Texas Comptroller of Public Accounts
Glenn Hegar

ehaynes Account

Contracts

SPD Applications

TSB Help

Solicitation Notice

Print

Thank you for using the ESBD, your bid solicitation entry is now complete

Status: Posted

Solicitation ID:720-1923

Solicitation Title: Third-Party Vendor Risk Rating & Scoring Services

Modify Solicitation

Agency/Texas SmartBuy Member Name: University Of Texas System - 720

Posting Requirements: 21+ Days for Solicitation Notice

Solicitation Posting Date: 7/17/2019

Internal Notes

Response Due Date:8/14/2019

Response Due Time: 2:30 PM

Cancel Solicitation

Solicitation Description: UT System Administration is soliciting proposals in response to this Request for Proposal for Selection of a Vendor to Provide Services related to Cyber Security Risk Scoring and Rating of Third-Party Information Technology service providers.

Class/Item Code: 20529-*Data/File Security Hardware/Software, To Include Encryption, Environmentally Certified Products

Published Details Internal Notes

Record Attachments

#	Name	Description
1	ESBD_File_167417_LINK - RFP 720-1923 Third-Party Vendor Risk Rating and Scoring Services.docx	Download the attached Bonfire submittal instructions to find the link to the project in Bonfire.

Texas Comptroller of Public Accounts
Glenn Hegar

- Home
- Contact Us

POLICIES

- Privacy and Security Policy
- Accessibility Policy
- Link Policy
- Texas.gov
- Search from the Texas State Library
- Texas Homeland Security
- Texas Veterans Portal
- Public Information Act
- Texas Secretary of State
- HB855 Browser Statement

OTHER STATE SITES

- texas.gov
- Texas Records and Information Locator (TRAIL)
- State Link Policy
- Texas Veterans Portal

REQUEST FOR PROPOSAL

RFP No. 720-1923 Third-Party Vendor Risk Rating and Scoring Services

Proposal Submittal Deadline: August 14, 2019 at 2:30 PM CST

The University of Texas System
Information Security Office

Prepared by:
Erica Haynes
The University of Texas System
210 West 7th Street
Austin, Texas 78701-2982
July 16, 2019

REQUEST FOR PROPOSAL

TABLE OF CONTENTS

Attachments:

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 University of Texas System ("UT System") is currently made up of system administration offices located in Austin, Texas ("UT System Administration"), eight academic institutions, six standalone health institutions collectively referred as "**UT Institutions**", and the University of Texas/Texas A&M Investment Management Company "**UTIMCO**." UT System is one of the nation's largest providers of higher education with more than 221,000 students and an FY2018 operating budget of $17.9

billion. UT System Administration is charged with overseeing policies and operations while supporting UT System's Board of Regents and Chancellor.
UT System Office of Information Security Office (ISO) within the UT System provides guidance and support to each UT Institution including efforts to:

- effectively reduce risk and secure the information assets under its stewardship against unauthorized use, disclosure, modification, damage or loss;
- are documented and verifiable; and
- meet regulatory compliance requirements.

1.3 Objective of Request for Proposal

The University of Texas System is soliciting proposals in response to this Request for Proposal No.720-1923 (this "**RFP**"), from qualified vendors to provide Third-Party Vendor Risk Rating and Scoring Services (the "**Services**") 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 August 14, 2019 (the "**Submittal Deadline**").

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. Vendor Experience (10%);
C. System Security (20%);
D. System Functionality (40%).

2.4 Key Events Schedule

Issuance of RFP	July 16, 2019
Pre-Proposal Conference (ref. **Section 2.6** of this RFP)	10:30am CST on July 31, 2019
Deadline for Questions / Concerns (ref. **Section 2.2** of this RFP)	August 6, 2019
Submittal Deadline (ref. **Section 2.1** of this RFP)	2:30 p.m. CST on August 14, 2019

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.

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". **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 submit the question via Bonfire portal.

Proposer must complete the HSP, then print, sign and scan *all pages* of the HSP Option selected, with additional support documentation*****, ***and submit via Bonfire portal***. 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 as non-responsive due to material failure to comply with advertised specifications.

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 Bonfire portal*** may result in University's rejection of the proposal as non-responsive due to material failure to comply with advertised specifications.

***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 Bonfire Portal**. **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 Call

University will hold a pre-proposal call at 10:30 a.m. CST on July 31, 2019.

Call-in number: (877)226-9790

Participant Code: 6269693#

SECTION 3

SUBMISSION OF PROPOSAL

3.1 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.

3.2 Terms and Conditions

3.2.1 Proposer must comply with the requirements and specifications contained in this RFP, including the Terms and Conditions (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:

3.2.1.1. Specifications and Additional Questions (ref. **Section 5** of this RFP);

3.2.1.2. Terms and Conditions (ref. **Section 4** and **APPENDIX TWO**);

3.2.1.3. Proposal Requirements (ref. **APPENDIX ONE**);

3.2.1.4. Notice to Proposers (ref. **Section 2** of this RFP).

SECTION 4

GENERAL TERMS AND CONDITIONS

Attached terms and conditions (ref. **APPENDIX TWO**) or, in the sole discretion of University, terms and conditions substantially similar to those contained in **APPENDIX TWO**, 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. Proposer's exceptions 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.

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 an initial three (3) year base term, with the option to renew for two (2) additional one (1) year renewal periods, upon mutual written agreement of both parties.

Disclosure of Existing Agreement: University has an existing Third-Party Vendor Risk Rating and Scoring Services agreement with Security Scorecard, which is scheduled to expire August 31st, 2019.

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 (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**).

5.2.4 By signing the Execution of Offer (ref. **Section 2** of **APPENDIX ONE**), Proposer agrees to comply with Certificate of Interested Parties laws (ref. §2252.908, *Government Code*) and 1 TAC §§46.1 through 46.5) as implemented by the Texas Ethics Commission ("**TEC"**), including, among other things, providing TEC and University with information required on the form promulgated by TEC and set forth in **APPENDIX FIVE**. *Proposer may learn more about these disclosure requirements, including applicable exceptions and use of the TEC electronic filing system, by reviewing* §2252.908, *Government Code*, *and information on the TEC website at* https://www.ethics.state.tx.us/data/forms/1295/1295.pdf. **The Certificate of Interested Parties must only be submitted by Contractor upon delivery to University of a signed Agreement.**

5.3 Scope of Work

Contractor will provide the following services to University:

UT System Administration is soliciting proposals in response to this Request for Proposal for Selection of a Vendor to Provide Services related to Cyber Security Risk Scoring and Rating of Third-Party Information Technology service providers. Proposed Services must include those listed below; however, they are not limited by this list and *should only be considered minimum requirements*. Any additional Services proposed that do not appear on the list below must be justifiable and cost-efficient for the University's environment:

1. Effective, data-driven Third-Party Vendor risk rating and scoring against a set of collected data points including a measure of the vendor's cyber security strength and security reputation.
2. Security Risk Profile for each Third-Party vendor that contain at a minimum the associated scores or ratings for the collected data points at the IP level with associated vulnerability remediation recommendations.
3. Performance Metrics including the ability to "drill down" into all supporting evidence.
4. Current and historical performance trends of Third-Party Vendors including industry or peer performance benchmarking.
5. Continuous, or ongoing, monitoring of the Third-Party vendor for technology risk using both public and private resources.
6. Provide the ability to segregate UT Institution specific data or Third-Party vendor information into portfolios.
7. Present a consolidated and summary view for each Institution and a combined summary view of all institutions.
8. Federated access to all 14 UT Institutions including UTIMCO.
9. Secure and stable Application Programming Interface for integration into popular data analysis tools such as Splunk and ELK.
10. Customizable alerting capabilities linked to changes in Third-Party Vendor's rating or scoring.
11. Flexible and robust reporting capabilities.

5.4 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 Proposer Proposer’s organization’s business background and ownership structure, including all parent and subsidiary relationships.

4. Describe Proposer Proposer’s Business Continuity, Disaster Recovery Plans, and Incident Response Plans.

5. Identify the review and testing frequency for the Business Continuity Plan/Disaster Recovery and Incident Response plans.

6. Describe Proposer Proposer’s Incident Response Plan.

7. Has Proposer company experienced a data breach within the past five (5) years? Explain.

8. Does Proposer’s company offer a dedicated account manager? If yes, identify and provide a resume.

9. Does Proposer provide training and detailed software, database, and process manuals? If yes, explain.

System Security (20%)

10. Provide a copy of the Cloud Security Alliance self-assessment or CAIQ.
11. Have you received the Cloud Security Alliance STAR certification? If so, state the date.
12. Does Proposer conform to a specific security framework? (NIST CSF, ISO 27001, etc.).
13. Does Proposer implement and follow secure coding practices?
14. Does Proposer have a data privacy policy?
15. Does Proposer have a FEDRAMP certification?
16. Describe Proposer Information Security Program and team.
17. Describe Proposer process for including application security into the SDLC.
18. Describe the user authentication methodology.
19. Does the application support integration with Shibboleth?
20. Describe the application user access control mechanisms.
21. Describe Proposer user password aging policy and implementation
22. Does the application audit user logins and user actions?
23. Describe Proposer notification process for preventive maintenance outages.
24. Describe Proposer notification process for operational malfunctions and outages.
25. Is sensitive data encrypted at rest, in process, and in transit?
26. Describe the segmentation and protection mechanisms of client data in the data stores.
27. Identify the geographical locations of the data stores.
28. Does the hosting provider have a SOC 2 Type 2 report available for review?
29. Does Proposer company own the physical data center?
30. Does Proposer conduct periodic vulnerability scanning? If so, identify the frequency.

31. Have Proposer had an independent 3rd party vulnerability scan within the last 12 months? If so, provide a copy of results.
32. Are there hard-coded passwords or undocumented features embedded in the code modules?
33. Describe Proposer's patch management and emergency change programs.
34. Describe Proposer's integration of the vulnerability scanning with Proposer ticketing system and software change control processes.

System Functionality (40%)

35. Describe how Proposer's solution tracks the security of third party vendors.
36. Describe how the solution can be used to track our own environment for cyber-risk.
37. What capabilities does Proposer solution offer to collect and analyze relevant security data and threat intelligence?
38. How does Proposer solution normalize data gathered from external sources and deep web / dark channels?
39. Identify the data sources or services used to assess the security of a third-party vendor?
40. How does Proposer solution build and maintain an accurate profile of a third-party vendors' cyber-risk profile and digital footprint?
41. Describe Proposer's rating methodology for measuring and scoring a vendor's cyber-risk exposure?
42. How does Proposer solution correlate real-life cyber-risk exposure and events that may trigger a change in scoring?
43. Describe how Proposer solution supports an organization's third-party vendor management program?
44. Describe how Proposer solution integrates additional risk context data about third-parties with internal security and risk data?
45. Describe how Proposer solutions integrates with external systems such as SEIMs, GRC platforms, etc.?
46. Describe how Proposer solution provides enterprise non-cybersecurity risk context data about third parties (e.g., financial, reputational, and regulatory?
47. Describe how Proposer application sets alerting thresholds to changes in vendor security ratings? Are these alerting thresholds configurable by the customer? How are customer's informed of changes to a given vendor's security risk profile?
48. Describe how Proposer can partition security ratings of a vendor, if the vendor uses hosting service like AWS or Azure? Can Proposer solution provide security ratings of a sub-domain or range of IP addresses of a given vendor?

49. Does Proposer solution provide a way to integrate with an external system via an API? is this included in the pricing of the base product or is it an additional cost?
50. Describe the pre-defined and customizing report functions of the application.
51. Describe the pre-defined and customizing dashboard functions of the application
52. Does Proposer solution allow vendors to provide input or feedback on their vendor security risk score? If yes, describe how Proposer solution incorporates vendor feedback into overall risk rating of the vendor? How quickly does the feedback or input get incorporated into a vendor’s security score?
53. Does Proposer solution provide recommendations to vendors on how to mitigate security issues uncovered and/or provide action steps? Does Proposer solution prioritize what actions a vendor should take to improve their security posture?
54. How frequently does Proposer solution perform assessments or scans of a given vendor’s environment? How quickly is this new information incorporated in the vendor security risk score?
55. What steps has Proposer company taken to validate the efficacy of Proposer security rating methodology?
56. Describe the operational administration practices of the application. Can multiple people be assigned as administrators to manage access to the application? What can administrators do that a non-administrator of the application cannot?
57. Does Proposer solution provide the capability to create collections of third party vendors? Can an overall risk rating be formed of vendor’s in the portfolio? Describe Proposer process for entering, updating, and deleting vendors into the portfolio.
58. Does Proposer solution check to see if a vendor has been previously added?
59. Is Proposer able to provide an on-demand security risk assessment of a given vendor?
60. Is Proposer able to provide on on-demand external security vulnerability scan?
61. Is Proposer able to provide a history of security event detail which triggered a change in each vendor’s security score? How far back in time is that history available?
62. If the vendor experiences a security breach will Proposer solution provide or collect information regarding that breach? Can Proposer solution weight the risk of a prior breach in a security risk score?
63. Can Proposer solution provide an alert regarding a change in digital internet footprint? Can you provide a history of devices, ports, and services that are externally accessible?
64. Can Proposer solution provide an insight / topology of what is being scanned in our organization’s network? what devices are being scanned? What IP ranges / domain / subdomain are being scanned? When was the scan completed? When is the next scan scheduled to begin?

65. How many risk and threat analysts are dedicated to ongoing risk analysis and threat intelligence activities?
66. Identify the application deployment platform. Meaning is it a SAAS or a web-based application not cloud-based?
67. Describe the supporting system, data repository, and network platforms.
68. Describe the application architecture.
69. Identify the location of the hosting platform and the owner.
70. Describe how the Institution data will be segregated from other clients.
71. Describe Proposer Software Configuration Management practices and Change Control.
72. Identify the web browsers and versions the application supports
73. Describe Proposer notification process for software updates.
74. If the application uses open source programs, identify the programs or modules.
75. Describe any non-API external application / system interfaces and their function.
76. Describe the Application Programming Interfaces, if the API is secure, and the interfacing system(s).
77. Identify if the application is hosted in a single or multi-tenant environment.
78. Does Proposer architecture include a Web Application Firewall? If so, does it check for SQL Injections, Cross-Site Scripting, and other web attacks?
79. Does the system architecture include an IDS or IS?
80. Does the company monitor for intrusions on a 24X7 basis? If no, identify the company that provides this service.
81. Does the company hire sub-contractors or consultants for application development or system administration?
82. Does the company hire or use off-shore sub-contractors for application development or system administration?
83. 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.
84. Identify the application deployment platform. Meaning is it a SAAS or a web-based application not cloud-based?
85. Describe the supporting system, data repository, and network platforms.
86. Describe the application architecture.
87. Identify the location of the hosting platform and the owner.
88. Describe how the Institution data will be segregated from other clients.
89. Describe Proposer Software Configuration Management practices and Change Control.
90. Identify the web browsers and versions the application supports
91. Describe Proposer notification process for software updates.

92. If the application uses open source programs, identify the programs or modules.

93. Describe any non-API external application/system interfaces and their function.

94. Describe the Application Programming Interfaces, if the API is secure, and the interfacing system(s).

95. Identify if the application is hosted in a single or multi-tenant environment.

96. Does Proposer architecture include a Web Application Firewall? If so, does it check for SQL Injections, Cross-Site Scripting, and other web attacks?

97. Does the system architecture include an IDS or IS?

98. Does Proposer monitor for intrusions on a 24X7 basis? If no, identify the company that provides this service.

99. Does Proposer hire sub-contractors or consultants for application development or system administration?

100. Does Proposer hire or use off-shore sub-contractors for application development or system administration?

101. 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.

SECTION 6

PRICING AND DELIVERY SCHEDULE

Proposal of: ___________________________________
(Proposer Company Name)

To: The University of Texas System

RFP No.: 720-1923 Third-Party Vendor Risk Rating and Scoring Services

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 Pricing for Services Offered (30%)

Provide a fee per slot, per year.

Number of Slots	Fee (Per Slot, Per Year)
1 - 100	
101 - 200	
201 - 300	
301 - 400	
401 - 500	
501 - 600	
601 - 700	
701 - 800	
801 - 900	
901 - 1,000	

6.2 Discounts

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

6.3 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

6.4 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

1.1 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 Agreement 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.: 720-1923 Third-Party Vendor Risk Rating and Scoring Services

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.: Third-Party Vendor Risk Rating and Scoring Services

RFP No.: 720-1923

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

HECVAT

(INCLUDED AS SEPARATE ATTACHMENT)

AGREEMENT BETWEEN UNIVERSITY AND CONTRACTOR

This Agreement between University and Contractor (**"Agreement"**) is made and entered into effective _______, 2019, (the **"Effective Date"**), by and between **The University of Texas System**, an agency and institution of higher education established under the laws of the State of Texas (**"University"**), for and on behalf of each of the fourteen University of Texas System institutions and The University of Texas System Administration (collectively, "Institutions" and each an "Institution" or "University", and ______________________ having Federal Tax Identification Number __________________ (**"Contractor"**).

1. Scope of Work

Contractor will perform services within the scope of work (**"Work"**) set forth in **Exhibit A**, Scope of Work, attached and incorporated for all purposes, only on the request of a University of Texas System Institution (the "Requesting Institution"), including the following: The University of Texas at Arlington, The University of Texas at Austin, The University of Texas at Dallas, The University of Texas at El Paso, The University of Texas at Permian Basin, The University of Texas at Rio Grande Valley, The University of Texas at San Antonio, The University of Texas at Tyler, The University of Texas Southwestern, The University of Texas Medical Branch Galveston, The University of Texas Health Houston, The University of Texas Health San Antonio, The University of Texas MD Anderson, The University of Texas Health Tyler. Time is of the essence in connection with this Agreement and each Order Form. University and the Requesting Institution will have no obligation to accept late performance or waive timely performance by Contractor.

Prior to Contractor's commencement of any services, the Contractor and the Requesting Institution must complete and enter into an Order Form. Each Institution shall purchase services via a separate Order Form. All of the terms and conditions contained in this Agreement are incorporated into each Order Form for all purposes.

2. Term

The term (Initial Term) of this Agreement will begin on the Effective Date and expire on ____________________. University will have the option to renew this Agreement for two (2) additional one (1) year terms (each a Renewal Term). The Initial Term and each Renewal Term are collectively referred to as the Term.

3. Payment.

University will pay Contractor for the performance of Services in accordance with **Exhibit C**, Payment for Services, beginning at the time each institution implements and launches the Services. The Parties acknowledge and agree that no fee shall be due from UT Institutions until they begin participation in the Services under this Agreement.

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.

Fees are due and payable as per the terms of this Agreement in compliance with **Exhibit B**, Order Form.

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 and each Participating Institution in writing on Contractor letterhead signed by an authorized representative of Contractor. Prior to the first payment, University and each Participating Institution will confirm Contractor's banking information. Changes to Contractor's bank information must be communicated to University and each Participating Institution in accordance with Section 20 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.

4. Tax Exemption. 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.

5. Contractor's Obligations.

5.1 Contractor will perform Work in compliance with (a) all federal, state or local, laws, statutes, regulations and ordinances (collectively, **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) the policies of The University of Texas System (http://www.utsystem.edu/board-of-regents/policy-library); and the applicable institutional rules, regulations and policies of University (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.

5.2 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

5.3 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.

5.4 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.

5.5 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.

5.6 Contractor will maintain a staff of properly trained and experienced personnel to ensure satisfactory performance under this Agreement. Contractor will assign to the Project a designated representative who will be responsible for administration and coordination of Work.

5.7 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.

5.8 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 and Requesting Institution); (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.

6. ***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.

7. **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.

8. **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.

9. **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.

Performance by University and the UT Institutions under the Order Forms that University and the UT Institutions enter into with Contractor under this Agreement may be dependent upon the appropriation and allotment of funds by the Texas State Legislature (the "Legislature") and/or allocation of funds by the Board of Regents of The University of Texas System (the "Board"). If the Legislature fails to appropriate or allot the necessary funds for an Order Form, or if the Board fails to allocate the necessary funds for an Order Form (a "Non-Funded Order Form") then University or the UT Institution that is a party to that Non-Funded Order Form shall issue written notice to Contractor and University or the UT Institution may terminate their further participation under the Non-Funded Order Form without further duty or obligation under that Order Form. Provided, however, that such termination of a Non-Funded Order Form shall not terminate or otherwise affect any other Order Forms entered into under this Agreement. Contractor acknowledges that appropriation, allotment, and allocation of funds are beyond the control of University and the UT Institutions.

10. **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:

UT System Administration
Office of Information Security
210 W 7th St, Austin, TX 78701
Attention: Al Arboleda, Assistant Chief Information Security Officer
Email: aarboleda@utsystem.edu

with copy to:

Dr. Scott Kelley. Ed.D.
Executive Vice Chancellor for Business Affairs
210 W 7th St, Austin, TX 78701

If to Contractor:

____
____
____

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

Notwithstanding any other requirements for notices given by a party under this Agreement, if Contractor intends to deliver written notice to University pursuant to §2251.054, *Texas Government Code*, then Contractor will send that notice to University as follows:

If to UT System:

UT System Administration
Office of Information Security
210 W 7th St, Austin, TX 78701
Attention: Al Arboleda, Assistant Chief Information Security Officer
Email: aarboleda@utsystem.edu

with copy to: Dr. Scott Kelley. Ed.D.
Executive Vice Chancellor for Business Affairs
210 W 7th St, Austin, TX 78701

or other person or address as may be given in writing by University to Contractor in accordance with this Section.

11. **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. **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.

13. **Breach of Contract Claims.**

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:

13.1. 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.

13.2 If the parties are unable to resolve their disputes under **Section 13.1** 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.

13.3 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.

13.4 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.

13.5 University and Contractor agree that any periods provided in this Agreement for notice and cure of defaults are not waived.

14. **Records.** Records of Contractor's costs, reimbursable expenses pertaining to the Work and payments will be available to University and Requesting Institution or its authorized representative during business hours and will be retained for four (4) years after final payment or abandonment of the Work, unless University and Requesting Institution otherwise instructs Contractor in writing.

15. Insurance.

15.1 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:

15.1.1 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. of the information page of the Workers' Compensation policy the state in which Work is to be performed for University.

15.1.2 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.

15.1.3 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 15.1.1** Employer's Liability; **15.1.2** Commercial General Liability.

15.1.4 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.

15.1.5 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 a period of two (2) years beyond the termination or expiration of the Term.

Contractor’s policy will provide a carve-back to the “Insured versus Insured” exclusion for claims brought by or on behalf of additional insureds.

15.2 Contractor will deliver to University:

15.2.1 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.

15.2.1.1 ***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.

15.2.1.2 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 15**.

15.2.1.3 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.

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

Name: Al Arboleda
Address: 210 W 7th St, Austin, TX 78701
Email Address: aarboleda@utsystem.edu

15.3 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

16. Indemnification.

16.1 To the fullest extent permitted by Applicable Laws, a party to this Agreement or to an Order Form (the "Indemnifying Party") will and does hereby agree to indemnify, protect, defend with counsel approved by the other party to this Agreement or to an Order Form (the "Indemnified Party"), and hold harmless the Indemnified party**,** and its respective affiliated institutions, enterprises, regents, officers, directors, attorneys, employees, representatives, successors, assigns, licensees, 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 the Indemnifying Party's breach of this Agreement or of an Order Form and that are caused in whole or in part by any negligent act, negligent omission or willful misconduct of the Indemnifying Party, anyone directly employed by the Indemnifying Party or anyone for whose acts the Indemnifying Party 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.

16.2 In addition, the Indemnifying Party will and does hereby agree to indemnify, protect, defend with counsel approved by the Indemnified party, 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 the Indemnifying Party, or the use by Indemnitees, at the direction of the Indemnifying Party, of any article or material; provided, that, upon becoming aware of a suit or threat of suit for infringement, the Indemnified party will promptly notify the Indemnifying Party and the Indemnifying Party will be given the opportunity to negotiate a settlement. In the event of litigation, the Indemnified Party agrees to reasonably cooperate with the Indemnifying party. All parties will be entitled to be represented by counsel at their own expense.

16.3 Notwithstanding the above, University will only be bound and obligated under this Section 16 to the extent authorized by the laws and Constitution of the State of Texas.

17. 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.

Further, Contractor agrees to comply with §2252.908, *Texas Government Code* (**Disclosure of Interested Parties Statute**), and 1 TAC §§46.1 through 46.5 (**Disclosure of Interested Parties Regulations**), as implemented by the Texas Ethics Commission (**TEC**), including, among other things, providing the TEC and University and UT Institutions with information required on the form promulgated by TEC. Contractor may learn more about these disclosure requirements, including the use of TEC's electronic filing system, by reviewing the information on TEC's website at https://www.ethics.state.tx.us/whatsnew/FAQ_Form1295.html.

18. 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 25**. 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.

19. **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 Services during the occurrence.

20. **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.

21. **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.

22. **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.

23. **Ownership and Use of Work Material**.

23.1 All data, documentation, screenshots, tapes, renderings, models, publications, statements, accounts, reports, studies, and files produced by Contractor as a result of its Services and other materials prepared in connection with 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.

23.2 Contractor grants and assigns to University all rights and claims of whatever nature and whether now or hereafter arising in and to 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 Work Material.

23.3 Contractor will deliver all Work Material to University upon expiration or termination of this Agreement. University will have the right to use Work Material for the completion of Work or otherwise. University may, at all times, retain the originals of Work Material. Work Material will not be used by any person other than University on other projects unless expressly authorized by University in writing.

23.4 Identifiable 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.

23.5 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 of Contractor IP. Contractor grants University and the UT Institution a non-exclusive, worldwide, royalty-free license to use Contractor IP in connection with the Work and Contractor's services related to the Work. "**Contractor IP**" means all tools, software and programs owned by Contractor (licensed to Contractor by a third party licensor) that (1) existed prior to the Effective Date and the commencement of the Work; (2) are not related to the Work or to Contractor's services in connection with the Work; or (3) were created by Contractor (or its licensor) totally separate from the Work or Contractor's services in connection with the Work.

23.6 University grants Contractor a non-exclusive, worldwide, perpetual, irrevocable, sub-licensable, royalty-free license to the Work Product Improvements to Contractor IP. "**Work Product Improvements to Contractor IP**" means Work Material comprising an improvement, enhancement or modification to

Contractor IP, whether or not patentable, copyrightable as a derivative work, or otherwise protectable as intellectual property.

24. **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 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 UTS165 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.

24.1 **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.

24.2 **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, notwithstanding the foregoing, Contractor may retain one (1) copy of all University data in a randomized, anonymized format for its own business purposes and record-keeping obligations.

24.3 **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 24.3**.

24.4 **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.

24.5 **Public Information.** University and UT Institutions 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 and UT Institutions, Contractor will make any information created or exchanged with University and UT Institutions pursuant to this Agreement (and not otherwise exempt from disclosure under TPIA) available in a format reasonably requested by University and UT Institutions that is accessible by the public**.**

24.6 **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.

24.7 **Duration.** The restrictions and obligations under this Section will survive expiration or termination of this Agreement for any reason.

25. Default and Termination

25.1 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.

25.2 Termination under **Sections 25.1** will not relieve Contractor from liability for any default or breach under this Agreement or any other act or omission of Contractor.

25.3 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.

25.4 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.

26. Binding Effect. This Agreement will be binding upon and inure to the benefit of the parties hereto and their respective permitted assigns and successors.

27. 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.

28. Limitation of Liability. IN NO EVENT SHALL ANY PARTY OR ITS SUBSIDIARIES, AFFILIATES, SHAREHOLDERS, DIRECTORS, OFFICERS OR EMPLOYEES BE LIABLE UNDER THIS AGREEMENT TO THE OTHER FOR INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL, STATUTORY, PUNITIVE, OR EXEMPLARY DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST SAVINGS AND LOST REVENUES, LOSS OF USE, LOSS OF TIME, SHUTDOWN OR SLOWDOWN COSTS, INCONVENIENCE, LOSS OF BUSINESS OPPORTUNITIES, EMOTIONAL HARM, DAMAGE TO GOOD WILL OR REPUTATION, OR OTHER ECONOMIC LOSS, REGARDLESS OF WHETHER SUCH LIABILITY IS BASED ON BREACH OF CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, AND EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR SUCH DAMAGES COULD HAVE BEEN REASONABLY FORESEEN. IN NO EVENT SHALL PROCTORU'S AGGREGATE LIABILITY TO THE OTHER PARTIES OR ANY THIRD PARTY UNDER THIS AGREEMENT FOR ANY CAUSE ACTION, WHETHER BASED ON CONTRACT, TORT, OR ANY OTHER LEGAL THEORY, RELATING TO OR IN CONNECTION WITH THE SERVICES, THE DOCUMENTATION OR THIS AGREEMENT EXCEED THE PURCHASE PRICE PAID FOR THE WORK.

29. Responsibility for Individuals Performing Work; Criminal Background Checks. 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.

30. **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.

31. **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.

32. **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.

33. **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.

34. **Enforcement.** 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.

35. **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. In the event that Contractor fails or is unable to do so, then Contractor will refund to University all amounts University has paid under this Agreement within thirty (30) days after University's written request. This Section will survive the termination or expiration of this Agreement.

36. **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.

37. **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.

38. **Websites and Mobile Applications.** As required by Section 2054.517, *Texas Government Code*, before deploying any website or mobile application included as part of the Work, Contractor must submit to the University 's information security officer the information required under policies adopted by the University to protect the privacy of individuals by preserving the confidentiality of information processed by the website or application. At a minimum, the information submitted by Contractor must describe:

(1) the architecture of the website or application;
(2) the authentication mechanism for the website or application; and
(3) the administrator level access to data included in the website or application.

Additionally, Contractor will provide all assistance and cooperation necessary for University to subject the website or mobile application to a vulnerability and penetration test conducted internally by University or by an independent third party, as required by Section 2054.517, *Texas Government Code*.

39. **Project Notifications and Reports.**

If a project is provided for in an applicable Order Form Contractor will, upon execution of any Order Form (Exhibit B) under this Agreement, send a fully executed copy to:

Al Arboleda
aarboleda@utsystem.edu

Contractor Reports

In addition to the reports and deliverables required under the agreement between the Contractor and the Requesting Institution who contracts for specific services, Contractor shall, on an annual basis, submit a report detailing number of slots procured by each UT Institution and total fees billed.

40. **University Institutions.** Contractor agrees that affiliated UT Institutes may subscribe to the Services under this Agreement via execution of an Order Form. By executing an Order Form, the Parties acknowledge and agree that such Institution is bound by the terms and conditions under this Agreement solely for the purposes of the subscription to be provided under the applicable Order Form. With regard to Order Forms entered into by a UT Institution: (i) all references to University or Customer in this Agreement shall be deemed to mean the UT Institution which entered into the Order Form, (ii) each Order Form shall be subject to the terms and conditions of this Agreement and legally binding exclusively upon the respective UT Institution entering into such Order Form and Contractor, and (iii) the termination of an Order Form by one UT Institution shall not impact the validity of any other Order Form.

41. **Historically Underutilized Business Subcontracting Plan.** Contractor will use good faith efforts to subcontract work performed under this Agreement in accordance with the Historically Underutilized Business Subcontracting Plan (**HSP**) (ref. **Exhibit H**). Except as specifically provided in the HSP, Contractor will not subcontract any of its duties or obligations under this Agreement, in whole or in part. This Agreement is subject to 34 TAC §20.285. Contractor will comply with all of its duties and obligations under 34 TAC §20.285. In addition to other rights and remedies, University may exercise all rights and remedies authorized by 34 TAC §20.285.

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

AGREED TO AND SIGNED BY THE PARTIES:

The University of Texas System	**COMPANY NAME**
By: ______________________________	By: ______________________________
Name: Scott C. Kelley, Ed.D.	Name:
Title: Executive Vice Chancellor, Business Affairs	Title:
Date: ____________________________	Date: ____________________________

Attached:

EXHIBIT A – Scope of Work
EXHIBIT B – Sample Order Form
EXHIBIT C – Payment for Services
EXHIBIT D – HUB Subcontracting Plan

EXHIBIT A

SCOPE OF WORK

(TO BE COMPLETED WHEN CONTRACTOR IS SELECTED)

<u>EXHIBIT B</u>

SAMPLE ORDER FORM

(TO BE COMPLETED WHEN CONTRACTOR IS SELECTED)

EXHIBIT C

PAYMENT FOR SERVICES

(TO BE COMPLETED WHEN CONTRACTOR IS SELECTED)

EXHIBIT D

HUB SUBCONTRACTING PLAN

(TO BE COMPLETED WHEN CONTRACTOR IS SELECTED)

EDUCAUSE

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 gooc save resources. As campuses deploy or identify cloud services, they must ensure the clou are appropriately assessed for managing the risks to the confidentiality, integrity and avai sensitive institutional information and the PII of constituents. Many campuses have establ cloud security assessment methodology and resources to review cloud services for privacy security controls. Other campuses don't have sufficient resources to assess their cloud se this manner. On the vendor side, many cloud services providers spend significant time re the individualized security assessment requests made by campus customers, often answe questions repeatedly. Both the provider and consumer of cloud services are wasting preci creating, responding, and reviewing such assessments.

The Higher Education Cloud Vendor Assessment Tool attempts to generalize higher educat information security and data protection questions and issues for consistency and ease of institutions may have specific issues that must be addressed in addition to the general qu provided in this assessment. It is anticipated that this Higher Education Cloud Vendor Ass Tool will be revised over time to account for changes in cloud services provisioning and th 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 security and privacy needs, including some that are unique to higher education
●Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs tł cloud services without increasing risks
●Reduces the burden that cloud service providers face in responding to requests for securi assessments from higher education institutions

This Higher Education Cloud Vendor Assessment Tool was created by the Higher Educatior Information Security Council Shared Assessments Working Group. Its purpose is to provic starting point for the assessment of third-party provided cloud services and resources. O 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 Educ Vendor Assessment Tool assessments.

https://www.educause.edu/hecvat
https://www.ren-isac.net/hecvat

This Higher Education Cloud Vendor Assessment Tool is brought to you by the Higher Educatior

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

nrough

ity

n
de a
ver time,
community
ation Cloud

.0

n

ı and

EDUCAUSE

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 o
a populated HECVAT for any/all of their services. Vendors have the choice
providing a link(s) to the index, or having the REN-ISAC host their popula

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).

at/cbi.html.

Higher Educ
Instructions

Target Audience

These instructions are fo
worksheet should not be
submit robust security s
Institution's assessment

Document Layout

There are five main sect
more detail. This docum
completed it can be pop
questions are nested an
in the correct order will

General Information
Higher Education Shared Assessments Confirmation
Qualifiers
Documentation
Company Overview
Safeguards

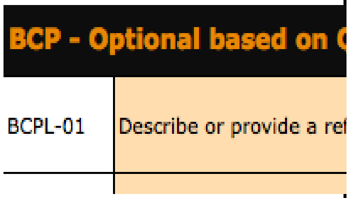
In sections where vendo
Answers and Additional
sometimes C and D are
down box and any supp
looking for the answer t
questions, check this co
question. Use the "Addit

Figure 1:

Optional Safeguard

Not all questions are rel
depending on the scope
become optional have th

Figure 2:



BCP - Optional based on Q	
BCPL-01	Describe or provide a ref

Proceed to the next ta

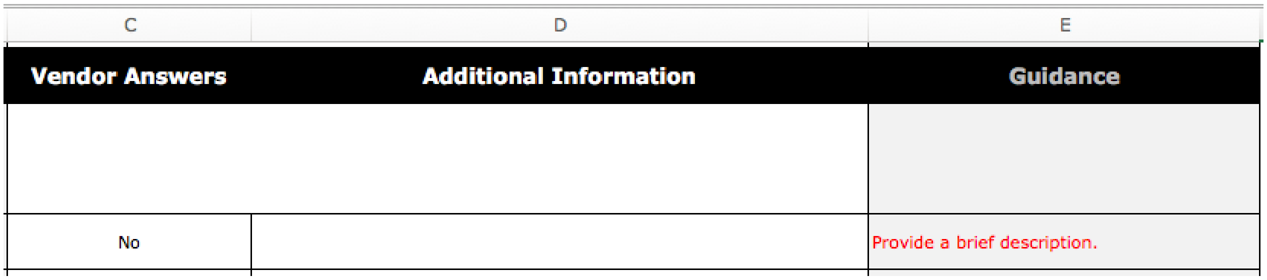
cation Cloud Vendor Assessment Tool
s

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

tions of the Higher Education Cloud Vendor Assessment Tool, all listed below and outlined in nent is designed to have the first two sections populated first; after the Qualifiers section is ulated in any order. Within each section, answer each question top-to-bottom. Some d 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.

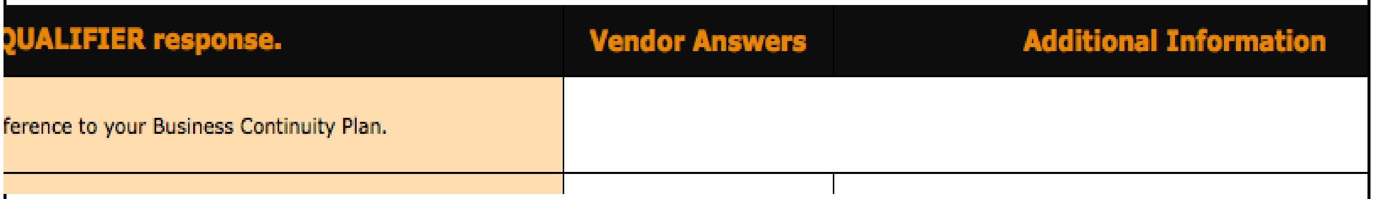
or input is required there are only one or two columns that need modification, Vendor Information, columns C and D respectively (see Figure 1 below). You will see that separate and other times are merged. If they are separate, C will be a selectable, drop-orting information should be added to column D. If C and D are merged, the question is o be in narrative form. At the far right is a column titled “Guidance”. After answering lumn to ensure you have submitted information/documentation to sufficiently answer the tional 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 ne 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**	□□

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 lea
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	*The University of Texas*
GNRL-02	Institution Department Primary Campus	*System Administration*
GNRL-03	Institution Department Code	*NA*
GNRL-04	Institution Department Contact Name	*Institution Department Con*
GNRL-05	Institution Department Contact Email	*Institution Department Con*
GNRL-06	Institution Department Contact Phone Number	*555-555-5555*
GNRL-07 through GNRL-14; populated by Vendor		
GNRL-07	Vendor Name	*Vendor Name*
GNRL-08	Product Name	*Product Name and Version*
GNRL-09	Product Description	*Please include a brief descr*

GNRL-10	Web Link to Product Privacy Notice	*http://www.vendor.domain*
GNRL-11	Vendor Contact Name	*Vendor Contact Name*
GNRL-12	Vendor Contact Title	*Vendor Contact Title*
GNRL-13	Vendor Contact Email	*Vendor Contact E-mail Addr*
GNRL-14	Vendor Contact Phone Number	*555-555-5555*
GNRL-15 and GNRL-16; populated by Institution Security Office		
GNRL-15	Institution Security Analyst/Engineer	*Institution Security Analyst*
GNRL-16	Assessment Contact	*ticket#@yourdomain.edu*
Higher Education Shared Assessments Confirmation		**Vendor Answers**
By completing the Higher Education Cloud Vendor Assessment Tool, cloud service providers understand that th **following statements will determine how this assessment may be shared within the Higher Educati**		
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 institutio

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 *application* 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 *application* 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 *system* (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 *applications* 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 *systems* 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**
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 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.	

Version 1.06

host institutional data must complete the Higher Education Cloud Vendor Assessment Tool (HECVAT). st 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

tact Name

tact Email

Information

iption 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 nal procedures.	
Additional Information	**Guidance**
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**.	
	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

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 you 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 *application* 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 *application* 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 *system* (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 *applications* 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 *systems* 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**

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

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

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

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		

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		

EDUCAUSE

Acknowledgments

The Higher Education Information Security Council Shared Assessments Working Group co
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

ontributed their