Are your <i>applications</i> scanned externally for vulnerabilities?	
VULN-02	What was the date of your applications last external assessment? (mm/dd/yyyy)	
VULN-03	Are your applications scanned for vulnerabilities prior to new releases?	
VULN-04	Are your <i>systems</i> scanned externally for vulnerabilities?	

VULN-05	What was the date of your systems last external assessment? (mm/dd/yyyy)	
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.	
VULN-07	Will you provide results of security scans to the Institution (if requested)?	
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).	
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?	
HIPAA - Optional based on QUALIFIER response.		Vendor Answers
HIPAA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?	
HIPAA-02	Do you monitor or receive information regarding changes in HIPAA regulations?	
HIPAA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?	

HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?	
HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?	
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?	
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?	
HIPA-08	Have you identified areas of risks?	
HIPA-09	Have you taken actions to mitigate the identified risks?	
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?	
HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?	
HIPA-12	Does your application lock-out an account after a number of failed login attempts?	

HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?	
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?	
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?	
HIPA-16	Does your application provide the ability to define user access levels?	
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?	
HIPA-18	Does your application support varying levels of access to records based on user ID?	
HIPA-19	Is there a limit to the number of groups a user can be assigned?	
HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?	
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?	

HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?	
HIPA-23	How long does the application keep access/change logs?	
HIPA-24	Can the application logs be archived?	
HIPA-25	Can the application logs be saved externally?	
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?	
HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?	
HIPA-28	Have the policies/plans mentioned above been tested?	
HIPA-29	Can the application logs be saved externally?	
HIPA-30	Can you provide a HIPAA compliance attestation document?	
HIPA-31	Are you willing to enter into a Business Associate Agreement (BAA)?	

HIPA-32	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?	
PCI DSS		Vendor Answers
PCID-01	Does your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?	
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?	
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?	
PCID-04	Are you classified as a service provider?	
PCID-05	Are you on the list of VISA approved service providers?	
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.	

PCID-08	What payment processors/gateways does the system support?	
PCID-09	Can the application be installed in a PCI DSS compliant manner ?	
PCID-10	Is the application listed as an approved PA-DSS application?	
PCID-11	Does the systems or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?	
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.	

Most institutional data must complete the Higher Education Cloud Vendor Assessment Tool (HECVAT).
All data and metadata. Answers will be reviewed by Institution security analysts upon submittal. This
policy, state, and federal law. This is intended for use by vendors participating in a Third Party Security

Contact Name

Contact Email

Information

Description of the product

/privacynotice

ress

/Engineer Name

Additional Information

Guidance

he completed assessment may be shared among higher education institutions. **Answers to the
ion community**. Shared assessment sharing details can be found on the "Sharing Read Me" tab.

Scope: Higher Education Institutions Only

Scope: Higher Education Institutions Only

Scope: Higher Education Institutions Only	
in order from top to bottom; the built-in formatting logic relies on this order. Step 3: Submit the final procedures.	
Additional Information	Guidance
<p>ment questions are relevant to each party. To alleviate complexity, a "qualifier" strategy is implemented. g questions will determine the need to answer additional questions below.</p>	
	Responses to the questions in the HIPAA section are optional.

	You are required to complete the questions in the PCI DSS section.
NOTE: If there is a possibility that any consulting services will be provided, the Consulting section must be completed.	Responses to the questions in the Consulting section are optional.
Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance
-------------------------------	-----------------

Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance
Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance
Additional Information	Guidance
Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance

Additional Information	Guidance

Higher Education Cloud Vendor Assessment T

HEISC Shared Assessments Working Group

Qualifiers

QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?
QUAL-02	Does the vended product host/support a mobile application? (e.g. app)
QUAL-03	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)
QUAL-04	Do you have a Business Continuity Plan (BCP)?
QUAL-05	Do you have a Disaster Recovery Plan (DRP)?
QUAL-06	Will data regulated by PCI DSS reside in the vended product?
QUAL-07	Is your company a consulting firm providing only consultation to the Institution?

Documentation

DOCU-01	Have you undergone a SSAE 16 audit?
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?
DOCU-03	Have you received the Cloud Security Alliance STAR certification?
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Special Publication 800-53, ISO 27001, etc.)
DOCU-05	Are you compliant with FISMA standards (indicate at what level)?
DOCU-06	Does your organization have a data privacy policy?

Company Overview

COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.
---------	--

COMP-02	Describe how long your organization has conducted business in this product area.
COMP-03	How many higher education, commercial customers and government customers do you serve in North America? Please provide a higher education customer reference if available.
COMP-04	Please explain in detail any involvement in business-related litigation in the last five years by your organization, its management, or the staff that will be providing the administrative services.
COMP-05	Describe the structure and size of your Security Office and overall information security staff. (e.g. Admin, Engineering, QA/Compliance, etc.)
COMP-06	Describe the structure and size of your Software and System Development teams. (e.g. Customer Support, Implementation, Product Management, etc.)
COMP-07	Use this area to share information about your environment that will assist those who are evaluating your company data security safeguards.

Third Parties

THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.
Consulting - Optional based on QUALIFIER response.	
CONS-01	Will the consulting take place on-premises or remotely?

CONS-02	Will the consultant require access to Institution's network resources?
CONS-03	Will the consultant require access to hardware in the Institution's data centers?
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?
CONS-06	Will any data be transferred to the consultant's possession?
CONS-07	How long will it remain in their possession?
CONS-08	Is it encrypted (at rest) while in the consultant's possession?
CONS-09	Will the consultant need remote access to the Institution's network or systems?
CONS-10	What software will be used to facilitate that access?

CONS-11	Can we restrict that access based on source IP address?
Application/Service Security	
APPL-01	Does the application/service support being virtualized?
APPL-02	Are the servers hosting institution data currently deployed in a virtualized environment?
APPL-03	Can user access be customized to allow read-only access, update access, or no-access to specific types of records, record attributes, components, or functions?
APPL-04	Describe or provide a reference to how user security administration is performed?
APPL-05	Define the access control roles of employees that will have access to the data and in what capacity.
APPL-06	Do you allow employees to remotely access data (i.e. work from home)?

APPL-07	Define what controls are in place to secure their remote environment and connection to the institution's data.
APPL-08	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?
APPL-09	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?
APPL-10	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.
APPL-11	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.
APPL-12	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)

APPL-13	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).
APPL-14	Describe or provide a reference to any OS and/or web-browser combinations that are not currently supported.
APPL-15	Can your system take advantage of mobile and/or GPS enabled mobile devices?
APPL-16	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.
APPL-17	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)
APPL-18	Does the system provide data input validation and error messages?
APPL-19	Do you employ a single-tenant or multi-tenant strategy in the environment hosting Institution's data?

APPL-20	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc...).
---------	--

Authentication, Authorization, and Accounting

AAAI-01	Can you enforce password/passphrase aging requirements?
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?
AAAI-03	What are the minimum and maximum password lengths supported, and what types of characters are supported?
AAAI-04	Describe the current/default/supported password/passphrase reset procedures?
AAAI-05	Describe or provide a reference to the types of authentication, including standards-based single-sign-on (SSO, InCommon), that are supported by the web-based interface?
AAAI-06	Are there any passwords/passphrases "hard coded" into your systems or products?
AAAI-07	Are user account passwords/passphrases visible in administration modules?

AAAI-08	Are user account passwords/passphrases stored encrypted?
AAAI-09	Describe or provide a reference to the algorithm/strategy that is used to encrypt stored passwords/passphrases?
AAAI-10	Does your <i>application</i> and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)
AAAI-11	List all supported multi-factor authentication methods, technologies, and/or products and provide a brief summary of each.
AAAI-12	Does your <i>application</i> support integration with other authentication and authorization systems such as Active Directory, Kerberos (what version) or another institution centralized authorization service?
AAAI-13	Will any external authentication or authorization system be utilized by an application with access to the institution's data?
AAAI-14	Does the <i>system</i> (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?
AAAI-15	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?

AAAI-16	Will any external authentication or authorization system be utilized by a system with access to institution data?
AAAI-17	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?
AAAI-18	Describe or provide a reference to the system capability to log security/authorization changes as well as user and administrator security (physical or electronic) events (e.g., login failures, access denied, changes accepted), and all requirements necessary to implement logging and monitoring on the system. Include information about SIEM/log collector usage.
AAAI-19	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).
Business Continuity Plan	
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).
BCPL-02	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?
BCPL-03	If possible, can the Institution review your BCP and supporting documentation?

BCPL-04	Is there a defined problem/issue escalation plan in your BCP for impacted clients?
BCPL-05	Is there a documented communication plan in your BCP for impacted clients?
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?
BCPL-07	Indicate the last time that the BCP was tested and provide a summary of the results.
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?
BCPL-09	Are specific crisis management roles and responsibilities defined and documented?
BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?
BCPL-11	Does your organization conduct an annual test of relocating to this alternate site for business recovery purposes?
BCPL-12	Indicate the priority of service restoration for services utilized by the Institution compared to other applications/services the vendor provides.

Change Management

CHNG-01	Do you have a documented and currently followed change management process (CMP)?
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.
CHNG-03	How and when will the Institution be notified of major changes to your environment that could impact the Institution's security posture?
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.

CHNG-07	Describe, if applicable, your support for client customizations from one release to another.
CHNG-08	How does your organization ensure that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?
CHNG-09	Describe or provide a reference to your release schedule for product updates.
CHNG-10	Describe or provide a reference to your technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed.
CHNG-11	Describe or provide a reference to your expectation of client involvement with product updates?
CHNG-12	Provide a brief summary of how critical patches are applied to all systems and applications.
CHNG-13	Describe or provide a reference to how security risks are mitigated until patches can be applied.

CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?
Data	
DATA-01	Describe the highest level of data classification that will be managed within your system(s) and/or application(s).
DATA-02	Describe or provide a reference to how institution data is physically and logically separated from that of other customers.
DATA-03	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, ...) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?
DATA-04	Is sensitive data encrypted in transport?
DATA-05	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?
DATA-06	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?

DATA-07	Describe or provide a reference to the encryption technology and strategy you employ for transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN).
DATA-08	List all locations (i.e. city + datacenter name) where the institution's data will be stored?
DATA-09	At the completion of this contract, will data be returned to the institution?
DATA-10	How will data be returned to the institution and in what format?
DATA-11	How long will the institution's data be available within the system at the completion of this contract?
DATA-12	Can the institution extract a full backup of data?
DATA-13	Are ownership rights to all data, inputs, outputs, and metadata retained by the Institution?
DATA-14	Are these rights retained even through a provider acquisition or bankruptcy event?
DATA-15	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?

DATA-16	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.
DATA-17	Are backup copies made according to pre-defined schedules and securely stored and protected?
DATA-18	How long are data backups stored?
DATA-19	Are data backups encrypted?
DATA-20	Summarize the encryption algorithm/strategy you are using to secure the backups.
DATA-21	Describe or provide a reference to your cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) of all system components (e.g. database, system, web, etc.).
DATA-22	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?
DATA-23	Are you performing offsite backups? (i.e. digitally moved off site)
DATA-24	Are physical backups taken off site? (i.e. physically moved off site)

DATA-25	Do backups containing the institution's data ever leave the United States of America either physically or via network routing?
DATA-26	Describe or provide a reference to your media handing process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures.
DATA-27	Does this process adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?
DATA-28	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?
DATA-29	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?
DATA-30	Will you handle data in a FERPA compliant manner?
DATA-31	Is any institution data visible in system administration modules/tools?
Database	
DBAS-01	Does the database support encryption of specified data elements in storage?
DBAS-02	Do you currently use encryption in your database(s)?

Datacenter

DCTR-01	Does your company own the physical data center where the Institution's data will reside?
DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e 24x7x365)?
DCTR-04	Do any of your servers reside in a co-located data center?
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?
DCTR-06	Does the physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?
DCTR-07	Select the option that best describes the network segment that servers are connected to.
DCTR-08	Does this data center operate outside of the United States?
DCTR-09	Will any institution data leave the United States?

DCTR-10	List all datacenters and their cities, states (provinces), and countries where the institution's data will be stored (including within the United States).
DCTR-11	Are your primary and secondary data centers geographically diverse?
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the United States?
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?
DCTR-14	Is the service hosted in a high availability environment?
DCTR-15	Is redundant power available for all datacenters where institution data will reside?
DCTR-16	How often are redundant power strategies tested?
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.

DCTR-19	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?
Disaster Recovery Plan	
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?
DRPL-03	If possible, can the Institution review your DRP and supporting documentation?
DRPL-04	Are any disaster recovery locations outside the United States?
DRPL-05	Does your organization have a Disaster Recovery site or a contracted Disaster Recovery provider?
DRPL-06	What type of availability does your Disaster Recovery site provide?
DRPL-07	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?

DRPL-08	Is there a defined problem/issue escalation plan in your DRP for impacted clients?
DRPL-09	Is there a documented communication plan in your DRP for impacted clients?
DRPL-10	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)
DRPL-11	Indicate the last time that the Disaster Recovery Plan was tested and provide a summary of the results (including actual recovery time).
DRPL-12	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?
DRPL-13	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?
DRPL-14	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?
Firewalls, IDS, IPS, and Networking	
FIDP-01	Are you utilizing a web application firewall (WAF)?

FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?
FIDP-03	State and describe who has the authority to change firewall rules?
FIDP-04	Do you have a documented policy for firewall change requests?
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?
FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?
FIDP-07	Do you employ host-based intrusion detection?
FIDP-08	Do you employ host-based intrusion prevention?
FIDP-09	Describe or provide a reference to any other safeguards used to monitor for attacks?
FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and/or IPS?

Mobile Applications

MAPP-01	On which mobile operating systems is your software or service supported?
MAPP-02	Describe or provide a reference to the application's architecture and functionality.
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?
MAPP-04	Does the application store, process, or transmit critical data?
MAPP-05	Is Institution data encrypted in transport?
MAPP-06	Is Institution data encrypted in storage? (e.g. disk encryption, at-rest)
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?
MAPP-09	Does the application adhere to secure coding practices?

MAPP-10	Has the application been tested for vulnerabilities by a third party?
MAPP-11	State the party that performed the test and the date it was conducted?
Physical Security	
PHYS-01	Describe or provide a reference to physical safeguards that are placed on facilities housing the institution's data (e.g., video monitoring, restricted access areas, man traps, card access controls, etc.)?
PHYS-02	Are employees allowed to take home Institution's data in any form?
PHYS-03	Are video monitoring feeds retained?
PHYS-04	Is the video feed monitored by data center staff?
PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?
PHYS-06	What are the equipment removal procedures for the clients?
Policies, Procedures, and Processes	

PPPR-01	Briefly describe your security organization. Include the responsible party for your information security program and the size of your security staff?
PPPR-02	Do you have a documented patch management process?
PPPR-03	Can you accommodate encryption requirements using open standards?
PPPR-04	Have your developers been trained in secure coding techniques?
PPPR-05	Was your application developed using secure coding techniques?
PPPR-06	Do you subject your code to Static Code Analysis and/or Static Application Security Testing prior to release? If so, what tool(s) do you use?"
PPPR-07	Describe testing processes that are established and followed (e.g., development of test plans, personnel involved in the testing process, and authorized individual accountable for approval and certification of test results)?
PPPR-08	Are information security principles designed into the product lifecycle?

PPPR-09	Do you have a documented systems development life cycle (SDLC)?
PPPR-10	Describe or provide a reference to your system development life cycle methodology including your environments, version control, and change management (if not already covered in the Change Management section).
PPPR-11	Do you have a formal incident response plan?
PPPR-12	Will you comply with applicable Breach Notification Laws?
PPPR-13	Will you comply with the Institution's IT policies with regards to user privacy and data protection?
PPPR-14	Is your company subject to US laws and regulations?
PPPR-15	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?
PPPR-16	Do you require new employees to fill out agreements and review policies?
PPPR-17	What agreements are required and policies reviewed? (i.e. confidentiality agreement, etc.)
PPPR-18	Do you have a documented information security policy?

PPPR-19	Do you have an information security awareness program?
PPPR-20	Is the security awareness training mandatory for all employees?
PPPR-21	How frequently are employees required to undergo the security awareness training?
PPPR-22	Is a process documented, and currently followed, that requires a review and update of the access-list for privileged accounts?
PPPR-23	Describe or provide a reference to your internal audit processes and procedures.

Product Evaluation

PROD-01	Do you incorporate customer feedback into security feature requests?
PROD-02	Can you provide an evaluation site to the institution for testing?

Quality Assurance

QLAS-01	Provide a general summary of your Quality Assurance program.
QLAS-02	Do you comply with ISO 9001?
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?
QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?
Systems Management & Configuration	
SYST-01	Are systems that support this service managed via a separate management network?
SYST-02	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)
SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?

SYST-04	Provide a general summary of your systems management and configuration strategy, including servers, appliances, and mobile devices (company and employee owned).
Vulnerability Scanning	
VULN-01	Are your <i>applications</i> scanned externally for vulnerabilities?
VULN-02	What was the date of your applications last external assessment? (mm/dd/yyyy)
VULN-03	Are your applications scanned for vulnerabilities prior to new releases?
VULN-04	Are your <i>systems</i> scanned externally for vulnerabilities?
VULN-05	What was the date of your systems last external assessment? (mm/dd/yyyy)
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.
VULN-07	Will you provide results of security scans to the Institution (if requested)?

VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?
HIPAA	
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?
HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?

HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?
HIPA-08	Have you identified areas of risks?
HIPA-09	Have you taken actions to mitigate the identified risks?
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?
HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?
HIPA-12	Does your application lock-out an account after a number of failed login attempts?
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?

HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?
HIPA-16	Does your application provide the ability to define user access levels?
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?
HIPA-18	Does your application support varying levels of access to records based on user ID?
HIPA-19	Is there a limit to the number of groups a user can be assigned?
HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?
HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?

HIPA-23	How long does the application keep access/change logs?
HIPA-24	Can the application logs be archived?
HIPA-25	Can the application logs be saved externally?
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?
HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?
HIPA-28	Have the policies/plans mentioned above been tested?
HIPA-29	Can you provide a HIPAA compliance attestation document?
HIPA-30	Are you willing to enter into a Business Associate Agreement (BAA)?
HIPA-31	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?

PCI DSS

PCID-01	Does your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?
PCID-04	Are you classified as a service provider?
PCID-05	Are you on the list of VISA approved service providers?
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.
PCID-08	What payment processors/gateways does the system support?
PCID-09	Can the application be installed in a PCI DSS compliant manner ?
PCID-10	Is the application listed as an approved PA-DSS application?

PCID-11	Does the systems or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.

Tool - Standards Crosswalk

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 13	Discovery	18.1.1
CSC 18		
CSC 13		
CSC 10		17.1.2
CSC 10		17.1.2
CSC 13		18.1.1
CSC 14		

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
		15.2.1
		15.2.1
		15.2.1
		18.1.1
		18.1.1
	§164.308(a)(1)(i)	18.1.4
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013

		15.2.1
		15.2.2
		15.2.1
		14.2.1
		15.2.1
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013

CSC 13		15.1.3
CSC 13		15.1.3
CSC 13		15.1.3
		15.1.3
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
		15.2.1

CSC 14		9.1.2
CSC 14		9.2.6
CSC 14		
CSC 13		18.1.1
CSC 13		9
CSC 13		9
CSC 13		10
CSC 14		9
CSC 13		

		9
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC18		
CSC 2, CSC 3		11.2.6
CSC 14		9.2.2
CSC16		9.1.1
CSC 14		9.1.1
CSC 14		6.2

CSC 12		6.2
CSC 2		12.5.1
		16
CSC 2		12.5.1
CSC 2		12.1.1
CSC 13		12.1.4

CSC 7		12.1.1
CSC 7		12.5.1
CSC 2		
CSC 14		9.2.3, 12.1.4
CSC 5		9.2
CSC 16		14.2.5
CSC 12		14.2.5

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 16		9.2.3, 9.3.1, 9.4.3
CSC 16		9.2.3, 9.3.1, 9.4.3
CSC 16		9.2.3, 9.3.1, 9.4.3
CSC 16		9.2.3, 9.3.1, 9.4.3
CSC 16		9.1.1, 9.2.3, 9.3.1, 9.4.3
CSC 16		9
CSC 16		9

CSC 16		9
CSC 16		9
CSC 16		9
CSC 16		9
CSC 16		9.4.3
CSC 16		9
CSC 16		9.4.3
CSC 16		

CSC 16		
CSC 6		12.4
CSC 6		12.4
CSC 6		12.4
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 10		17.1.1
CSC 10		17.1.1
CSC 10		

CSC 10		17
CSC 10		17.1.2
CSC 10		17.1.2
CSC 10		17.1.3
CSC 10		7.2.2, 17.1.3
CSC 10		7.2.2, 16.1.1, 17.1.3
CSC 10		17.2.1
CSC 10		17.1.3
CSC 10		

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 10		12.1.2
CSC 10		12.1.2
CSC 10		12.1.2
CSC 10		
CSC 2		
CSC 2		

CSC 10		
CSC 2		12.1.1
CSC 10		
CSC 2		
CSC 2		12.6.1
CSC 13	§164.308(a)(1)(ii)(B)	12.6.1

CSC 10		
CSC 10		12.1.2
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
		8.2.1
CSC 12		
CSC 12		
CSC 13		10.1.1
CSC 13		8.2.3, 10.1.1
CSC 13		8.2.3, 10.1.1

CSC 13		13.2
CSC 1		
CSC 13		8.1.4
CSC 13		8.1.4
CSC 13		8.1.4
		12.3.1
CSC 13		8.1.2
CSC 13		8.1.2
CAC 13		8.1.2

CSC 10		12.3.1
CSC 10		12.3.1
CSC 10		12.3.1
CSC 10		12.3.1
CSC 10		12.3.1
CSC 10		10.1.2
CSC 10		12.3.1
CSC 10		12.3.1
CSC 10		12.3.1

CSC 13		12.3.1
CSC 13		8.3.1
CSC 13		8.3.1, 18.1.1
CSC 13		8.3.1, 18.1.1
CSC 13		8.3.1, 18.1.1
CSC 13		18.1.1
CSC 13, CSC 14		14.2.5
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 13		10.1.1
CSC 13		10.1.1

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 14		11.1.1
CSC 13		11.1.1
CSC 3		17.2.1
CSC 3, CSC 14		
CSC 3, CSC 14		13.1.2
CSC 14		11.1.1, 11.1.2
CSC 9		
CSC 12		18.1.1
CSC 12		18.1.1

CSC 12		11.2.1
CSC 10		11.1.4
CSC 12		18.1.1
		17.1.1
CSC 10		17.1.1
		17.2.1
		17.1.3
		17.2.1
CSC 10		17.2.1

CSC 13		17.2.1
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 10		17.1.1
CSC 10		16.1.1, 17.1.1
CSC 10		
CSC 10, CSC 12		17.1.1
CSC 10		17.2.1
CSC 10		17.2.1
CSC 10		17.1.3

CSC 10		
CSC 10		17.1.2
CSC 10		17.1.3
CSC 10		17.1.3
CSC 10		7.1.3
CSC 10		17.1.1
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 9		13.1.1

CSC 9		13.1.1
CSC 9		13
CSC 9		12.1.2
CSC 19		13.1.2
CSC 19		13.1.2
CSC 19		13.1.2
CSC 19		13.1.2
CSC 19		12.4.1
CSC 19		12.4.1
CSC 6, CSC 19		12.4.1
CSC 6		12.4.1

CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 18		
CSC 3		
CSC 18		
CSC 13, CSC 18		8.2.1; 8.2.3
CSC 13		8.2.3
CSC 14		8.2.3
CSC 16		9.4.2
CSC 16		
CSC 18		14.2.1

CSC 18		12.7.1, 18.2.1
CSC 18		12.7.1, 18.2.1
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 3		11.1.1
CSC 13		8.2.3
CSC 3		11.1.2, 11.1.3
CSC 3		11.1.2, 11.1.3
CSC 14		11.1.2
CSC 1		11.1.2, 11.2.5
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013

		5.1.1
CSC 4		12.6.1
CSC 13		10.1.1, 18.1.5
CSC 4, CSC 17		14.2.1
CSC 4		14.2.1
CSC 4		14.2.1, 14.2.5, 14.2.8
CSC 4		14.2.8
CSC 4		14.2.1

CSC 4		14.2.1
CSC 4		14.2.1
CSC 19		16.1.5
CSC 19		18.1.1
CSC 13		18.1.1
CSC 19		18.1.1
CSC 5		7.1.1
CSC 17		7.1.2
CSC 17		7.1.2
CSC 17	§164.308(a)(1)(i)	5.1.1

CSC 17	§164.308(a)(5)(i)	7.2.2
CSC 17	§164.308(a)(5)(i)	7.2.2
CSC 17	§164.308(a)(5)(i)	7.2.2
CSC 17		9.2.5
		12.7.1
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013

CSC 13		
CSC 13		18.1.1
CSC 13		
CSC 17		
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 12		13.1.1
CSC 3		
CSC 3		6.2.1

CSC 3		12.1.1
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 4		12.6.1
CSC 4		12.6.1
CSC 4		
CSC 4		
CSC 4		
CSC 4		
CSC 4		

CSC 7, CSC 18		12.6.1
CSC 20		18.2.1
CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013
CSC 17	§164.308(a)(5)(i)	18.1.1, 7.2.2
CSC 13	§164.316(b)(2)(iii)	18.1.1
CSC 17	§164.308(a)(2)	18.1.1
CSC 13		18.1.1
CSC 19	§164.308(a)(6)(i)	16.1.1

CSC 19	§164.308(a)(6)(ii)	16.1.2, 16.1.5, 18.1.1
CSC 13	§164.308(a)(1)(i)	
CSC 4	§164.308(a)(1)(i), §164.308(a)(1)(ii)(A)	
CSC 4	§164.308(a)(1)(ii)(B)	
CSC 16	§164.308(a)(5)(ii)(D)	9.4.3
CSC 16	§164.308(a)(5)(ii)(D)	9.4.3
CSC 16	§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)	9.4.3
CSC 16	§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)	9.4.3
CSC 16	§164.308(a)(4), §164.312(d)	9.4.3

CSC 16	§164.308(a)(4), §164.312(d)	
CSC 16	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	
CSC 16, 5	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	9.1.1
CSC 16	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	9.2.3
CSC 16	§164.308(a)(4), §164.312(a)(1)	9.2.3
CSC 6, CSC 16	§164.308(a)(4), §164.312(a)(1)	
CSC 6	§ 164.308(a)(1)(ii)(D)	12.4.1
CSC 6	§164.312(b)	12.4.1

CSC 6	§164.312(b)	12.4.1
CSC 6	§164.312(b)	12.4.1
CSC 6	§164.312(b)	12.4.1
CSC 10	§164.312(a)(2)(ii)	18.1.1
CSC 10	§164.308(a)(7)(i)	17.1.1
CSC 10	§164.308(a)(7)(i)	17.1.3
CSC 10	§164.308(b)(2)	18.1.1
CSC 10	§164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)	18.1.1
CSC 10	§164.308(a)(3)(i), §164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)	18.1.1
CIS Critical Security Controls v6.1		
HIPAA		
ISO 27002:2013		

CSC 10		18.1.1
CSC 10		18.1.1
CSC 10		18.1.1
CSC 1, CSC 2		
CSC 18		
CSC 10		

CSC 12, CSC 13		
CSC 10		

Version beta1.06b		
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
ID.GV-3	ID.GV-3	RA-2
		IA-2, IA-3, CM-3, SI-2
ID.AM-6, PR.AT-3	ID.AM-6, PR.AT-3	
PR.IP-9	PR.IP-9	AU-7, AU-9, IR-4
PR.IP-9	PR.IP-9	CA-5, PL-2
ID.GV-3	ID.GV-3	RA-2

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
		SA-9
		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9
		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9
		SA-9
		SA-9
ID.GV-3	ID.GV-3	SA-9
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4

		SA-3, SA-15, SC-2, PM-2, PM-10, SI-5,PM-3
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4

ID.AM-6, PR-AT-3	3.8.2	MP-2, RA-3
ID.AM-6, PR-AT-3	3.8.2	
ID.GV-3		PS-3
ID.AM-6, PR.AT-3		PS-5
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
ID.AM-6, PR.AT-3		

ID.AM-6, PR.AT-3	3.1.2, 3.1.3	AC-4
ID.AM-6, PR.AT-3	3.1.2	
ID.AM-6, PR.AT-3		
ID.AM-6, PR.AT-3		
ID.AM-6, PR.AT-3	3.8.2	MP-2
ID.AM-6, PR.AT-3	3.8.2	MP-2
ID.AM-6, PR.AT-3	3.1.2, 3.1.19, 3.8.2	MP-2
ID.AM-6, PR.AT-3		
ID.AM-6, PR.AT-3		

ID.AM-6, PR.AT-3		
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
ID.AM-5		
ID.AM-5		
PR.AC-4	3.1.1, 3.1.2, 3.1.7	AC-2, AC-3, AC-6
PR.AC-4, PR.PT-3	3.4.9	CM-11
PR.AC-4	3.1.2	
PR.AC-3, PR.MA-2	3.1.2	AC-17; NIST SP 800-46

PR.PT-3	3.1.12, 3.1.13, 3.1.14, 3.1.14, 3.1.15, 3.1.8, 3.1.20, 3.7.5, 3.8.2, 3.13.7	AC-3, CM-7; NIST SP 800-46
PR.PT-3		AC-17; NIST SP 800-46
ID.AM-2		
ID.AM-1, ID.AM-2, ID.AM-4		CA-9, SC-4

PR.AC-4, PR.PT-3	3.1.4	AC-5
PR.AC-4, PR.PT-3	3.1.1, 3.1.5, 3.1.6, 3.7.1, 3.7.2	AC-2, AC-3, AC-6, MA-2, MA-3
PR.DS-6		
		RA-2

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.AC-1	3.5.6	IA-4
PR.AC-1	3.5.7	IA-5(1)
PR.AC-1		
PR.AC-1	3.5.5, 3.5.8	IA-4
PR.AC-1	3.5.1	IA-2, IA-5
PR.AC-1		

PR.AC-1	3.5.10	IA-5(1)
PR.AC-1		
PR.AC-4	3.5.2, 3.5.3	IA-5
PR.AC-4	3.5.3, 3.7.5	IA-2(1,2,3)
PR.AC-1, PR.AC-4		
PR.AC-1, PR.AC-4		
PR.AC-1, PR.AC-4		
PR.AC-1, PR.AC-4		

PR.AC-1, PR.AC-4	3.1.1	
PR.PT-1	3.1.7, 3.3.1	AC-6(1,3,9), AU-2, AU-2(3), AU-3, AU-7, AU-9(4), AU-12, NIST 800-92
PR.PT-1	3.1.7, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.4.3, 3.7.1, 3.7.6, 3.10.4, 3.10.5	AU-2(3), AU-6, AU-12, AC-6(9), CM-3, MA-2, MA-5, PE-3
PR.PT-1	3.3.8, 3.3.9	AU-9
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34

PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.2.1, 3.2.2	AT-3, AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.IP-3	3.4.3, 3.4.4	CM-3, CM-4, CM-5
PR.IP-3, PR.DS-7	3.4.3, 3.4.4, 3.4.5	CM-3, CM-4, CM-5
		CM-3, CM-4, CM-5
		CM-3, CM-4, CM-5
		CM-3, CM-4, CM-5
		CM-3, CM-4, CM-5

		CM-3, CM-4, CM-5
PR.DS-6	3.4.4	CM-3, CM-4, CM-5
	3.14.4	CM-3, CM-4, CM-5
		CM-3, CM-4, CM-5
		CM-3, CM-4, CM-5
		CM-3, CM-4, CM-5
		CM-3, CM-4, CM-5

		CM-3, CM-4, CM-5
PR.IP-3		CM-3, CM-4, CM-5
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
ID.AM-3		
PR.AC-2, PR.IP-5	3.1.3, 3.8.1	AC-4, MP-2, MP-4
PR.AC-2, PR.IP-5	3.1.22	AC-22
PR.DS-2		
PR.DS-1	3.1.19, 3.8.1	MP-2, AC-19(5)
	3.8.6, 3.13.11	

PR.DS-2		PE-2, PE-3, PE-5, MP-5
	3.8.1	MP-2
	3.8.1	MP-2
	3.8.1	MP-2
	3.8.1	
	3.8.2	
	3.8.1	

PR.IP-4	3.8.9	CP-9
PR.IP-4	3.8.9	CP-9
PR.IP-4	3.8.9	CP-9
PR.DS-1, PR.IP-4	3.8.9	CP-9
PR.DS-1	3.8.6, 3.8.9	CP-9, MP-5
	3.13.10	SC-28, SC-13, FIPS PUB 140-2
ID.AM-1, ID.AM-2, PR.IP-9	3.8.9	CP-9
PR.IP-4	3.8.1, 3.8.9	CP-9
PR.IP-4	3.8.1, 3.8.5, 3.8.9	CP-9, MP-5

	3.8.9	CP-9, MP-5
PR.DS-3	3.7.1, 3.7.2, 3.8.3	CP-9 MP-6, NIST SP 800-60, NIST SP 800-88, AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2, MA-3, MP-6
PR.DS-3	3.7.3, 3.8.3,	AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2
PR.DS-3, ID.GV-3	3.7.3, 3.8.3,	SI-12, AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2
PR.DS-3	3.8.1, 3.8.2	AC-2, AC-6, IA-4, PM-2, PM-10, SI-5
ID.GV-3		
PR.AC-4		
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.DS-1		
PR.DS-1, PR.DS-2		

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.AC-2, PR.IP-5		
		AC-4
PR.AC-2		
PR.AC-2	3.8.1, 3.8.2	
PR.AC-5	3.1.3	

PR.DS-4		
PR.DS-4		
PR.DS-4		
		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14
PR.DS-4		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14

PR.DS-4		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34

PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34
PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34
	3.6.2	AC-5, CP-4, CP-10; NIST SP 800-34
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.DS-5		

PR.DS-5		
PR.AC-5		
PR.AC-5		
DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5
DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-6
DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-7
DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-8
	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-9
DE.CM-1, DE.CM-2, DE.CM-7	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-10
DE.CM-1, DE.CM-2, DE.CM-7	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-11
DE.AE-1, DE.CM-1, PR.PT-4	3.3.1	AU-2

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
DE.CM-7		
DE.CM-7		
DE.CM-7, PR.DS-2		
DE.CM-7, PR.DS-2	3.1.19	AC-19(5)
DE.CM-7, PR.DS-1		
DE.CM-7		

DE.CM-7, DE.CM-8, ID.RA-1		
DE.CM-7, DE.CM-8, ID.RA-1		
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.AC-2, PR.AT-5, PR.IP-5, DE.CM-2	3.8.2, 3.10.1, 3.10.2, 3.10.5, 3.10.6, 3.12.1	MP-4, PE-2, PE-5, PE-6, PE-17
PR.AC-2, PR.AC-4, PR.DS-1, PR.DS-3, PR.DS-5	3.8.1, 3.8.5, 3.8.7	MP-2, MP-5, MP-7
DE.CM-2	3.10.2	PE-6
DE.CM-2	3.10.2	PE-6
PR.DS-3	3.7.3, 3.8.1, 3.8.5, 3.8.7, 3.10.3	MP-2, MP-5, MP-7
PR.DS-3	3.7.3, 3.8.7, 3.10.3	MP-2, MP-5, MP-7, PE-3
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4

ID.GV-2	3.9.1, 3.9.2	PM-2, PM-10, SI-5, CA-5, PM-1
PR.IP-12		CA-5, PM-1
		CA-5, PM-1
		CA-5, PM-1
		CA-5, PM-1
DE.CM-8, RS.MI-3		CA-5, PM-1
PR.DS-7	3.12.2	CA-5, PM-1
	3.13.2	CA-5, PM-1

PR.IP-2		CM-3, SA-15, SA-3, SA-8, SC-2, CA-5, PM-1
PR.IP-2		CM-3, SA-15, SA-3, SA-8, SC-2, CA-5, PM-1
PR.IP-9	3.6.1, 3.12.2	CA-5, PM-1, IR-4, IR-5, IR-7, IR-8
ID.GV-3	3.6.2,	CA-5, PM-1, IR-4, IR-5, IR-6, IR-7, IR-8
	3.6.2	CA-2, SA-15, CA-5, PM-1, IR-4, IR-5, IR-6, R-7, IR-8
ID.GV-3		CA-5, PM-1
PR.IP-11	3.9.1	CA-5, PM-1, PS-3
PR.IP-11		CA-5, PM-1
PR.IP-11		CA-5, PM-1
ID.GV-3		CA-5, PM-1

PR.AT-1	3.2.1	AT-2, CA-5, PM-1
PR.AT-1	3.2.1, 3.2.2, 3.2.3	AT-2, AT-3, CA-5, PM-1
PR.AT-1		CA-5, PM-1
PR.AC-4, PR.PT-3	3.1.7	CA-5, PM-1
		CA-5, PM-1, PS-4, PS-5, PE-2, PE-3, PE-5, AC-6, RA-3, SA-8, CA-2, NIST SP 800-37; NIST SP 800-39; NIST SP 800-115; NIST SP 800-137
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.DS-7		
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4

NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
PR.PT-4	3.1.3	AC-4
PR.IP-1	3.4.1, 3.4.2, 3.4.3	CM-2, CM-3, CM-6, CM-8
	3.13.13	

PR.IP-1, PR.IP-2	3.1.18, 3.7.1, 3.13.13	CM-2, CM-6, CM-3, AC-19, MA-2
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2
DE.CM-8		SI-2
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2
DE.CM-8		SI-2

ID.RA-1, DE.CM-8, PR.IP-12	3.11.1, 3.11.2, 3.11.3, 3.14.2	SI-2
DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4
ID.GV-3	3.2.2	AT-3
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3	3.6.1, 3.14.1	IR-2, IR-4, IR-5, IR-7

ID.GV-3	3.6.2, 3.12.2	IR-6
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3	3.5.6	IA-4
ID.GV-3	3.5.9	IA-5(1)
ID.GV-3	3.1.8	AC-7
ID.GV-3	3.1.10, 3.1.11	AC-11, AC-11(1), AC-12
ID.GV-3	3.5.10	IA-5(1)

ID.GV-3		
ID.GV-3	3.1.2	
ID.GV-3	3.1.2, 3.1.5	
ID.GV-3	3.1.2	
ID.GV-3		
ID.GV-3	3.3.1	AU-2, AU-6, AU-12
ID.GV-3	3.3.2	AU-3
ID.GV-3		

ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3	3.12.2	
ID.GV-3	3.6.3, 3.12.2	
ID.GV-3		
ID.GV-3		
ID.GV-3		
NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4

ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3		
ID.GV-3		

ID.GV-3		
ID.GV-3		

Acknowledgments

The Higher Education Information Security Council Shared Assessments Working Group cc vision and significant talents to the conception, creation, and completion of this resource.

Members that contributed to Phase II (2017) of this effort are:

- Jon Allen, Baylor University
- Samantha Birk, IMS Global Learning Consortium
- Jeff Bohrer, IMS Global Learning Consortium
- Sarah Braun, University of Colorado - Denver
- David Cassada, University of California - Davis
- Matthew Dalton, University of Massachusetts Amherst
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Todd Herring, REN-ISAC
- Kolin Hodgson, University of Notre Dame
- Tom Horton, Cornell University
- Leo Howell, North Carolina State University
- Alex Jalso, West Virginia University
- Nick Lewis, Internet2
- Wyman Miles, Cornell University
- Kim Milford, REN-ISAC
- Valerie Vogel, EDUCAUSE

Members that contributed to Phase I (2016) of this effort are:

- Jon Allen, Baylor University
- John Bruggeman, Hebrew Union College, Jewish Institute of Religion
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Karl Hassler, University of Delaware
- Todd Herring, REN-ISAC
- Nick Lewis, Internet2
- Kim Milford, REN-ISAC
- Craig Munson, Minnesota State Colleges & Universities
- Mitch Parks, University of Idaho
- Laura Raderman, Carnegie Mellon University
- Valerie Vogel, EDUCAUSE

Contributed their

ADDENDUM 1

DATE: January 10, 2019
PROJECT: Event Management Software
RFP NO: 720-1904
OWNER: The University of Texas System Administration
TO: Prospective Bidders

This Addendum forms part of Contract Documents and modifies Bid Documents dated October 5th, 2018 with amendments and additions noted below.

Questions and Answers:

1. Question: Are there other forms/appendices to be downloaded with the RFP? I cannot find them on the website.

Answer: There are three (3) documents to download from the website – RFP document, sample agreement, and HECVAT questionnaire.

2. Question: Do you prefer a custom-made solution (made from scratch) or an “off-the-shelf” / “out-of-the-box” platform?

Answer: “Off-the-shelf” / “out-of-the-box” platform.

3. Question: Does this solution require/demand the vendor to host it or can the University host the solution?

Answer: Vendor to host.

4. Question: Is there an approved budget for this project?

Answer: UT System will not be sharing any budget-related information. We invite the vendors to provide best price for the solution that fits our needs (SOW).

5. Question: If yes to the above, what is the amount of the approved budget?

Answer: See previous answer.

6. Question: We are a U.S based company with office across the globe. With that said, will you accept offshore development services for this project?

Answer: If off-the-shelf, should not be any development services.

7. Question: If you are seeking development, will onsite visits be required during development?

Answer: *N/A.*

8. Question: If you are seeking full development, how should we answer the chart in Section 5.4 if the system has not yet been developed?

Answer: *N/A.*

9. Question: Is there an incumbent competing? Is there an internal team currently working on the development, or are you outsourcing current development?

Answer: *N/A.*

10. Question: When is the anticipated award date?

Answer: *Mid to late November.*

11. Question: When are you expecting to engage with the vendor after the award has been given?

Answer: *Agreement negotiations will start right after the award is made.*

12. Question: When is the expected/needed “go-live” date of the project?

Answer: *TBD.*

**13. Question: To the best of your knowledge, are there any circumstances that will cause you to:
Cancel the RFP?**

Answer: *No proposals received.*

Not move forward with the winning bidder?

Answer: *No.*

Lower the budget for the project?

Answer: *N/A.*

Prolong the evaluation process or reissue the RFP?

Answer: *No proposals.*

14. Question: Are there any other systems (IE: AMS, CRM, etc) you would like to integrate with that are not listed on this RFP? If so, what are the potential systems?

Answer: *UT System does have a preference for a software to integrate with customer relation management (CRM) software, but it is not a requirement.*

15. Question: PCI compliance:

I assume UT has a mandate to have all possible ecommerce transactions related to event have to be PCI level 1 compliant, however I didn't see language specially in the documents. Can you confirm that to be true? Also, will your treasury departments will be issuing separate guidance around ecommerce transitions at a later date?

Answer: *The RFP does address PCI. It's included in Section 5.3, number 3, letter c.*

UT System expects vendors to provide software / platforms including any hosted environments to be compliant with current / applicable Payment Card Industry (PCI) standards including applicable attestations of compliance (e.g., as a service provider, validated payment application, etc.). UT System has policies and practices that require UT merchants/departments to adhere to the same PCI standards for merchants. Compliance will be in accordance with PCI standards as well as the applicable merchant processing gateway used, transactions/events and appropriate PCI compliance level.

END OF ADDENDUM 1