REQUEST FOR PROPOSAL
CURRICULUM & CATALOG MANAGEMENT SOFTWARE
AND OTHER RELATED SERVICES
RFP 301905
DUE: 3:00 P.M., MST, 7/10/19

Time and Date of Pre-Proposal Conference       10 A.M., MST, 6/20/19
Deadline for Inquiries                        3 P.M., MST, 6/27/19
Time and Date Set for Closing                 3 P.M., MST, 7/10/19
<table>
<thead>
<tr>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECTION I – REQUEST FOR PROPOSAL</td>
<td>3</td>
</tr>
<tr>
<td>SECTION II – PURPOSE OF THE RFP</td>
<td>4</td>
</tr>
<tr>
<td>SECTION III – PRE-PROPOSAL CONFERENCE</td>
<td>6</td>
</tr>
<tr>
<td>SECTION IV – INSTRUCTIONS TO PROPOSERS</td>
<td>7</td>
</tr>
<tr>
<td>SECTION V – SPECIFICATIONS/SCOPE OF WORK</td>
<td>12</td>
</tr>
<tr>
<td>SECTION VI – GREEN PURCHASING REQUIREMENTS/SPECIFICATIONS</td>
<td>23</td>
</tr>
<tr>
<td>SECTION VII – PROPOSER QUALIFICATIONS</td>
<td>24</td>
</tr>
<tr>
<td>SECTION VIII – EVALUATION CRITERIA</td>
<td>25</td>
</tr>
<tr>
<td>SECTION IX – PRICING SCHEDULE</td>
<td>26</td>
</tr>
<tr>
<td>SECTION X – FORM OF PROPOSAL/SPECIAL INSTRUCTIONS</td>
<td>27</td>
</tr>
<tr>
<td>SECTION XI – PROPOSER INQUIRY FORM</td>
<td>28</td>
</tr>
<tr>
<td>SECTION XII – AGREEMENT - TERMS &amp; CONDITIONS</td>
<td>29</td>
</tr>
<tr>
<td>SECTION XIII – MANDATORY CERTIFICATIONS</td>
<td>33</td>
</tr>
<tr>
<td>SECTION XIV - SECURITY REVIEW (REFERENCE DOCUMENT #1) AND SECURITY ARCHITECTURE DIAGRAM (REFERENCE DOCUMENT #2)</td>
<td>42</td>
</tr>
<tr>
<td>APPENDIX 1 - RFP CHECKLIST / COVER PAGE</td>
<td>68</td>
</tr>
</tbody>
</table>
SECTION I – REQUEST FOR PROPOSAL

RFP 301905

Arizona State University is requesting sealed proposals from qualified firms or individuals for **Curriculum and Catalog Management Software and Other Related Services.**

Proposals are to be addressed and delivered to the receptionist area, first floor, University Services Building, Purchasing and Business Services, Arizona State University, 1551 S. Rural Road, (located on the east side of Rural Road between Apache Boulevard and Broadway Road) Tempe, Arizona 85281 **on or before 3 PM MST on Wednesday, July 10th. No proposal will be accepted after this time. PROPOSALS MUST BE IN A MARKED SEALED CONTAINER** (i.e., envelope, box):

Name of Proposer
Title of Proposal
RFP Number
Date and Time Proposal is Due

All times noted are Mountain Standard Time (MST). Please note that Daylight Savings Time is NOT observed. No telephone, electronic or facsimile proposals will be considered. **Proposals received after the time and date for closing will be returned to the proposer unopened.**

A representative of Purchasing and Business Services will announce publicly the names of those firms or individuals submitting proposals. No other public disclosure will be made until after award of the contract.

Arizona State University’s Overnight Delivery (FedEx, Airborne, and UPS) address is:
Purchasing and Business Services
University Services Building
Arizona State University
1551 S. Rural Rd
Tempe, AZ 85281

Arizona State University’s U.S. Postal Service Mail address is:
Purchasing and Business Services
Arizona State University
P.O. Box 875212
Tempe, AZ 85287-5212

ARIZONA STATE UNIVERSITY

Allyson Taylor, Buyer
AT/AP
SECTION II – PURPOSE OF THE RFP

1. INTENT

ASU intends to procure a transparent, integrated system to effectively manage the full suite of curriculum development processes for undergraduate and graduate curricula. Major components should include proposals for degrees, certificates, minors and courses etc., a tracking dashboard, customizable workflows by academic unit, agenda and approval management and PeopleSoft integration. Functionality should also include the ability to attach documentation to proposals as they move through the workflow and robust reporting capabilities as identified by individual academic units and users. The successful Application will be aligned to the key business goal of improving and automating Curriculum Management processes, workflow and deliverable realization.

The University may choose to enter into multiple contracts under this solicitation. After awarding, the University does not guarantee a certain amount of hours or work or projects per year.

2. BACKGROUND INFORMATION

ASU currently uses a variety of disparate and inefficient systems to process curriculum development and implementation. Some of our current systems and supporting media include Curriculum ChangeMaker (ACRES), PeopleSoft, email, GoogleDocs, Word documents, spreadsheets and workflow diagrams. There is no central location where the data is held which contributes to unclear and confusing processes.

Many internal stakeholders are affected by our current workflows. These stakeholders include individuals from the Department Chairs/Directors, Curriculum Committee Review, Deans, University Senate, and Curriculum Coordinators and Managers. Curriculum management teams within the Office of the University Provost and Graduate College engage in this process as well.

Arizona State University is a new model for American higher education, an unprecedented combination of academic excellence, entrepreneurial energy and broad access. This New American University is a single, unified institution comprising four differentiated campuses positively impacting the economic, social, cultural and environmental health of the communities it serves. Its research is inspired by real world application blurring the boundaries that traditionally separate academic disciplines. ASU serves more than 98,000 students in metropolitan Phoenix, Arizona, the nation's fifth largest city. ASU champions intellectual and cultural diversity, and welcomes students from all fifty states and more than one hundred nations across the globe.
If you would like more information about ASU, please visit us at http://www.asu.edu.

3. TERM OF CONTRACT

The initial contract term will be for two (2) years with the possibility of three (3) successive one (1) year renewals, for a total term not to exceed five (5) years. The contract will be available for use by other University departments during this term.

The University may consider alternative contract term periods if it is deemed advantageous to do so. If alternative contract terms are proposed, they should be specific in the Pricing Schedule (Attachment A). Note: Alternative terms cannot be in lieu of the term stated above.
SECTION III – PRE-PROPOSAL CONFERENCE

A pre-proposal conference will be held on Thursday, June 20th at 10 A.M. MST. Attendance will be via a Zoom Video Conference.

The purpose of this conference will be to clarify the contents of this Request for Proposal in order to prevent any misunderstanding of the University's intention and desires, and/or to give prospective suppliers an opportunity to review the site of the work. Any doubt as to the requirements of this solicitation, or any apparent omission or discrepancy should be presented to the University representative at this conference. The University representative will then determine the appropriate action. If necessary, the University representative will issue a written amendment to this Request for Proposal. Oral statements or instructions shall not constitute an amendment to this Request for Proposal.

You do not have to send a representative to this pre-proposal conference. However, if you decide to not send a representative, then we may not know of your intent to participate in this Request for Proposal, and so may not send you any written amendments to this Request for Proposal. Further, we will assume that your failure to attend the pre-proposal conference is an indication that you expect us to review your proposal as if you had taken advantage of the pre-proposal conference.

To participate in the pre-proposal conference, please register below:

https://asu.zoom.us/meeting/register/cf522aa6a48f5f35cde7dc3c8da9331e

During the registration process, the following information will be requested:

- Name
- Email Address
- Organization
- Title
- Phone Number

After registering, you will receive a confirmation email containing information about joining the meeting.
SECTION IV – INSTRUCTIONS TO PROPOSERS

1. You must address and deliver your proposal to the receptionist area, first floor, University Services Building, Purchasing and Business Services, Arizona State University, 1551 S. Rural Road, Tempe, Arizona 85281, on or before the time and date set for closing. No proposal will be accepted after this time. The University Services Building is located on the east side of Rural Road between Apache Boulevard and Broadway Road. PROPOSALS MUST BE IN A MARKED SEALED CONTAINER (i.e., envelope, box):

   Name of Proposer
   Title of Proposal
   RFP Number
   Date and Time Proposal is Due

   All times noted are Mountain Standard Time (MST). Please note that Daylight Savings Time is NOT observed. No telephone, electronic or facsimile proposals will be considered. Proposals received after the time and date for closing will be returned to the proposer unopened.

2. DIRECTIONS TO USB VISITOR PARKING. Purchasing and Business Services is in the University Services Building (“USB”) 1551 S. Rural Road, Tempe, AZ, 85281 (located on the east side of Rural between Broadway Road and Apache Boulevard). A parking meter is located near the main entry to USB.

   All visitors to USB are required to check in at the USB Reception Desk to obtain a visitor’s badge to wear while in the building. The receptionist will call to have you escorted to your meeting.

3. Proposer should use recycled paper and double-sided copying for the production of all printed and photocopied proposal documents. Furthermore, the documents should be clearly marked to indicate that they are printed on recycled content (minimum 30% post-consumer waste paper).

4. You may withdraw your proposal at any time prior to the time and date set for closing.

5. No department, school, or office at the University has the authority to solicit or receive official proposals other than Purchasing and Business Services. All solicitations are performed under the direct supervision of the Chief Procurement Officer and in complete accordance with University policies and procedures.

6. The University reserves the right to conduct discussions with proposers, and to accept revisions of proposals, and to negotiate price changes. During this discussion period, the University will not disclose any information derived from proposals submitted, or from discussions with other proposers. Once a contract is executed, the solicitation file, and the proposals contained therein, are in the public record and will be disclosed upon request.

7. Proposers submitting proposals which meet the selection criteria and which are deemed to be the most advantageous to the University may be requested to give an oral presentation to a selection committee. Purchasing and Business Services will do the scheduling of these oral presentations.
8. The award shall be made to the responsible proposer whose proposal is determined to be the most advantageous to the University based on the evaluation factors set forth in this solicitation. Price, although a consideration, will not be the sole determining factor.

9. If you are submitting any information you consider to be proprietary, you must place it in a separate envelope and mark it “Proprietary Information”. If the Chief Procurement Officer concurs, this information will not be considered public information. The Chief Procurement Officer is the final authority as to the extent of material, which is considered proprietary or confidential. Pricing information cannot be considered proprietary.

10. The University is committed to the development of Small Business and Small Disadvantaged Business (“SB & SDB”) suppliers. If subcontracting (Tier 2 and higher) is necessary, proposer (Tier 1) will make every effort to use SB & SDB in the performance of any contract resulting from this proposal. A report may be required at each annual anniversary date and at the completion of the contract indicating the extent of SB & SDB participation. A description of the proposers expected efforts to solicit SB & SDB participation should be enclosed with your proposal.

11. Your proposal should be submitted in the format shown in Section X. Proposals in any other format will be considered informal and may be rejected. Conditional proposals will not be considered. An individual authorized to extend a formal proposal must sign all proposals. Proposals that are not signed may be rejected.

12. The University reserves the right to reject any or all proposals or any part thereof, or to accept any proposal, or any part thereof, or to withhold the award and to waive or decline to waive irregularities in any proposal when it determines that it is in its best interest to do so. The University also reserves the right to hold all proposals for a period of one hundred twenty (120) days after the opening date and the right to accept a proposal not withdrawn before the scheduled proposal opening date.

13. EXCEPTIONS: The Arizona State University contract terms and conditions are included in this Request for Proposal in Section XII. These terms and conditions will be incorporated into the contract between the University and the successful proposer. Proposals that are contingent upon any changes to these mandatory contract terms and conditions may be deemed nonresponsive and may be rejected. All exceptions must be submitted with justification and alternate language, and MUST be submitted with the proposal. In no event is a Proposer to submit its own standard contract terms and conditions as a response to this RFP.

14. Unless specifically stated to the contrary, any manufacturer's names, trade names, brand names or catalog numbers used in the specifications of this Request for Proposal are for the purpose of describing and/or establishing the quality, design and performance required. Any such reference is not intended to limit or restrict an offer by any proposer and is included in order to advise the potential proposer of the requirements for the University. Any offer, which proposes like quality, design or performance, will be considered.

15. Days: Calendar days

May: Indicates something that is not mandatory but permissible/ desirable.

Shall, Must, Will: Indicates mandatory requirement. Failure to meet these mandatory requirements will result in rejection of your proposal as non-responsive.
16. Any person, firm, corporation or association submitting a proposal shall be deemed to have read and understood all the terms, conditions and requirements in the specifications/scope of work.

17. All proposals and accompanying documentation will become the property of the University at the time the proposals are opened. **It will be the proposer’s responsibility to request that samples be returned to the proposer and provide a method for doing so at the expense of the proposer.** If a request is not received and a method of return is not provided, all samples shall become the property of the University 45 days from the date of the award.

18. All required performance and payment bonds shall be held by the University in a secure location until the performance of the contract and the payment of all obligations rising there under have been 100% fulfilled. Upon completion of the project and all obligations being fulfilled, it shall be the proposer’s responsibility to request the surety bonding company to submit to the University the necessary documents to approve the release of the bonds. Until such time the bonds shall remain in full force and effect.

19. The University of Arizona, Northern Arizona University, and Arizona State University are all state universities governed by the Arizona Board of Regents. **Unless reasonable objection is made in writing as part of your proposal to this Request for Proposal, the Board or either of the other two Universities may purchase goods and/or services from any contract resulting from this Request for Proposal.**

20. The University has entered into Cooperative Purchasing Agreements with the Maricopa County Community College District and with Maricopa County, in accordance with A.R.S. Sections 11-952 and 41-2632. Under these Cooperative Purchasing Agreements, and with the concurrence of the proposer, the Community College District and/or Maricopa County may access a contract resulting from a solicitation done by the University. If you do not want to grant such access to the Maricopa County Community College District and or Maricopa County, please state so in your proposal. In the absence of a statement to the contrary, the University will assume that you do wish to grant access to any contract that may result from this Request for Proposal.

21. A Arizona State University is a member of various co-operative organizations, in accordance with A.R.S Sections 11-952 and 41-2632. Under these Cooperative Purchasing Agreements, the University may share and distribute a contract resulting from a solicitation. In the absence of a statement to the contrary, the University will assume that you do wish to grant access to any contract that may result from this Request for Proposal.

22. **Administrative Fee:** Awarded Suppliers shall pay ASU an Administrative Fee in the amount of 1 percent of the gross funds received by the Supplier from any of the Arizona Entities or any other similar entity in any other state. This fee will apply only to contracts entered into after the effective date of the signed contract. This fee will apply to any and all products and services sold by the Supplier that reference the signed contract as the supporting documentation to meet competitive bidding requirements. The Administrative Fee will be calculated based on all sales transacted under the contract, minus all taxes and any returns or credits. The Supplier will submit the Administrative Fee, along with a quarterly usage report documenting all contract sales, to the ASU Chief Procurement Office within thirty (30) days following the end of each calendar quarter.
Each quarterly report at a minimum, shall disclose all purchased goods and services, prices paid, and quantity, by individual purchasing agency, for all sales within the calendar 10 Revision Dec. 18, 2018 quarter just ended. The Supplier will upload to and make continuously available in the Central Repository the quarterly usage report.

23. All formal inquiries or requests for significant or material clarification or interpretation, or notification to the University of errors or omissions relating to this Request for Proposal must be directed, in writing, to:

Allyson Taylor  
Purchasing and Business Services  
University Services Building  
Arizona State University  
PO Box 875212  
Tempe, AZ 85287-5212

Tel: 480-965-2074  
E-mail: allyson.taylor@asu.edu

Requests must be submitted on a copy of the Proposer Inquiry Form included in Section XI of this Request for Proposal. All formal inquiries must be submitted at least ten (10) calendar days before the time and date set for closing this Request for Proposal. Failure to submit inquiries by this deadline may result in the inquiry not being answered.

Note that the University will answer informal questions orally. The University makes no warranty of any kind as to the correctness of any oral answers and uses this process solely to provide minor clarifications rapidly. Oral statements or instructions shall not constitute an amendment to this Request for Proposal. Proposers shall not rely on any verbal responses from the University.

24. The University shall not reimburse any proposer the cost of responding to a Request for Proposal.

25. In accordance with an executive order titled “Air Pollution Emergency Proclamation” modified by the Governor of Arizona on July 16, 1996, the University formally requests that all products used in the performance of any contract that results from this Request for Proposal be of low- or no-content of reactive organic compounds, to the maximum extent possible.

26. Arizona requires that the University purchase ENERGY STAR® products or those certified by the Federal Energy Management Program as energy efficient in all categories available. If this Request for Proposal is for a product in a category for which ENERGY STAR® or certified products are available, please submit evidence of the ENERGY STAR® status or certification for the products you are bidding. Please note that if you fail to submit this information but a competitor does, the University will select your competitor’s product as meeting specifications and deem your product as not meeting specifications. See A.R.S. §34-451.

27. The University requires that all desktop computers, notebooks, and monitors purchased must meet Electronic Product Environmental Assessment Tool (EPEAT) Gold status as contained in the IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products. The registration criteria and a list of all registered equipment are at http://www.epeat.net/about-epeat/ on the Web.
28. To the extent applicable to any contract resulting from this Request for Proposal, the proposer shall comply with the Standards for Privacy of Individually Identifiable Information under the Health Insurance Portability and Accountability Act of 1996 contained in 45 CFR Parts 160 and 164 (the “HIPAA Privacy Standards”) as of the effective date of the HIPAA Privacy Standards on April 14, 2003 or as later determined. Proposer will use all security and privacy safeguards necessary to protect Protected Health Information (PHI), as defined by HIPAA, and shall immediately report to University all improper use or disclosure of PHI of which it becomes aware. Proposer agrees to ensure that its agents and subcontractors agree to and abide by these requirements. **Proposer agrees to indemnify the State of Arizona, its departments, agencies, boards, commissions, universities and its officers, officials, agents, and employees against all harm or damage caused or contributed to by proposer’s breach of its obligations under this paragraph.**

29. The University believes that it can best maintain its reputation for treating suppliers in a fair, honest, and consistent manner by conducting solicitations in good faith and by granting competitors an equal opportunity to win an award. If you feel that we have fallen short of these goals, you may submit a protest pursuant to the Arizona Board of Regents procurement procedures, section 3-809,

Protests should be directed to:

Jamon Hill  
Deputy Chief Procurement Officer  
Purchasing and Business Services  
PO Box 875212  
Tempe AZ 85287-5212  
Email: Jamon.Hill@asu.edu

Please note that as the University takes protests very seriously; we expect you to do so as well. Frivolous protests will not result in gain for your firm.
SECTION V – SPECIFICATIONS/SCOPE OF WORK

Instructions to Proposers

Place an “X” on the line acknowledging this section.

The proposer may request from ASU Purchasing (allyson.taylor@asu.edu) the following documents:

- Excel Document for Attachment A in Section IX - Pricing Schedule
- Word Document for Appendix 1 - RFP Checklist/Cover Page

A. System Functionality

Respondents may propose solutions for separate elements within a suite of products. Please be sure to list all the different elements / modules within your system that you are proposing as part of this RFP.

There are various roles and tasks to support current workflow that are expected to be automated and available for customization by academic unit and workflow type. When responding please indicate where functionality would require customization and additional costs incurred. These costs must be listed in the Attachment A Pricing Schedule.

Respondents must have each of the following capabilities, qualities, or modules already existing within their solution. Please check each box according to your proposed solution.

- A fully cloud-based or SaaS model
- Curriculum management & review (degrees, courses, prefixes etc.) which:
  - Facilitates strategic academic planning and proposal processes such that all entries and responses can be submitted and communicated electronically
  - Allows for unique and specific workflow processes to be designed not only for multiple types of curriculum proposals, but for each college or academic unit (See Exhibits A and B Undergraduate and Graduate sample workflows below)
  - Connects curriculum proposals with associated proposals for prefixes, courses (new, modified etc.), multiple internal approval levels, and fees allowing curriculum packages to move through the approval process together
  - Formats proposals in full view and also in an abbreviated form suitable for review and approval by multiple audiences
  - Allows for review and editing of handbooks and policy manuals
  - Creates agendas for governance reviews
  - Customizable workflow based on academic structure and permissions-based requirements

- Real-time catalog integration that:
  - Performs tasks and manages workflow for the annual catalog review process and creation of the catalog archive
- Directly connects data, or has the ability to feed data into/from PeopleSoft (include information on which versions of PeopleSoft integration APIs are in use currently)

- Supports standardized and customized reporting that:
  - Pushes notifications to users suitable for official university documentation and implementation purposes
  - Ad hoc and customized reporting
  - Solution is transparent; thereby allowing academic units, deans and the university’s user community to know precisely where in the workflow curricular and course approvals are being reviewed
  - Provides an out-of-the-box solution for dashboards that facilitates customizable view of individual proposal’s progress based on security level access

- Functions as an archival database which:
  - Maintains all curriculum/program data, including:
    - Proposed curriculum/programs
    - Curriculum/programs under review
    - Approved curriculum/programs
    - Historical/archived curriculum/programs
  - Utilizes the concept of effective dating to allow future modifications to be proposed and reviewed for currently existing programs, in advance of implementation of those modifications
  - Serves as an approval system

- Provides a user-friendly interface that is simple and intuitive to use
  - Single-sign on capability for all ASU faculty and staff
  - Access levels based on defined roles and permission settings
  - Allows for users to modify notification settings

- Customer support services, data backup and disaster recovery

- After initial implementation, ability for ASU to maintain and modify forms, processes and workflow

- Meets security standards as defined by ASU Security Policy and Standards (see Information Security provision under ASU Terms and Conditions) and provide any applicable certifications
Exhibit A. Undergraduate Sample Workflow:

Exhibit B. Graduate Sample Workflow:
1. A fully cloud-based or SaaS model with robust data security and backup plan.

2. Curriculum management & review (degrees, courses, prefixes etc.) which:
   a. Facilitates strategic academic planning and proposal processes such that all entries and responses can be submitted and communicated electronically

   b. Allows for unique and specific workflow processes to be designed not only for multiple types of curriculum proposals, but for each college or academic unit (See undergraduate and graduate sample workflows below)

   c. Connects curriculum proposals with associated proposals for prefixes, courses (new, modified etc.), multiple internal approval levels, and fees allowing curriculum packages to move through the approval process together

   d. Formats proposals in full view and also in an abbreviated form suitable for review and approval by multiple audiences

   e. Allows for review and editing of handbooks and policy manuals

   f. Creates agendas for governance reviews

   g. Customizable workflow based on academic structure and permissions-based requirements

3. Real-time catalog integration that:
   a. Performs tasks and manages workflow for the annual catalog review process and creation of the catalog archive

   b. Directly connects data, or has the ability to feed data into/from PeopleSoft (include information on which versions of PeopleSoft integration APIs are in use currently)
4. Supports standardized and customized reporting that:
a. Pushes notifications to users suitable for official university documentation and implementation purposes

b. Ad hoc and customized reporting
c. Solution is transparent; thereby allowing academic units, deans and the university’s user community to know precisely where in the workflow curricular and course approvals are being reviewed
d. Provides an out-of-the-box solution for dashboards that facilitates customizable view of individual proposal’s progress based on security level access

5. Functions as an archival database which:
a. Maintains all curriculum/program data, including:
   i. Proposed curriculum/programs
   ii. Curriculum/programs under review
   iii. Approved curriculum/programs
   iv. Historical/archived curriculum/programs

b. Utilizes the concept of effective dating to allow future modifications to be proposed and reviewed for currently existing programs, in advance of implementation of those modifications
c. Serves as an approval system

6. Provides a user-friendly interface that is simple and intuitive to use
   a. Single-sign on capability for all ASU faculty and staff

   b. Access levels based on defined roles and permission settings

7. Customer support services, data backup and disaster recovery
8. After initial implementation, ability for ASU to maintain and modify forms, processes and workflow.

9. Meets security standards as defined by ASU Security Policy and Standards (see Information Security provision under ASU Terms and Conditions)

Respondents should have each of the following capabilities, qualities, or modules already existing within their solution. Please check each box according to your proposed solution.

☐ A fully implemented application inclusive of licensing and professional services
☐ Phased implementation schedule
☐ Mobile accessibility for both iOS and Android
☐ Separate application instances for Development, Test, and Production
☐ Integration API’s readily available and demonstrable for the following systems:
  ○ Single Sign-On
  ○ PeopleSoft (Campus Solutions & HCM)
  ○ BI data mining tools
☐ Robust security requirements including:
  ○ FERPA
  ○ HIPAA
  ○ GDPR
☐ Connected user community and conference

Provide responses and additional information related to each of the items below based on your system’s capabilities. Please include a graphic visualizations as where appropriate. Please reply directly underneath each item below for ease of evaluation.

1. A fully implemented application inclusive of licensing and professional services

2. Phased implementation schedule

3. Mobile accessibility for both iOS and Android

4. Separate application instances for Development, Test, and Production
5. Integration API’s readily available and demonstrable for the following systems:
   a. Single Sign-On
   
   b. PeopleSoft (Campus Solutions & HCM)
   
   c. BI data mining tools such as Asential Datastage

6. Robust security requirements including:
   a. FERPA
   
   b. HIPAA
   
   c. GDPR

7. Connected user community and conference

B. Implementation

Respondents must have each of the following capabilities, qualities, or modules already existing within their solution. Please check each box according to your proposed solution.

☐ Documented implementation plan describing support provided from start to finish of implementation, and listing major deliverables, milestones, and necessary resources

☐ Description of required consultation assistance needed to configure the application and system implementation

☐ User documentation available that is customizable for ASU’s specific implementation

Provide responses and additional information related to each of the items above based on your system’s capabilities. Please include a graphic visualizations as where appropriate. Please reply directly underneath each item below for ease of evaluation.

1. Documented implementation plan describing support provided from start to finish of implementation, and listing major deliverables, milestones, and necessary resources

2. Description of required consultation assistance needed to configure the application and system implementation
3. User documentation available that is customizable for ASU’s specific implementation

C. Support and Training

Provide responses and additional information related to each of the items above based on your system’s capabilities. Please include a graphic visualizations as where appropriate. Please reply directly underneath each item below for ease of evaluation.

1. Provide a copy of your standard support level agreement(s). Please indicate:
   ○ The initial period of software support
   ○ Any options for annual or multi-year software support
   ○ Support for error corrections (fixes), tracking and prioritization
   ○ Upgrades and technical assistance on the installation, use, performance tuning, maintenance and repair of the software
   ○ Outage time and schedule
   ○ Uptimes

2. Provide a comprehensive description of your software and technical support organization and capabilities including:
   ○ Performance monitoring processes and notifications
   ○ Service locations
   ○ Service days
   ○ Service hours (24/7)
   ○ Methods of contact
○ Number of university contacts allowed

○ Agreed response times after initial incident report and problem escalation

○ Disaster management plan, including information on past test

○ Description of how violations of service are recorded and communicate

3. Describe your training offerings including:
   ○ Onsite vs. virtual training

   ○ User guides and training manuals

D. Transition In/Out Plan

A Transition-In/Out Plan which will describe the process for transitioning the University’s data to another product in the future, and, in a hosted model, transitioning to another hosting provider. The proposer shall provide a Transition-In/Out Plan that establishes and contains the transition responsibilities, descriptions and schedules for the required tasks. The purpose of the Transition-In/Out Plan is to ensure an efficient and effective transition from the proposer to another service provider or product with minimal disruption to operations. The University expects compliance with the following activities in order to meet this requirement:

No later than 30 calendar days from date of Contract award, contractor must finalize the details of the proposed Transition-In/Out Plan and submit it to the University Project Director for review and approval. The Transition-In/Out Plan must, at a minimum, include:

Goals, expectations and specific objectives of the Transition-In/Out Plan;

Description of the methodology and approach for transferring data and other information to another service provider;

Assumptions and dependencies associated with the Transition-In/Out;

and Estimated timelines and milestones for specific tasks throughout the Transition-In/Out Period.

A finalized plan shall be coordinated and drafted between the awarded proposer and ASU for transition in/out services.
1. Please describe your standard or typical transition plan to describe any information on their firm’s transition in/out services.

During execution of the approved Transition-In/Out Plan, the Transition-In/Out Team (composed of University staff, contractor, and personnel of another service provider) shall meet regularly to review and update the Transition-In/Out Plan to reflect revisions to schedules, resource requirements, dependencies, and priorities; and to summarize the progress on the Transition-In/Out Plan to date.

___________ Place an “X” on the line acknowledging this section.

The Transition-In/Out Plan submitted by the contractor to the University must be reviewed and approved by University project leadership prior to implementation. Any clarifications or modifications to the Transition-In/Out plan required by the University must be made by Vendor no later than five (5) calendar days from the date of written request.

___________ Place an “X” on the line acknowledging this section.

During a transition-in/out period, contractor will be required to work cooperatively and expeditiously to transfer the existing responsibilities to the University or another service provider.

___________ Place an “X” on the line acknowledging this section.

E. Value-Added Services

ASU is looking for more than a vendor/client relationship. It is interested in companies that have like minded views towards education who are interested in a relationship where developing innovative solutions that provide an enhanced learning experience for students and faculty is prioritized over a more traditional, transactional, sales relationship. The University is involved in multiple projects to improve student retention and success therefore it is looking for proposals that offer a more comprehensive strategic relationship.

Proposer should provide a brief summary of any other value-added services or programs which may contribute to the overall value of your proposal, including but not limited to:

- Training
- Industry Partnerships
- Support of ASU’s Charter and Goals
- Support of sustainable development, veterans’ affairs, initiatives in support of women, wellness, and our changing regional demographics
- Support and enhancement of ASU’s reputation as an innovative foundational model for the New American University
- Comment to provide significant financial and non-financial support for the University and its signature program

1. Describe any special resources which you firm possesses that are not part of this RFP that would be available as part of our agreement.
2. Describe any special skills which your firm possesses that are not part of this RFP that would be available as part of our agreement.

3. Describe any special services which your firm possesses that are not part of this RFP that would be available as part of our agreement.

4. Please demonstrate any advantages that would be realized by the University as a result of any stated value-added resources
SECTION VI – GREEN PURCHASING REQUIREMENTS/SPECIFICATIONS

In order to reduce the adverse environmental impact of our purchasing decisions the University is committed to buying goods and services from manufacturers and suppliers who share the University’s environmental concern and commitment. Green purchasing is the method wherein environmental and social considerations are taken with equal weight to the price, availability and performance criteria that we use to make purchasing decisions.

Proposer shall use environmentally preferable products, materials and companies where economically feasible. Environmentally preferable products have a less or reduced effect on human health and the environment when compared to other products and companies that serve the same purpose. If two (2) products are equal in performance characteristics and the pricing is within 5%, the University will favor the more environmentally preferable product and company.

If you are citing environmentally preferred product claims, you must provide proper certification or detailed information on environmental benefits, durability and recyclable properties.

The University and the supplier may negotiate during the contract term to permit the substitution or addition of Environmentally Preferable Products (EPPs) when such products are readily available at a competitive cost and satisfy the university’s performance needs.

Unless otherwise specified, proposers and contractors should use recycled paper and double-sided copying for the production of all printed and photocopied documents. Furthermore, the documents shall be clearly marked to indicate that they are printed on recycled content (minimum 30% post-consumer waste) paper.

Proposer shall minimize packaging and any packaging/packing materials that are provided must meet at least one of, and preferably all, of the following criteria:

- Made from 100% post-consumer recycled materials
- Be recyclable
- Reusable
- Non-toxic
- Biodegradable

Further, proposer is expected to pick up packaging and either reuse it or recycle it. This is a requirement of the contract or purchase order.
SECTION VII – PROPOSER QUALIFICATIONS

The University is soliciting proposals from firms, which are in the business of providing services as listed in this Request for Proposal. Your proposal shall include, at a minimum, the following information. Failure to include these items may be grounds for rejection of your proposal.

1. The proposer shall present evidence that the firm or its officers have been engaged for at least the past five (5) years in providing services as listed in this Request for Proposal.

2. Submit three (3) present client references comparable in scope of the RFP that have been implemented and functional for over one year. References should be verifiable and should be able to comment on the firm’s experience, with a preference related to services similar to this project and organizations of similar size and scope of our university. Include the name, title, telephone number, and e-mail address of the individual at the client organization who is most familiar with this engagement.

3. All key personnel proposed by the firm should have relevant experience, and be fully qualified to successfully provide the services described in the Scope of Work. Provide an organizational chart that provides organizational sections, highlighting the section that will have responsibility for performing this initiative, clearly noted.

4. Describe your firm’s approach to providing the services described in Section V, as well as the methodology used. Provide a detailed timeline (ex. Gantt Chart), including major milestones, for each of the steps outlined in Section V. Include other steps if appropriate as well as the resources, from both organizations, that will be necessary for a successful implementation.

5. Describe what distinguishes the ability of your firm from that of your competitors to perform the services described in the Request for Proposal.

6. Provide a statement acknowledging your Legal or Contract team’s review and acceptance of ASU’s Terms and Conditions and Insurance Requirements. Note: all exceptions with justification and alternative language MUST be submitted with the proposal.
SECTION VIII – EVALUATION CRITERIA

Proposals will be evaluated on the following criteria, listed in order of their relative priority with most important listed first:

<table>
<thead>
<tr>
<th>Weight</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>Response to Specifications/Scope of Work</td>
</tr>
<tr>
<td>25%</td>
<td>Response to Pricing Schedule</td>
</tr>
<tr>
<td>15%</td>
<td>Response to Proposer Qualifications</td>
</tr>
<tr>
<td>10%</td>
<td>Sustainability Efforts / Sustainability Questionnaire</td>
</tr>
</tbody>
</table>

Confidential and/or Proprietary Information must be submitted per the instructions in Section IV, item 9. Any watermarks, footnotes or reference to Confidential and/or Proprietary throughout the submitted proposal will be disregarded as boilerplate markings.
SECTION IX – PRICING SCHEDULE

Proposer shall submit a detailed cost proposal to include all aspects of providing the scope of work associated with this Request for Proposal. Any additional costs, fees, and expenses must be detailed in the proposer’s proposal. Any additional expenses, not explicitly stated, will not be honored by ASU unless negotiated and agreed upon prior to the start of additional work. ASU is interested in receiving creative and comprehensive pricing matrices, which leverage the proposer’s options with regard to the scope and level of service.

The supplier must fill in “Attachment A” Pricing sheet for license fees and costs.

The University may consider alternative contract term periods if it is deemed advantageous to do so. If alternative contract terms are proposed, they should be specified in the Pricing Schedule (Attachment A). Note: Alternative terms cannot be in lieu of the requested term of two (2) years with three (3) successive renewals.

If ASU agrees to reimburse vendor for any travel expenses, all reimbursable travel expenses must be authorized in writing by ASU in advance of the planned travel and must be consistent with ASU Financial Services Policy FIN 421-01, www.asu.edu/aad/manuals/fin/fin421-01.html. If ASU agrees to reimburse vendor for any expenses, vendor will submit all receipts and any required backup documentation to ASU within 60 days after the applicable expenses were incurred. ASU will not be required to reimburse Licensor for any expenses, invoices, or receipts for expenses received after that time. Proposer must acknowledge and accept this provision.
SECTION X – FORM OF PROPOSAL/SPECIAL INSTRUCTIONS

Format of Submittal

To facilitate direct comparisons, your proposal must be submitted in the following format:

- **One (1) clearly marked hardcopy “original” in 8.5” x 11” double-sided, non-binding form. No metal or plastic binding – may use binder, folder, or clip for easy removal of proposal; and**

- **One (1) “single” continuous (no folders) electronic copy (flash drive only), PC readable, labeled and no passwords.**

- Any confidential and/or proprietary documents must be on a separate flash drive and labeled appropriately.

- Proposer must check all flash drives before submitting. Company marketing materials should not be included unless the Request for Proposal specifically requests them. All photos must be compressed to small size formats.

Content of Submittal

If proposer fails to provide any of the following information, with the exception of the mandatory proposal certifications, the University may, at its sole option, ask the proposer to provide the missing information or evaluate the proposal without the missing information.

1. Appendix 1 – RFP Checklist/Cover Page
2. Section XIII – Mandatory Certifications, Voluntary Product Accessibility Template (VPAT), & Supplier Sustainability Questionnaire
3. Section VII – Proposer Qualifications
4. Section V – Specifications/Scope of Work
5. Section IX – Pricing Schedule (Attachment A)
6. Exceptions, justification, and alternate language proposed by Legal or Contract team and acknowledgement of Insurance Requirements Section XII, Terms and Conditions
7. Confidential/Proprietary Justification Letter with sealed documents, if applicable. Please review instructions under Section IV, page 9, item 9.
SECTION XI – PROPOSER INQUIRY FORM

Pre-Proposal Questions, General Clarifications, etc.— Email to allyson.taylor@asu.edu

PROJECT NAME: ________________________________________________________________

PROPOSAL NUMBER: __________________________________________________________

INQUIRY DEADLINE: 3:00 P.M., MST, June 27th, 2019

QUESTIONS ON: _____ ORIGINAL PROPOSAL or _____ ADDENDUM NO. ____________

DATE: __________________________

WRITER: _________________________

COMPANY: _______________________

E-MAIL ADDRESS: _______________________

PHONE: _________________________ FAX: _________________________

QUESTIONS:

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________
ASU will issue a Purchase Order(s) for goods and/or services awarded under this RFP. The parties to the Purchase Order will be bound by the ASU Terms and Conditions effective on the date the purchase order is received. The ASU Terms and Conditions are available at https://www.asu.edu/purchasing/pdf/Stand_TsCs_Provisions.pdf. Insurance requirements are outlined within this RFP and will be included in any resulting Purchase Order. Proposals that are contingent upon any changes to these mandatory contract terms and conditions may be deemed non responsive and may be rejected. All exceptions must be submitted with justification and alternate language, and MUST be submitted with the proposal.

ASU Terms and Conditions Amendment: Unless and until the District Court’s injunction in Jordahl v. Brnovich et al., Case No. 3:17-cv-08263 (D. Ariz.) is stayed or lifted, the Anti-Israel Boycott Provision (A.R.S.35-393.01 (A)) is unenforceable and the State will take no action to enforce it. Offers will not be evaluated based on whether this certification has been made.
Insurance Requirements

Please confirm your acknowledgement of ASU’s standard Insurance Requirements. Note: The Insurance Requirements are subject to change contingent upon ASU Emergency and Risk Management department’s assessment of the Scope of Work during the RFP Evaluation.

Without limiting any liabilities or any other obligation of Supplier, Supplier will purchase and maintain (and cause its subcontractors to purchase and maintain), until all of their obligations have been discharged or satisfied, including any warranty periods under the Agreement, insurance against claims that may arise from or in connection with the performance of the work hereunder by Supplier, its agents, representatives, employees or subcontractors, as described below.

These insurance requirements are minimum requirements for the Agreement and in no way limit any indemnity covenants in the Agreement. ASU does not warrant that these minimum limits are sufficient to protect Supplier from liabilities that might arise out of the performance of the work under the Agreement by Supplier, its agents, representatives, employees, or subcontractors. These insurance requirements may change if Supplier is a foreign entity, or with foreign insurance coverage.

A. Minimum Scope and Limits of Insurance: Supplier’s insurance coverage will be primary insurance with respect to all other available sources. Supplier will provide coverage with limits of liability not less than those stated below:

1. Commercial General Liability – Occurrence Form. Policy will include bodily injury, property damage, personal injury, and broad form contractual liability coverage.

   - General Aggregate $2,000,000
   - Products – Completed Operations Aggregate $1,000,000
   - Personal and Advertising Injury $1,000,000
   - Contractual Liability $1,000,000
   - Fire Legal Liability (only if Agreement is for leasing space) $50,000
   - Each Occurrence $1,000,000

   a. Policy will include the following additional insured language: “The State of Arizona, its departments, agencies, boards, commissions, universities, and its officers, officials, agents, and employees, will be named as additional insureds with respect to liability arising out of the activities performed by or on behalf of Supplier.”

   b. Policy will contain a waiver of subrogation against the State of Arizona, its departments, agencies, boards, commissions, universities, and its officers, officials, agents, and employees, for losses arising from work performed by or on behalf of Supplier.

2. Automobile Liability. If Supplier will be driving on ASU campus or on ASU business the following section will apply:

   Policy will include Bodily Injury and Property Damage for any owned, hired, and/or non-owned vehicles used in the performance of the Agreement in the following amounts. If Supplier is not an individual then coverage will be a combined single limit of $1,000,000. If Supplier is an individual then coverage will be $100,000 per person, $300,000 per accident, and $50,000 property damage.

   a. Policy will include the following additional insured language: “The State of Arizona, its departments, agencies, boards, commissions, universities, and its officers, officials, agents, and employees, will be named as additional insureds with respect to liability arising out of the activities performed by or on behalf of Supplier, involving vehicles owned, leased, hired, or borrowed by Supplier.”

   b. Policy will contain a waiver of subrogation against the State of Arizona, its departments, agencies, boards, commissions, universities, and its officers, officials, agents, and employees, for losses arising from work performed by or on behalf of Supplier.

   c. Policy will contain a severability of interest provision.
3. **Worker’s Compensation and Employers’ Liability.** Applicable statutory limits, as amended from time to time.

   a. Employer’s Liability in the amount of $1,000,000 injury and disease.

   b. Policy will contain a waiver of subrogation against the State of Arizona, its departments, agencies, boards, commissions, universities, and its officers, officials, agents, and employees, for losses arising from work performed by or on behalf of Supplier.

   c. This requirement will not apply to any contractor or subcontractor exempt under ARS § 23-901, when such contractor or subcontractor signs the [Sole Proprietor Waiver Form](#).

4. **Technology/Network Errors and Omissions Insurance.** The terms of this section apply if: 1) ASU is purchasing or leasing software, or processing a software renewal; 2) Supplier is creating any code for ASU; 3) Supplier receives, stores, or analyzes ASU Data (including if the data is not online); 4) Supplier is hosting, or managing by infrastructure outside of ASU, including in the cloud, ASU Data; OR 5) ASU is purchasing or leasing equipment that will connect to ASU’s data network.

   - Each Claim $2,000,000
   - Annual Aggregate $4,000,000

   a. This insurance will cover Supplier’s liability for acts, errors and omissions arising out of Supplier’s operations or services, including loss arising from unauthorized access, or use that results in identity theft or fraud.

   b. If the liability insurance required by the Agreement is written on a claims-made basis, Supplier warrants that any retroactive date under the policy will precede the effective date of the Agreement, and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of 2 years beginning at the time work under the Agreement is completed.

   c. Policy will cover professional misconduct for those positions defined in the scope of work of the Agreement.

5. **Professional Liability (Errors and Omissions Liability).** If the Supplier will provide ASU Services under the Agreement, the Policy will include professional liability coverage as follows:

   - Each Claim $1,000,000
   - Annual Aggregate $2,000,000

   a. If the professional liability insurance required by the Agreement is written on a claims-made basis, Supplier warrants that any retroactive date under the policy will precede the effective date of the Agreement; and that either continuous coverage will be maintained or an extended discovery period will be exercised for 2 years beginning at the time work under the Agreement is completed.

   b. Policy will cover professional misconduct for those positions defined in the scope of work of the Agreement.

B. **Cancellation; Material Changes:** Cancellation notices will be delivered to ASU in accordance with all policy provisions. Notices required in this Section must be sent directly to ASU Purchasing and Business Services, email [insurance.certificates@asu.edu](mailto:insurance.certificates@asu.edu) or mail to PO Box 875212, Tempe, AZ, 85287-5212.

C. **Acceptability of Insurers:** Insurance is to be placed with duly licensed or approved non-admitted insurers in the State of Arizona with an “A.M. Best” rating of not less than A- VII. ASU in no way warrants that the above required minimum insurer rating is sufficient to protect Supplier from potential insurer insolvency. Self-Insurance may be accepted in lieu of or in combination with insurance coverage requested.

D. **Verification of Coverage:** Each insurance policy required by the Agreement must be in effect at or prior to
commencement of work under the Agreement and remain in effect for the term of the Agreement. Failure to maintain the insurance policies as required by the Agreement, or to provide evidence of renewal, is a material breach of contract.

If requested by ASU, Supplier will furnish ASU with valid certificates of insurance. ASU’s project or purchase order number and project description will be noted on each certificate of insurance. The State of Arizona and ASU may require complete, certified copies of policies at the time of notice of any loss or claim.

E. **Subcontractors.** Supplier’s certificate(s) may include all subcontractors as insureds under its policies as required by the Agreement, or Supplier will furnish to ASU upon request, copies of valid certificates and endorsements for each subcontractor. Coverages for subcontractors will be subject to the minimum requirements identified above.

F. **Approval.** These insurance requirements are the standard insurance requirements of ASU. Any modification or variation from the insurance requirements in the Agreement will require the approval of ASU’s Department of Risk and Emergency Management.
SECTION XIII – MANDATORY CERTIFICATIONS

Fillable PDF versions of mandatory certifications are at: https://cfo.asu.edu/business/do-business-asu under the Formal Solicitations tab. ORIGINAL signatures are REQUIRED for either version.

CONFLICT OF INTEREST CERTIFICATION

________________________________  _______________ ________________
(Firm)        (Address)

________________________________
(Email Address)

________________________________
(Signature required) (Phone)

________________________________
(Print name) (Fax)

________________________________
(Print title) (Federal Taxpayer ID Number)

(Date)

The undersigned certifies that to the best of his/her knowledge:  (check only one)

(   ) There is no officer or employee of Arizona State University who has, or whose relative has, a substantial interest in any contract resulting from this request.

(   ) The names of any and all public officers or employees of Arizona State University who have, or whose relative has, a substantial interest in any contract resulting from this request, and the nature of the substantial interest, are included below or as an attachment to this certification.
FEDERAL DEBARRED LIST CERTIFICATION

Certification Other Responsibility Matters (April 2010)

_____________________

(Date)

In accordance with the Federal Acquisition Regulation, 52.209-5:

(a) (1) The Offeror certifies, to the best of its knowledge and belief, that—

(i) The Offeror and/or any of its Principals—

(A) (check one) Are (    ) or are not (    ) presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency; (The debarred list (List of Parties Excluded from Federal Procurement and Non-Procurement Programs) can be found at https://www.sam.gov/index.html/.)

(B) (check one) Have (    ) or have not (    ), within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, state, or local) contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; and

(C) (check one) Are (    ) or are not (    ) presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision.

(D) (check one) Have (    ) or have not (    ) within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds $3,500 for which the liability remains unsatisfied.

(ii) The Offeror (check one) has (    ) or has not (    ), within a three-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.

(2) “Principal,” for the purposes of this certification, means an officer; director; owner; partner; or, person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a subsidiary, division, or business segment, and similar positions).

(b) The Offeror shall provide immediate written notice to the University if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the certification will be considered in connection with a determination of the Offeror’s responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the University may render the Offeror nonresponsible.
(d) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the University may terminate the contract resulting from this solicitation for default.

_________________________________________  ________________________________
(Firm)                                        (Address)

_________________________________________  ________________________________
(Email Address)                                (Phone)

_________________________________________  ________________________________
(Signature required)                           (Fax)

_________________________________________  ________________________________
(Print name)                                    (Federal Taxpayer ID Number)

_________________________________________  ________________________________
(Print title)                                    (Fax)
ANTI-LOBBYING CERTIFICATION

Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions
(Sept 2007)

_____________________
(Date)

In accordance with the Federal Acquisition Regulation, 52.203-11:

(a) The definitions and prohibitions contained in the clause, at FAR 52.203-12, Limitation on Payments to Influence Certain Federal Transactions, included in this solicitation, are hereby incorporated by reference in paragraph (b) of this certification.

(b) The offeror, by signing its offer, hereby certifies to the best of his or her knowledge and belief that on or after December 23, 1989—

(1) No Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with the awarding of this contract;

(2) If any funds other than Federal appropriated funds (including profit or fee received under a covered Federal transaction) have been paid, or will be paid, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with this solicitation, the offeror shall complete and submit, with its offer, OMB standard form LLL, Disclosure of Lobbying Activities, to the University; and

(3) Offeror will include the language of this certification in all subcontract awards at any tier and require that all recipients of subcontract awards in excess of $100,000 shall certify and disclose accordingly.

(c) Submission of this certification and disclosure is a prerequisite for making or entering into this contract imposed by Section 1352, Title 31, United States Code. Any person who makes an expenditure prohibited under this provision or who fails to file or amend the disclosure form to be filed or amended by this provision, shall be subject to a civil penalty of not less than $10,000, and not more than $100,000, for each such failure.

________________________________  _______________ _________________
(Firm)        (Address)
________________________________  ______________________________
(Email Address)                                            ______________________________
(Signature required)                        (Phone)
________________________________  ______________________________
(Print name)                               (Fax)
________________________________  ______________________________
(Print title)          (Federal Taxpayer ID Number)
Voluntary Product Accessibility Template (VPAT)

A Voluntary Product Accessibility Template (VPAT™) is a document that explains how information and communication technology (ICT) products such as software, hardware, electronic content, and support documentation meet (conform to) the Revised 508 Standards for IT accessibility. VPATs™ help Federal agency contracting officials and government buyers to assess ICT for accessibility when doing market research and evaluating proposals.

Government solicitations which include ICT will specify accessibility requirements, indicating which provisions are required to ensure the deliverable is accessible. A VPAT™ is a good way to address the accessibility requirements defined in the solicitation.

All electronic and information technology developed, procured, maintained, or used in carrying out University programs and activities must be compliant with Sections 504 and 508 of the Rehabilitation Act of 1973, the Americans with Disabilities Act of 1990, as amended, other relevant local, state, and federal laws, and related university policies.

This VPAT was designed to provide information on how a product or service conforms to the section 508 accessibility standards (from the U.S. Access Board) for electronic and information technology (EIT) in a consistent fashion and format. Supplier must make specific statements, in simple understandable language, about how their product or service meets the requirements of the section 508 standards.

The proposer must access the current VPAT template by visiting https://www.section508.gov/sell/vpat and provide the completed form as part of their proposal, per the instructions of the RFP.

- Download the current VPAT™ template from the Information Technology Industry Council (ITI) website.
- Make it easy to find your product’s VPAT™ on your company’s website (e.g., link to it on the product description page).
SUPPLIER SUSTAINABILITY QUESTIONNAIRE – SMALL COMPANY

Firm Name: ___________________________ Date: ___________________________

The Supplier Sustainability Questionnaire must be completed and returned with your Proposal. This
questionnaire is applicable to firms that provide services as well as those that provide goods.
Arizona State University’s vision is to be environmentally sustainable while expanding our education,
research, and community support programs. The University seeks suppliers who share our
sustainability vision. Accordingly, please answer the following questions.

To each question please provide at least one of the following types of responses:

- An explanation or description
- A URL of your policy or program

An electronic copy of your illustrative policies or programs must be provided if requested. If the
question does not apply, answer with N/A and provide an explanation as to why.

Energy
1. What is your firm doing to be energy efficient?
2. What plan is in place to reduce greenhouse gas emissions in the future?

Solid Waste
1. What is your firm doing to reduce waste to landfill?
2. What plan is in place to reduce waste to landfill generated in the future?

Water Waste
1. What is your firm doing to reduce water waste?
2. What plan is in place to reduce water waste in the future?

Packaging
1. What is your firm’s plan to minimize packaging and/or describe your firm’s packaging “Take
Back” program?
2. What kind of reusable, recyclable, and/or compostable packaging materials does your firm
use?
3. What does your firm do to encourage/require your suppliers to minimize packaging and/or use
reusable, recyclable, or compostable packaging materials?

Sustainability Practices
1. What programs does your firm have to encourage your employees to use alternative
transportation while commuting to work and travelling locally?
2. What sustainability guidelines or environmental statement does your firm have to guide the
firm as a whole?
3. What are your firm’s sustainable purchasing guidelines?
4. What kind of position(s) or team(s) does your firm have dedicated to overseeing sustainability
initiatives?
5. List the sustainability related professional associations of which your firm is a member.
6. What kind of effort does your firm make to reduce the use of environmentally harmful
materials?
7. Does your firm use Green Seal/EcoLogo certified or biodegradable/eco-friendly cleaning
products?
8. Has your firm been cited for non-compliance of an environmental or safety issue in the past ten years?
9. Name any third party certifications your firm has in regards to sustainable business practices?
10. Describe any other initiatives your firm has taken to integrate sustainability practices principles into your operations.

Community
1. What charity, community development, educational programs, or environmental programs is your firm involved in within your local community?
2. What educational programs does your firm have to develop employees?

SUPPLIER SUSTAINABILITY QUESTIONNAIRE – LARGE COMPANY
Firm Name: __________________________ Date: __________________________
The Supplier Sustainability Questionnaire must be completed and returned with your Proposal. This questionnaire is applicable to firms that provide services as well as those that provide goods. Arizona State University’s vision is to be environmentally sustainable while expanding our education, research, and community support programs. The University seeks suppliers who share our sustainability vision. Accordingly, please answer the following questions.
To each question please provide at least one of the following types of responses:
- An explanation or description
- A URL of your policy or program
An electronic copy of your illustrative policies or programs must be provided if requested. If the question does not apply, answer with N/A and provide an explanation as to why.

Energy
1. What is your firm doing to be energy efficient?
2. What are your firm’s annual greenhouse gas emissions in metric tons of carbon dioxide equivalent? (Enter total metric tons of CO2 equivalency [includes the following GHGs: CO2, CH4, N2), SF6, HFCs and PFCs])
3. What plan is in place to reduce greenhouse gas emissions in the future?

Solid Waste
1. What is your firm doing to reduce waste to landfill?
2. What is your firm’s annual waste to landfill generated in metric tons? (Enter total metric tons)
3. What plan is in place to reduce waste to landfill generated in the future?

Water Waste
1. What is your firm doing to reduce water waste?
2. What is your firm’s annual water waste in gallons? (Enter total gallons)
3. What plan is in place to reduce water waste in the future?

Packaging
1. What is your firm’s plan to minimize packaging and/or describe your firm’s packaging “Take Back” program?
2. What kind of reusable, recyclable, and/or compostable packaging materials does your firm use?
3. What does your firm do to encourage/require your suppliers to minimize packaging and/or use reusable, recyclable, or compostable packaging materials?

**Sustainability Practices**
1. What programs does your firm have to encourage your employees to use alternative transportation while commuting to work and travelling locally?
2. What sustainability guidelines or environmental statement does your firm have to guide the firm as a whole?
3. What are your firm’s sustainable purchasing guidelines?
4. What kind of position(s) or team(s) does your firm have dedicated to overseeing sustainability initiatives?
5. List the sustainability related professional associations of which your firm is a member.
6. What kind of effort does your firm make to reduce the use of environmentally harmful materials?
7. Has an environmental life-cycle analysis of your firm’s products been conducted by a certified testing organization?
8. Does your firm use Green Seal/EcoLogo certified or biodegradable/eco-friendly cleaning products?
9. Has your firm been cited for non-compliance of an environmental or safety issue in the past ten years?
10. Name any third party certifications your firm has in regards to sustainable business practices?
11. Describe any other initiatives your firm has taken to integrate sustainability practices principles into your operations.

**Community**
1. What charity, community development, educational programs, or environmental programs is your firm involved in within your local community?
2. What educational programs does your firm have to develop employees?

If your firm is just beginning the sustainability journey, or is looking for tools and resources, here are some suggestions:

**Energy**
- Greenhouse Gas Protocol provides tools to calculate emissions that are industry specific: [http://www.ghgprotocol.org/calculation-tools](http://www.ghgprotocol.org/calculation-tools)

**Solid Waste**
- The EPA’s pre-built excel file to help measure and track your waste and recycling: [http://www.epa.gov/epawaste/hazardouswaste/inventoriesandreporting/measure-progress.htm](http://www.epa.gov/epawaste/hazardouswaste/inventoriesandreporting/measure-progress.htm)

**Water Waste**
EPA information about conserving water:
  o http://water.epa.gov/polwaste/nps/chap3.cfm

Packaging
  Links to get you started on sustainable packaging:
  o http://www.epa.gov/oswer/international/factsheets/200610-packaging-directives.htm

Sustainability Practices
  Ideas for alternative transportation programs:
  o http://www.ctaa.org/webmodules/webarticles/articlefiles/SuccessStoriesEmpTranspPrograms.pdf

  The EPA environmentally preferable purchasing guidelines for suppliers:
  o http://www.epa.gov/epp/

EPA life cycle assessment information:
  o http://www.epa.gov/nrmrl/std/lca/lca.html

Green Seal green products & services:

Ecologo cleaning and janitorial products:

EPA information on sustainable landscape management:
  o http://www.epa.gov/epawaste/conserve/tools/greenscapes/index.htm
SECTION XIV - SECURITY REVIEW

Security Review Form
Form version: 2017-04-13

Expectations

This checklist is to be filled out by the ASU project team, because the ASU project team is responsible for designing and implementing security controls. Vendor provided documents and diagrams are not sufficient.

Please have your answers -- in this checklist and in your Security Architecture Worksheet (example here) -- completed and your Security Architecture Diagram available in your google project folder one week before your scheduled review. Projects with incomplete documentation will be asked to reschedule.

A preliminary review may be held, and is recommended, early in a project's lifecycle while there is still time to change course if design issues are identified. The final review should be held shortly before the project goes live, when the contemplated servers have been set up at least to the point where the required vulnerability scans can be done.

Overview

The ASU security review process is designed to guide each project team to implement solutions efficiently while minimizing security risks. At the beginning of a project, for most of the questions below the answer will probably be "Unknown". As design and development continues, you can start filling in the answers you know. When you are ready for a discussion with an Information Security Architect, please use ServiceNow to submit a request for a security review.

Where you see the checkbox "□" symbol below, if that is your answer, delete the checkbox and replace it with an "X".

Projects do not always achieve a "perfect" score; however the goal is to reduce all risks to low or addressed. The purpose of this document is to allow management to get an evaluation of the risk in this project as compared to other projects and ASU standards.

Scope of Review

It is not practical to bring all existing systems up to current standards. Instead, our goal is "No new bad". So for each project we look at what changes are being made as part of that project. This includes:

- New hardware
- New software developed for the project: web sites or otherwise
- New software acquired, installed here, hosted elsewhere...
- New software in the form of a "cloud service" or similar
● New connections between new or existing systems
● New data flows between new or existing systems
● New data stores: added tables or columns, data files, network shares...

For our purposes "new" means new to ASU -- it has not been through an ASU Security Review before. So if ASU starts using an existing "cloud service" that service should be reviewed even if the service is not implementing any changes for ASU's project.

Also if an existing system is changed for the project, the change is "new" because it hasn't previously been reviewed.

Example: Existing system "A" regularly transfers a data file to existing system "B". The project will add software that runs on "B" and makes a new use of the data on "B". System "B" is in scope because it is being changed, but system "A" and the data file transfer are not in scope because they are not changing. System "A" can still be shown on your Security Architecture Diagram to clarify the workflow.

**Project Information**

What is the name of your project? Please use the same name that appears in project status systems.

[Blank]

If you are using Planview for project management, what is the Planview project ID number (usually 4 to 7 digits)?

[Blank]

☐ This project is not using Planview.

What is the purpose of your project? Briefly describe the business problem you are trying to solve.

[Blank]

Who is the Steward for the project (the ASU employee who decided we should do this, the sponsor from a business perspective)?
Name:
Title:
Department:

Who is the Technical Administrator for this system (the ASU employee who will manage ongoing system maintenance, enhancement and patching or manage the vendor who will perform this function)?
Name:
Title:
Department:
(For separation of duties reasons, the Steward and the Technical Administrator should not be the same person. Technical people implement business requirements. Technical people should not unilaterally create systems for which there is no business requirement or sponsor.)
### Responsibility for Secure Design

Security practitioners have found that to be effective, security measures must be "baked in from the beginning" rather than "pasted on at the end". This is one of the reasons for using a System Development Life Cycle (mentioned elsewhere in this checklist) that includes security checkpoints as the project progresses.

Attackers usually take advantage of mistakes. These flaws frequently arise at the boundaries between independent components, due to misunderstandings or weaknesses in how the parts are put together. This means you can have a collection of "secure" parts, but yet not have a secure whole. Someone must create a holistic design that ensures all the parts fit together in a way that complies with regulations and ASU standards.

### Who is responsible for the secure design of the entire system?

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>We don't know who is responsible for the security design of the entire system.</td>
</tr>
<tr>
<td>High</td>
<td>Although certain parts may be designed for security, nobody is responsible for the security design and ASU standards compliance of the entire system including users and their devices.</td>
</tr>
<tr>
<td>Medium</td>
<td>A vendor claims to be responsible for the security design and ASU standards compliance of the entire system, but the vendor has not signed ISO language, or the scope of the vendor's contracted responsibility does not cover the entire system including users and their devices.</td>
</tr>
</tbody>
</table>
| Low     | A single vendor has accepted responsibility for all of the security design and ASU standards compliance, has signed ISO language, and the scope of the vendor's contracted responsibility covers the entire system including users and their devices. If the vendor has signed or has intent to sign the ISO contract language ensure you provide a copy of the following documents from the vendor:  
  - SOC2 Report  
  - System Development Life Cycle (SDLC) |
| Addressed | One or more ASU employees have designed the system with a holistic security perspective from the beginning, selecting components and/or vendors that meet regulatory requirements and ASU standards. The ASU employee(s) responsible for the security design and ASU standards compliance are:  
  ____________________________________________  
  ____________________________________________ |

### Additional information (optional)


Sensitive Data

The expectations for the project's security measures depend on how much harm could occur when things go wrong. For definitions of the following data classifications please see the Data Handling Standard at http://links.asu.edu/datahandlingstandard

What is the most sensitive data in this project? (Check all that apply.)

Regulated Data

☐ PCI regulated (credit card data)
☐ FERPA regulated (student data)
☐ HIPAA regulated (health data)
☐ ITAR (import, export, defense-related technical data or foreign students)

ASU Data Classifications

☐ Highly Sensitive - disclosure endangers human life health or safety
☐ Sensitive - regulated data (including regulations above) or Personally Identifiable Information
☐ Internal - a login is required
☐ Public - anyone can see it without logging in

Additional information (optional) - examples of sensitive data elements etc.

Note: If you checked any of the highlighted boxes above, ASU’s Data Handling Standard calls for this data to be encrypted for all new systems, and an encryption transition plan for existing systems. In addition, encryption is recommended for all data classifications on all systems. If you can, encrypt everything everywhere.

One reason for encryption in transit is to prevent other computers on the network from reading sensitive data as it goes by.

How will sensitive data be protected in transit, as it travels across the network? (Check all that apply.)

☐ High Sensitive data will be traveling across one or more external connections outside of the ASU data Center without any protection.

☐ High All systems and connections storing or processing sensitive data are within the ASU data center, but sensitive data is not encrypted as it moves from system to system.

☐ High Firewalls, network segmentation, and/or other techniques limit sensitive traffic to only those systems that are intended to receive it. Other
systems are prevented from connecting, or listening to sensitive traffic. However, sensitive data is not encrypted in transit.

- Addressed

  All sensitive data is encrypted as it travels over each network connection.

- Addressed

  All* web sites are using https encryption. Servers have valid https certificates. (The certificates are correctly configured and installed so that no warnings are seen.)

- Addressed

  This project has no sensitive data.

- Addressed

  This question is not applicable for this project because all of the following are true:
  - No ASU equipment or network connections will be used to transmit sensitive data.
  - If a vendor is transmitting or receiving sensitive data, the vendor has accepted responsibility for protecting the data by signing a contract that includes ISO language.

Additional information (optional)

* Note: ASU Information Security recommends https encryption for all web pages, whether there is sensitive data or not. Here are some reasons:
  - Some Internet Service Providers have started altering page content so you don't see what you requested, you see what they want you to see. Thus even the simplest public static web page can be abused. The http protocol cannot detect this; https can.
  - An increasing variety of entities are interested in eavesdropping on your Internet use, which also becomes much harder under https.

Encryption at rest is a defense against the possibility that media might be misplaced, stolen, or not disposed of properly. Sensitive data should be protected wherever it goes -- on servers, desktops, laptops, mobile devices, and backups of these systems.

How will sensitive data be protected at rest, wherever it is stored? (Check all that apply.)

- High

  Sensitive data will be stored without any protection, on devices available to the general public without logging in.

- High

  Sensitive data will be stored without encryption at rest, even though PCI or other applicable regulations require it.

- Medium

  Sensitive data will be stored without encryption, but the devices require a login, and there is no applicable regulation requiring encryption at rest.
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>All systems storing or processing sensitive data are within the ASU data center, but sensitive data is not encrypted on disk. There is no applicable regulation requiring encryption at rest.</td>
</tr>
<tr>
<td>Low</td>
<td>Sensitive data is encrypted on disk, but not on backups. There is no applicable regulation requiring encryption at rest.</td>
</tr>
<tr>
<td>Addressed</td>
<td>All sensitive data is encrypted at every location where it is stored, including user devices and backups.</td>
</tr>
<tr>
<td>Addressed</td>
<td>This project has no sensitive data.</td>
</tr>
</tbody>
</table>
| Addressed| This question is not applicable for this project because all of the following are true:  
- No ASU equipment will be used to store sensitive data.  
- If a vendor is storing sensitive data, the vendor has accepted responsibility for protecting the data by signing a contract that includes ISO language. |

**Security Architecture Diagram**

For instructions on how to create a security architecture diagram, please see How to Create a Security Architecture Diagram. Note: this is a detailed technical diagram specific to your implementation at ASU. Vendor diagrams are usually NOT security architecture diagrams suitable as the roadmap for your review.

Include administrative interfaces. Although they may not be intended for users, they are still a potential point of attack and, given the privileged access they provide, are even more valuable to attackers.

A Security Architecture Worksheet (example here) is also required. It can help you gather the information needed for your diagram. You should find a blank worksheet in your security review folder. The information in your worksheet should match your diagram and vice versa.

Has a complete security architecture diagram been submitted?

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td><em><strong>RESERVED FOR SECURITY ARCHITECT SELECTION ONLY.</strong></em></td>
</tr>
<tr>
<td></td>
<td>There are one or more diagrams, but they are incomplete, inconsistent, or do not provide the necessary information (all endpoints with fully qualified DNS hostname or IP address, all connections with protocol, encryption type, and listening port). The rating is &quot;Unknown&quot; because there may be systems or connections that are not reviewed because they are not detailed on the diagram.</td>
</tr>
<tr>
<td>□ Unknown</td>
<td><em><strong>RESERVED FOR SECURITY ARCHITECT SELECTION ONLY.</strong></em></td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>A diagram has been submitted, but it is a vendor's generic diagram and does not show ASU specific systems, hostnames, IP addresses, connections, or other details. The rating is &quot;Unknown&quot; because there may be systems or connections that are not reviewed because they are not detailed on the diagram.</td>
<td></td>
</tr>
</tbody>
</table>

| □ Addressed | The security architecture diagram includes every endpoint that will be part of the project, and every connection between endpoints. Every endpoint that listens for connections is identified with its fully qualified DNS hostname and/or IP address. Every connection is labeled with protocol, encryption type if any, and port number on the listening device. |

| □ Addressed | The security architecture diagram includes every ASU specific endpoint and connection, but not vendor internal architecture. However all connections from ASU to the vendor's border are shown, and the vendor has signed a contract including ISO language accepting responsibility for adequately protecting ASU's sensitive data. Every ASU endpoint that listens for connections is identified with its fully qualified DNS hostname and/or IP address. Every ASU connection is labeled with protocol, encryption type if any, and port number on the listening device. |

If you checked one of the answers saying there is a diagram, please upload a copy of it to your google Security Review folder and fill in its document name here:  

Additional information (optional)  

☐ Has this project been to the Architecture Review Board? (Suggestion: share this document with ARB to provide advance answers to many possible ARB questions.)

**Servers**

As you look at your Security Architecture Diagram you will most likely see two types of endpoints: clients and servers. A server is any device that listens on a defined port for incoming connections.

Each server used by your project should be shown on the diagram (unless all connections to the server occur inside a vendor's "cloud", the vendor has signed ISO language, and ASU cannot make any changes to the server's software or configuration). If the server is new for your project, or is being changed for your project, the server should be scanned for vulnerabilities that may be introduced by your changes.

List each server's fully qualified **DNS hostnames** and/or IP addresses in the boxes below. (Note: A **DNS name is not a URL**. URLs for web servers are requested in a different question.)
Your Security Architecture Worksheet (example here) should already have this information on the first tab (endpoints) under the Servers heading.

Production (intended for normal use)

QA (should be virtually identical to production)

Development (for unfinished work, programmer testing etc.)

Additional information (optional)

Have the above servers been scanned or penetration tested for security vulnerabilities? What was the outcome? **Note:** ASU managed only - to request a server scan send email to scanrequest@asu.edu

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ Unknown</td>
<td>Some new or changed servers have not yet been scanned or penetration tested.</td>
</tr>
<tr>
<td>□ High</td>
<td>A scan or penetration test reported one or more high severity issues that have not yet been addressed.</td>
</tr>
<tr>
<td>□ Medium</td>
<td>A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).</td>
</tr>
<tr>
<td>□ Low</td>
<td>A vendor says the server(s) have been scanned or penetration tested and issues have been addressed but we do not have evidence (e.g. a copy of the report).</td>
</tr>
<tr>
<td>□ Addressed</td>
<td>All new servers have been scanned or penetration tested. No high or medium severity security issues were reported, or all issues have been addressed. Any fixes have been rescanned to confirm the fix. We have evidence of the scan (e.g. a copy of the report).</td>
</tr>
<tr>
<td>□ Addressed</td>
<td>This project has no new servers and no changes to existing servers (other than servers inside a vendor's &quot;cloud&quot; and the vendor has signed ISO language).</td>
</tr>
</tbody>
</table>

Additional information (optional)
Web Servers

Each device that accepts connections using the http (or https) protocol is a web server. In addition to the server vulnerability scan above, each web site on a web server should be scanned.

A "web site" is anything that responds to the Hypertext Transfer Protocol (HTTP) whether or not a traditional web browser is used. The term includes, for example, Web Services and device control interfaces, in addition to human-oriented "web applications".

To facilitate automated vulnerability discovery (scanning) a web site should have an entry point that provides links, directly or indirectly through intermediate pages, to all of the URLs offered by that site. For example, some web services use a WSDL to allow automated enumeration of the available calls and parameters. Any URLs that are not found by automated testing should be manually tested for potential security vulnerabilities.

The web site may offer more than one entry point, for example to support different user roles. In this case each entry point should be listed. Your Security Architecture Worksheet (example here) should already have some of this information on the third tab (web sites).

If your project includes new web sites or changes to existing web sites show their entry point URLs here:

Production (intended for normal use)

QA (should be virtually identical to production)

Development (for unfinished work, programmer testing etc.)

Additional information (optional)

Based on the above URLs, do the web sites have adequate test environments?
At present we don't know if there will be development or QA instances of the web site(s).

Only a production instance exists. There is no place to test code or changes without impacting live systems and data.

A QA or development instance exists, but it is different from production to the extent that there could be flaws in one environment that do not exist in the other.

All sites have QA instances that are sufficiently identical to production that the results of tests in QA can be relied on to evaluate the production instance.

This project has no web sites.

**Additional information (optional)**

---

**Have these new web sites or changes to existing web sites been scanned or penetration tested for security vulnerabilities? What was the outcome?** Note: For best results, we recommend scanning QA first, then after any issues are resolved and migrated to production, scan production to verify the fixes.

**NOTE:** ASU managed websites only - To request a web scan submit a web application scan through the MyASU Service tab (or here: [http://links.asu.edu/requestascan](http://links.asu.edu/requestascan)).

---

Some web sites have not yet been scanned or penetration tested.

A scan or penetration test reported one or more high severity issues that have not yet been addressed.

A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).

A vendor says the site has been scanned or penetration tested and issues have been addressed but we do not have evidence (e.g. a copy of the report).

All sites have been scanned or penetration tested, but the tests were not run against the production site or against a QA site that is essentially identical to production. No high or medium severity security issues were reported, or all issues have been addressed. Any fixes have been rescanned to confirm the fix.

All sites have been scanned or penetration tested against the latest version of code that has gone live or will go live. Tests were run against the production site or against a QA site that is essentially identical to what
is or will be in production. ASU has received evidence of the scan (e.g. a copy of the report.) No high or medium severity security issues were reported, or all issues have been addressed. Any fixes have been rescanned to confirm the fix.

☐ Addressed

This project has no web sites.

Based on the project's access to sensitive data, what is the proposed criticality rating of your web site(s)?

For a definition of "criticality" see the Web Application Security Standard at http://links.asu.edu/webapplicationsecuritystandard.

☐ High
The web site will have access to modify the authoritative source of sensitive data. (To request that an application be considered for ASU's High Criticality list, submit a request to your Security Review Architect.)

☐ Medium
The web site has access to sensitive data, but is not rated High.

☐ Medium-Low
The web site has confidential data, but not sensitive data. (Most web sites with a password fall in this category, unless they have sensitive data, which would be Medium or High.)

☐ Low
The web site only has public information. Web sites in this category do not use a password.

Database Servers

Servers that have databases containing sensitive data should be protected from various types of attacks. A database server directly connected to the Internet has no defenses except the ID and password that may be required. A database server directly connected to a web server may lose even that ID/password defense if the web server is compromised.

What database protections are in place?

☐ High
There are one or more databases with access to sensitive data. The database servers have publicly routable IP addresses and there is no firewall limiting connections to the database. People from anywhere in the world can connect directly to the database server.
<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>A database containing sensitive data is directly accessible by a web server, but the database only accepts requests from the web server. Other devices cannot make connections to the database.</td>
</tr>
<tr>
<td>Low</td>
<td>Web servers can connect to database servers directly, but alternate protections are in place to defend the database from a web server compromise, such as a Web Application Firewall in front of the web server. (Describe in the notes how the protective technology protects the database from a web server compromise.)</td>
</tr>
<tr>
<td>Addressed</td>
<td>Web servers cannot connect directly to database servers due to network segmentation, firewall rules, etc. Web servers interact with database servers through an application server that only permits a white list of known good transactions (a three tier architecture). Web servers also have defenses against typical attacks (such as SQL injection) via parameterized queries, stored procedures, or other techniques that do not pass arbitrary strings to the SQL command interpreter.</td>
</tr>
<tr>
<td>Addressed</td>
<td>None of the systems in this project have access to a database containing sensitive data.</td>
</tr>
</tbody>
</table>
| Addressed | This question is not applicable for this project because all of the following are true:  
- No ASU equipment will be used to store a database with sensitive data.  
- If a vendor has a database with sensitive data, the vendor has accepted responsibility for protecting the data by signing a contract that includes ISO language. |

Additional information (optional)

**User Authentication**

How do the project's systems verify user identity and access rights?

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>When a user logs in, their password is sent across the network without encryption. For example, users log in from a web page that does not use https encryption. Or as another example, users have client software on their computers which logs in to a server, but the connection to the server is not encrypted.</td>
</tr>
<tr>
<td>High</td>
<td>Passwords are stored in a way that if obtained by a hacker, the hacker could use them to log in. For example (1) the plain text of the password is stored, or (2) the password is encrypted at rest but the encryption could be reversed to obtain the plain text of the password.</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>High</td>
<td>One or more systems maintain an independent user authentication technique instead of standard ASU enterprise &quot;single-sign-on&quot; authentication systems such as WebAuth or CAS.</td>
</tr>
<tr>
<td>Medium</td>
<td>The login page uses https encryption and standard ASU enterprise &quot;single-sign-on&quot; authentication systems such as WebAuth or CAS, but subsequent pages revert back to http.</td>
</tr>
<tr>
<td>Low</td>
<td>Ordinary users are authenticated using standard ASU enterprise &quot;single-sign-on&quot; systems, but privileged users, such as site owners or administrators, are authenticated using a separate mechanism.</td>
</tr>
<tr>
<td>Addressed</td>
<td>All systems that require users to identify themselves use standard ASU enterprise &quot;single-sign-on&quot; authentication systems such as WebAuth or CAS.</td>
</tr>
<tr>
<td>Addressed</td>
<td>Access is in compliance with the ASU Privileged account standard: <a href="https://docs.google.com/file/d/0B7bqVGx3GJQbaC10bEl0ZndjVVE/">https://docs.google.com/file/d/0B7bqVGx3GJQbaC10bEl0ZndjVVE/</a></td>
</tr>
<tr>
<td>Addressed</td>
<td>Because all data is public, no user authentication is needed. Administrator access is controlled through existing mechanisms outside the scope of this project.</td>
</tr>
</tbody>
</table>

Additional information (optional)

**Servers Authentication**

When one server connects to another server, both ends of the connection should have a way to verify that the other server is the correct one and not an impostor.

**How do the project's servers authenticate each other?**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>One or more servers initiate or accept connections with their peers, but do not verify or otherwise restrict which servers can connect.</td>
</tr>
<tr>
<td>High</td>
<td>When a server logs in to another server, a password or other secret is transmitted across a network connection without encryption.</td>
</tr>
<tr>
<td>Medium</td>
<td>Firewalls, network segmentation, or other controls make it impossible for connections to be opened between anything other than the intended servers. Connections are limited by a &quot;black list&quot; identifying which addresses are not allowed to connect.</td>
</tr>
<tr>
<td>Low</td>
<td>Firewalls, network segmentation, or other controls make it impossible for connections to be opened between anything other than the intended servers. Connections are limited by a &quot;white list&quot; specifically identifying which addresses are allowed to connect, and denying all others by default.</td>
</tr>
</tbody>
</table>
Servers use credentials to identify each other, but there are weaknesses (explain in the notes). For example: (A) the credentials are not unique to one application (B) the credentials are not safely stored, or (C) it is difficult to change the credentials.

Each server uses a standard mechanism, such as https, to verify the other server's identity when initiating a connection to another server. If using https, servers have valid https certificates, and clients verify certificate validity. (The certificates are correctly configured and installed so that no warnings are seen.) The listening server authenticates the requesting server using credentials that are unique to this application. The credentials are not stored where they can be accessed without authorization. Credentials are periodically updated, and can be quickly updated if a compromise is suspected.

The project does not have more than one server, so there is no need for servers to authenticate each other.

The changes being made as part of this project will not affect a situation where two or more servers are communicating with each other, so the question does not apply.

Additional information (optional)

Vendor Involvement

This project is being done entirely by ASU employees, including development and hosting of all components.

If you did not check the box above, list the companies or people contributing to this project who are not ASU employees, and indicate when (if) the vendor agreed to ISO Contract Language:

Any vendor that provides hosting services, physical or virtual, has access to the data stored or processed there. Thus even hosting providers should be included in your list of vendors.

However if you contract with Vendor A and they subcontract with Vendor B, ASU may not require a contract directly with Vendor B. Vendor A may be responsible for Vendor B.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Date vendor signed contract with ISO language</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Revision June, 12, 2019
Is there a contract with each vendor, and does the contract include ISO language?
Note: ISO's standard contract language can be found [here](#) and is essential for contracts involving sensitive or highly sensitive data.

- **Unknown**: Status of vendor contract(s) or inclusion of ISO language is presently unknown.
- **High**: There are one or more vendors with whom we do not yet have a contract.
- **Medium**: There is a contract with each vendor, but one or more contracts do not include current ISO language. The vendor is not willing to change the contract to include ISO language.
- **Low**: There is a contract with each vendor, but one or more contracts do not include current ISO language. The vendor is willing to change the contract to include current ISO language.
- **Addressed**: There is a contract with each vendor, and each contract includes current ISO language.
- **Addressed**: This project has no vendor involvement.

Backup, Disaster Recovery, and Business Continuity Strategy

Systems should be able to recover from damaging events such as hardware failures or accidental or malicious data or software corruption.

What is the backup strategy?

- **High**: There are no backups of some or all systems that are relied upon to store data.
- **Medium**: Backups are being made, but the ability to fully restore after a total data loss has not been tested.
- **Low**: All essential systems are regularly backed up. Restore capability is tested at least once a year. If data or software damage or loss were to occur,
restoring the latest backup or reinstalling the software would be sufficient; the loss of updates since the last backup would be tolerable.

All essential systems are frequently and automatically backed up to a separate physical location. Restore capability is tested at least once a year. Audit logs or other mechanisms are in place that can back out accidental or malicious changes.

Not applicable. The systems involved in this project are not the authoritative store of any data. It could be recreated from elsewhere if lost, so no backups are needed. Original software install media and ASU-specific install instructions will be kept in a safe place so that the system can be rebuilt in the event of hardware failure or system corruption.

Additional information (optional)

For the following question, your project has "Mission Critical" components if any of the following are true:

- Any website associated with this project has a "Tier 1" rating. (The Web Application Security Standard at [http://links.asu.edu/webapplicationsecuritystandard](http://links.asu.edu/webapplicationsecuritystandard) defines these ratings.)
- There are regulatory requirements that mandate Disaster Recovery and/or Business Continuity planning.
- Your project sponsor wants this considered a "Mission Critical" system for some other reason (by whatever definition is meaningful to the sponsor).

A plan is recommended whether your project includes Mission Critical elements or not. However, expectations are higher for Mission Critical components.

□ This project has no Mission Critical components.

Have you documented and tested your disaster recovery and business continuity plan?

- Unknown: We do not currently know the status of Disaster Recovery and Business Continuity plans.
- High: This is a Mission Critical project but it doesn't currently have Disaster Recovery and Business Continuity plans.
- Medium: Disaster Recovery and Business Continuity plans don't exist at this time, however, the project is not Mission Critical.
- Medium: The Disaster Recovery and/or Business Continuity plans have been drafted, but key elements are missing, for example: redundant systems are not in place, contracts with vendors are not finalized, or the plan has not been tested.
<table>
<thead>
<tr>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>All mission critical components have geographically-dispersed redundancy with enough capacity to sustain mission critical operations during an extended loss of the primary systems. Disaster Recovery and Business Continuity plans are in place, complete with any contracts for vendor services during an adverse event. However, these are not regularly tested by staging mock disaster scenarios.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>All mission critical components have geographically-dispersed redundancy with enough capacity to sustain mission critical operations during an extended loss of the primary systems. Disaster Recovery and Business Continuity plans are in place, complete with any contracts for vendor services during an adverse event. Systems, plans, and recovery-critical personnel are tested annually by staging mock disaster scenarios.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Disaster Recovery and/or Business Continuity plan has been documented and tested, and there are no Mission Critical components. (Projects with Mission Critical components should choose one of the other answers.)</td>
</tr>
</tbody>
</table>

Additional information (optional)

If this project is "Mission Critical", please upload a copy of your plans to your google Security Review folder and fill in the document name(s) here:

Logging and Alerting

Please see ASU System Audit Requirements Standard [http://links.asu.edu/systemauditrequirementsstandard](http://links.asu.edu/systemauditrequirementsstandard) for information about what is required to be logged.

Systems should be designed to recognize and alert on typical attacks. For example, authentication or authorization systems should watch for brute force password attempts or other unauthorized access. Web servers, or protective appliances, should watch for the OWASP Top Ten Vulnerabilities and similar attacks.

**Do systems watch for undesirable or unexpected activity and log these events? Do logged events trigger alerts? What happens then?**

<table>
<thead>
<tr>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>No logging is performed on any system</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some systems do not recognize and log typical attacks, or other unexpected or undesired events.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential security events are logged, but there is no human or automated review of those logs to alert on possible problems.</td>
</tr>
</tbody>
</table>
Potential security events are logged, but the logs do not fully comply with the ASU System Audit Requirements Standard http://links.asu.edu/systemauditrequirementsstandard.

Logs are maintained in compliance with the ASU System Audit Requirements Standard http://links.asu.edu/systemauditrequirementsstandard, alerts are raised when appropriate, but staff may not be available to respond to the alerts.

Logs are maintained in compliance with the ASU System Audit Requirements Standard http://links.asu.edu/systemauditrequirementsstandard, events are raised when appropriate, and staff will be available to respond to the alerts throughout the lifecycle of the application.

Additional information (optional)

Software Integrity

Whoever writes your software gains control of your computer, sensitive data, and identity. Thus it is important to be sure the software comes from sources you trust. Verify the origin of software before installing it, and keep it up to date if security fixes have been released.

Current versions should be originally installed, upgrades should be applied when available, and security patches should be applied promptly. During original installation or subsequent updates, controls should be in place to ensure that all software comes from trustworthy authors, and has not been tampered with along the way.

Are current versions of software being deployed? Will upgrades and patches be promptly applied?

Some systems run outdated versions of their operating system, utilities, or installed applications. Or, systems are initially deployed with current software, but nothing will be in place to keep them current in the future.

There is a capability in place to distribute the most recent software version or updates, but it does not have controls to protect against fake (malicious) updates.

Initial install files and/or updates carry a signature (e.g. a hash or checksum) to verify file integrity, but the file must be (and will be) manually checked against a trusted list of valid signatures.

Software, including operating system, utilities, applications, and any other executable code, is only obtained from trusted sources. It is distributed using mechanisms that automatically ensure it is not altered, for example, files are cryptographically signed or delivered over a channel that ensures end-to-end file integrity. Current versions of software are initially
installed. Patching and upgrades are performed regularly and as needed. Patches are automatically verified so that administrators and users cannot be tricked into installing a malicious update.

☐ Addressed  This project does not include any new software. Nothing new is installed on user computers or on servers used by this system. There are no new web pages with code that runs on the server (for example, receiving form input) and no new web pages with code that runs on the browser (such as media players, Java, Active X, JavaScript etc.)

Additional information (optional)

ASU's Software Development Life Cycle (SDLC) standard (http://links.asu.edu/softwaredevelopmentlifecycle) calls for all software development to occur within an SDLC that includes information security controls and separation of duties to help ensure the controls are effective.

Is the software included in this project developed under a written Software Development Life Cycle?

☐ Unknown  We do not know if software (including vendor software, ASU developed software, or software obtained from other sources such as libraries or frameworks) is or was developed under the control of a written SDLC.

☐ High  One or more software components used within this project have no SDLC.

☐ Medium  An SDLC exists, but it is not written, it is not routinely followed, or it does not include security controls.

☐ Low  We have evidence that a written SDLC with security controls is routinely followed, however the development organization does not have enough people to implement full separation of duties.

☐ Addressed  All software (including vendor software, ASU developed software, and software libraries imported from other sources) is or was developed under the control of a written SDLC which includes security checkpoints and separation of duties to control the advancement of software past those checkpoints.

☐ Addressed  This project does not include any new software. Nothing new has to be installed on user computers or on servers used by this system. There are no new web pages with code that runs on the server (for example, receiving form input) and no new web pages with code that runs on the browser (such as media players, Java, Active X, JavaScript etc.)

If you checked one of the answers saying there is a written SDLC, please upload a copy of it to your google Security Review folder and fill in its document name here:
Has the new software developed or purchased in this project undergone vulnerability scanning or penetration testing by an entity other than the developer?

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>No vulnerability scanning or penetration testing has been conducted.</td>
</tr>
<tr>
<td>High</td>
<td>One or more components of new software (other than web sites) have not been vulnerability scanned or penetration tested.</td>
</tr>
<tr>
<td>Medium</td>
<td>Vulnerability scanning or penetration testing has been performed, but by a member or close affiliate of the development team or vendor, such that its independence is not assured.</td>
</tr>
<tr>
<td>Low</td>
<td>New software (other than web sites) has been vulnerability scanned or penetration tested by a party independent from the developer or vendor, however some issues remain unaddressed. The project team has evaluated the open issues and does not consider them a risk to ASU (explain in notes below).</td>
</tr>
<tr>
<td>Addressed</td>
<td>New software (other than web sites) has been vulnerability scanned or penetration tested by a party independent from the developer or vendor, and any issues found have been addressed.</td>
</tr>
<tr>
<td>Addressed</td>
<td>Vulnerability scanning or penetration testing is not required for this project because there is no new software other than web sites, and the web sites have been scanned for security vulnerabilities.</td>
</tr>
<tr>
<td>Addressed</td>
<td>This project does not include any new software. Nothing new has to be installed on user computers or on servers used by this system. There are no new web pages with code that runs on the server (for example, receiving form input) and no new web pages with code that runs on the browser (such as media players, Java, Active X, JavaScript etc.)</td>
</tr>
</tbody>
</table>

**Deprecated or Dangerous Technologies**

Frequently an exciting new technical capability is rapidly adopted without due consideration for the security consequences. Hackers begin taking advantage of weaknesses, so some technologies carry added risk. Users can defend themselves by disallowing unwanted technologies, but then some web sites refuse to serve those users until they place themselves at risk again.
Many of these techniques include automatically or manually downloading software from unknown or untrusted authors. Also see the **Software Integrity** section for additional questions that pertain to any executable code that is downloaded or installed such as a plug-in or media player.

**Does the project require any of the following technologies in order to make full use of the system?**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>Users are required to enable Java in their web browsers. (Due to a history of many vulnerabilities that go unpatched for months or years, Java has become one of the top malware distribution mechanisms.)</td>
</tr>
<tr>
<td>Medium</td>
<td>Users are required to permit Active-X controls. (Active-X controls give a web site more control of a user's computer, making it easier for attackers to exploit defects in the operating system, browser, or Active-X control itself. Also, dependence on Active-X locks out users of operating systems and browsers that may be more secure.)</td>
</tr>
<tr>
<td>Medium</td>
<td>A password protected web site imports JavaScript code or other client-executed code from another web site that is beyond ASU's control. (This makes it possible for the other site's script to perform identity theft against ASU users.) Users are not allowed to use essential features of the site if they protect themselves by disabling JavaScript.</td>
</tr>
<tr>
<td>Medium</td>
<td>A password protected web site imports JavaScript code or other client-executed code over an http (unencrypted) connection. (This makes it possible for a man-in-the-middle to inject a script to perform identity theft against ASU users.) Users are not allowed to use essential features of the site if they protect themselves by disabling JavaScript.</td>
</tr>
<tr>
<td>Low</td>
<td>Users are required to enable Flash in their web browsers. (Due to a history of many vulnerabilities that go unpatched for months or years, Flash has become a common malware distribution mechanism.)</td>
</tr>
<tr>
<td>Low</td>
<td>Users are required to allow pop-up windows in their browsers. (Several popular web browsers now disable pop-ups by default because they have been abused by advertisers and malware.)</td>
</tr>
<tr>
<td>Low</td>
<td>The web site only allows certain browsers, and refuses service to users of other browsers. (Such web sites frequently lock out users of operating systems and browsers that may be more secure.)</td>
</tr>
<tr>
<td>Low</td>
<td>Users are required to enable or install other plug-ins or media players not listed above. (Please describe in notes below.)</td>
</tr>
<tr>
<td>Addressed</td>
<td>The project uses one or more of the above technologies, but they are entirely optional. Users can still accomplish all the functions of the system even if the user shuts off the deprecated technologies.</td>
</tr>
<tr>
<td>Addressed</td>
<td>The project will not use any of the technologies listed in this section.</td>
</tr>
</tbody>
</table>

Additional information (optional)
Other Risks

If you are aware of other risks you would like to document, describe them here and assign what you think is the appropriate risk rating, considering the classification of the data involved. (Copy and paste a table cell containing the rating you want to apply.)

<table>
<thead>
<tr>
<th>□</th>
<th>□</th>
<th>□</th>
<th>□</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Additional information (optional)

Risk Score

Total up the boxes checked above. Each question should have at least one box checked.

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Unknown</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count of boxes checked</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Risk Acceptance

After your documents are complete and the review discussion has been held, someone will be asked to accept any remaining risk. Please be aware that if your Risk Score includes any **Red** items, the ASU Provost or CFO will be asked to accept the risk. **Orange** items go to the sponsoring business unit’s Dean or comparable leadership for risk acceptance. **Low** risks may be accepted in writing by a member of the project team.
Upon award, the successful Proposer(s) is expected to submit a Security Architecture Diagram.

How to Create a Security Architecture Diagram  
Revised 2016-05-27

This describes how to make a Security Architecture Diagram for a security review.

Here is the information you will need to gather to create a Security Architecture Diagram:

- Identify each role your new system will support. A role is a group of users who can all do pretty much the same things. For example your system may offer one collection of services to students and other services to faculty. These are two roles. Roles may also depend on the type of device being used. For example if mobile devices use an "app" instead of using the web site provided for desktop users, you probably have a mobile users role and a desktop users role, although different descriptions may be more applicable.
  - Don’t leave out the administrators. The administrator role is an important part of system maintenance, and privileged roles are an attractive hacker target.

- Identify each endpoint in the system. Each role will be an endpoint, and each type of server is also an endpoint. Endpoints include any device that sends or receives data. But if there are multiple devices that perform the same operation, they can be represented as a single endpoint. For example, we don’t need to distinguish each end user computer when they all do the same thing. Similarly, if there is a cluster of identical servers doing the same thing, that’s one endpoint.

- Identify each connection between endpoints. If data is moving, there must be a connection to carry it. But unlike a data flow diagram, what matters here is not which way the data flows (it might be both ways) but which endpoint initiates the connection. Usually a connection is requested by a client (for example, your web browser) and accepted by a server (the web site). The server is listening for connections, usually on a predefined port.

- If you make backups, that is yet another data flow from one endpoint to another. How does the data get there? Show the connection if it is network based, or describe the physical security if sensitive data is moved by hand (e.g. backup tapes to a vault).

- For each server, determine what IP address and/or Fully Qualified DNS hostname will be used by the server, and on what port(s) it will be listening. What protocol is being used to communicate over each connection? Is the data protected in transit? How do the endpoints of the connection authenticate each other? (How do they verify that they have connected to the correct endpoint?)

You are now ready to start making your drawing.
Choose a symbol to represent the endpoints. Typically this is a box, but it could be something else. Draw a box (if that’s your choice) for each endpoint. Again, that would be one box to represent all the users who share a single role, and another box for each server (or group of identical servers). If different users connect to different servers, that would be a distinct endpoint. Don’t forget the users! The system can’t work without them.

Label endpoints that are permanent (e.g. servers) with their IP address and/or Fully Qualified DNS hostname*. Users, of course, come and go all the time, and their IP address or name doesn’t matter.

Choose a symbol to represent the connections. Typically this is a line, but it could be something else. Draw a line (or whatever) from each endpoint to each other endpoint with which it communicates.

Choose a symbol to identify which end of the connection is the client and which end is the server. Remember that the server is passively listening on a port for requests, and the client is initiating those requests. You could represent this, for example, by an arrowhead on the server end of the line, indicating that the client sends a connection request to the server.

Near the server end of the connection, identify the port number on which the server is listening.

Indicate the communication protocol used by the connection. For example, a web site may use the http or https protocol. Even for public sites, https is preferred.

Describe, on the diagram or elsewhere, what type of data is flowing along each connection. Is it confidential? Regulated? If the data is sensitive, describe how it is protected in transit. For example, is it encrypted? Using what type of encryption? Describe any controls to limit who or what can connect and fetch the information.

If there is confidential or sensitive data, describe how it is protected at each endpoint of the connection. Is it encrypted at rest? If so, how? Is the endpoint protected by a firewall? If so, what does the firewall block or allow? Is the data viewed but not stored (e.g. by a client) so that secure storage is a non-issue?

*See https://en.wikipedia.org/wiki/FullyQualifiedDomainName

Summary

So for each server (anything that accepts connections) you should have:

- Fully Qualified DNS name and/or IP address
- Description of what it is or what it does (web server? database?)

For each connection you should have:

- Port number where the server is listening
- Protocol (http, ssh...)
- Sensitivity of data flowing across that connection
- Protection of data flowing across that connection, if it is not public (encryption? what type?)
- If the server authenticates the client, how? (User ID and password?)
- If the client authenticates the server, how? (For example https uses a server certificate signed by a known certificate authority, which the client can verify.)

Additional Info

It may also help to distinguish existing endpoints, to which you will merely connect, from new endpoints that will be created as part of your project.

It may also help, if it is not obvious, to briefly describe the role or purpose of certain endpoints. For example: web server, database server, normal user, administrative user -- don’t forget to show them too if they use different connections! Use consistent and unique names throughout; don’t call it the “data server” here and “MySQL server” somewhere else and “repository” a third place.

It is not necessary to show disk drives that are physically within a single server. However network shares are most likely part of a file server, and the file server should also be shown as a distinct endpoint.

When you are done, save your diagram in a format that will open on other types of computers (e.g. pdf) for people who may not have your software.

EXAMPLES
The diagram need not be colorful. Although this diagram (below) is very simple, it conveys all the requested information. Visual appeal can be beneficial, but the factual information is what really matters.
# APPENDIX 1 - RFP CHECKLIST/COVER PAGE

The following documents are required for this proposal (please mark off each document to acknowledge that you have submitted the document in the proper order and format):

<table>
<thead>
<tr>
<th>Document</th>
<th>Marked</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFP Checklist/Cover Page, Mandatory Certifications, Voluntary Product Accessibility Template (VPAT), &amp; Supplier Sustainability Questionnaire.</td>
<td>☐</td>
</tr>
<tr>
<td>Proposer Qualifications, Section VII</td>
<td>☐</td>
</tr>
<tr>
<td>Response to the Specifications/Scope of Work, Section V</td>
<td>☐</td>
</tr>
<tr>
<td>Pricing Schedule, Section IX (Attachment A)</td>
<td>☐</td>
</tr>
<tr>
<td>Exceptions to Terms and Conditions reviewed by Legal or Contract team and Insurance Requirements acknowledged, Section XII</td>
<td>☐</td>
</tr>
<tr>
<td>Confidential/Proprietary Justification Letter with Sealed documents, if applicable. Section IV, page 9, item 9.</td>
<td>☐</td>
</tr>
</tbody>
</table>

In addition, the proposer must provide their review and acknowledgement of the following documents provided in this RFP. Please mark off each box to acknowledge that you have reviewed the below documents in the RFP:

<table>
<thead>
<tr>
<th>Document</th>
<th>Marked</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFP 301905 (PDF Document)</td>
<td>☐</td>
</tr>
<tr>
<td>All RFP Addenda (PDF Document)</td>
<td>☐</td>
</tr>
<tr>
<td>Attachment A – Pricing Schedule (Excel Document)</td>
<td>☐</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Point of Contact Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Email Address</th>
<th>Phone #</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>