Arizona State University

January 11, 2019

REQUEST FOR PROPOSAL

COMPUTER AIDED DISPATCH, RECORDS MANAGEMENT SYSTEM, & MOBILE DATA SYSTEM FOR THE ASU POLICE DEPARTMENT

RFP 341904

DUE: 3:00 P.M., MST, 02/22/19

Deadline for Inquiries	3:00 P.M., MST, 02/07/19
Time and Date Set for Closing	3:00 P.M., MST, 02/22/19

TABLE OF CONTENTS

TITLE **PAGE**

SECTION I – REQUEST FOR PROPOSAL

RFP 341904

Arizona State University is requesting sealed proposals from qualified firms or individuals for **Computer Aided Dispatch, Records Management System, & Mobile Data System for the ASU Police Department.**

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 3:00 P.M. MST February 22, 2019. 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

No telephone, electronic or facsimile proposals will be considered. **Proposals received after the time and date set 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

DocuSigned by:
9A7881725D4C414...
Lorenzo Espinoza, Senior Buyer

LE/KD

SECTION II – PURPOSE OF THE RFP

1. INTENT

The Arizona State University Police Department seeks to purchase and institute a public safety-based Computer Aided Dispatch System, Mobile Data System, and Records Management System that will afford each of the four (4) identified campus locations, as well as future locations, to effectively share criminal justice and public safety incident information data between locations in a secure manner. Each module should interoperate as a holistic solution as well as have the capability to integrate with other various value-add applications that make Police dispatch centers a hub for all policing activity. ASU Police understands that over the past few years many CAD/RMS solutions have evolved to highly end-user configurable and user-friendly solutions that are far more effective and efficient than the existing system in every area, from Dispatch to Records to the end users in the field. The ASU PD has decided to move forward with a plan to replace the department's existing CAD, RMS, Mobile Computing, and Property Systems to meet the departments growing needs. The system network will be required to provide standard deliverables for a police computer-aided dispatch that manages calls for service for law enforcement, and emergency management, as well as the standards for the Arizona Criminal Justice Information System (ACJIS). Additionally, the University requires this product to meet the standards to integrate with Arizona Uniform Crime Reporting System, with the ability to transition and report to the National Incident Reporting System and provide immediate reporting to meet the requirements of the Federal Jeanne Clery Act. The solution is expected to also integrate to various other applications and work within our ASU technology environment and innovative strategies moving forward.

2. BACKGROUND INFORMATION

Arizona State University Police Department's mission is to foster a safe, community-centered environment through engaged collaboration committed to dignity and respect while promoting a safe and secure campus environment for students, faculty, staff, and visitors. We provide quality police services ethically, fairly and equally in partnership with the members of our community. The ASU Police ranks as the 20th largest agency in Arizona and is a CALEA and ICALEA accredited department.

ASU Police provides first-response public safety services to the Tempe, Downtown Phoenix, Polytechnic, and West campuses, which are situated throughout the Phoenix metropolitan area. ASU Police headquarters is located on the Tempe campus whose population is similar to a small city. ASU Police and currently employs 92 sworn officers and 80 support personnel including civilian police aides. Patrol efforts are divided between four campuses, which includes roving lieutenants who support each campus when needed. ASU police officers face the same challenges as municipal agencies across the country. All sworn officers are equipped with body cameras and other technology, to categorize and review evidence from their smartphones, as well as have access to the dispatch center headquarters and other operations centers that utilize other technological applications that enhance our situational awareness and provide effective communications with our staff and our public.

The Department headquarters houses a 24-hour full-service police communications center, which provides dispatching services for all four campuses for law enforcement and ASU special events, and is the primary 9-1-1 public safety answering point (PSAP) for the university. Dispatchers monitor Motorola public safety radio consoles in addition to answering incoming administration and 911 calls. Dispatchers monitor the Arizona Criminal Justice Information System ("ACJIS"), fire alarms, across all University properties, and closed-circuit cameras. Dispatch uses an emergency alert system to notify each campus community of life-threatening situations on campus and in the immediate area.

The Records division uses an RMS database, which houses current and some historical case files. The files are used to query UCR, and Clery reports required by the State and Federal entities. The records division currently depends on a suite of public safety records and management system to ensure all public safety incidents occurring on and about its jurisdiction are appropriately documented. In its current design, there is a significant level of duplication to ensure all records systems contain all relevant and required information. It is the goal of this initiative to create a system with a single data entry platform to record and manage all incidents on campus.

The ASU Police Department currently uses Tyler Technology's New World CAD, RMS, and Mobile Data Computing solutions, which were procured in 2004.
These applications have been satisfactory for many years, but are no longer meeting the needs of the department. In addition to the Tyler Technology's New World applications mentioned above, the department also uses LexisNexis for online reporting. Some systems in use, many of which are stand-alone, characterizes the current public safety technology environment. Some of these applications are national, regional or county databases, while others were implemented to augment in the existing systems. The current version inhibits efficiency and prevents other modules from auto-populating information for a streamlined effect.

Current ASU PD hardware includes:

- Currently operating in a Windows 7 environment
    - 2 IBM Servers – a Message Switch and backup
    - Microsoft SQL Database
- 100 workstations across 4 campus locations which includes:

- 6 dispatch workstations
- 2 CAD development/test computers
- Administrative Personnel
- 8 Records workstations
- Report writing
- Sergeants
- Investigations
- Evidence
- Crime Prevention
- Fleet Supply
- Briefing
- Lobby
- 27 Mobile units

Arizona State University (ASU) is among the largest public universities in the nation with over 100,000 students enrolled and a Level One-designated research institution that houses over 1 million square feet of research and classroom laboratory space on four geographically separated campuses. The four main campuses span a 60-mile distance across the Phoenix metropolitan area and are adjacent to seven different city, county, and tribal jurisdictions. With such a large geographical area and the presence of mass amounts of people, assets, and research or intellectual property, the need for immediate, detailed access to vast information (human or social, hazardous and high-security, or physical or tangible-property) is critical to operations. It is imperative that data sharing capabilities and interfaces between CAD/RMS/Mobile systems and other ASU systems are leveraged. Such systems ASU currently have in place, but not all are integrated include: the environmental health and safety hazardous materials management system, radio/voice systems, mass communications system, video management system, business intelligence systems, and more. The University wishes to capitalize on data sharing capabilities between the proposed CAD/RMS/Mobile system and the new hazardous materials management system that contains location, acquisition, dissemination, and dilution and destruction information. The current Hazardous Materials Management System incumbent is OnSite Systems.

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 of more than 600 buildings that include classrooms, laboratories, residential complexes, residential housing, three public elementary schools, and a high school and is comprised of 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 100,000 students and 12,000 staff/faculty 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.

ASU has locations across the nation and provides auxiliary services to each and every location including:

- ASU Tempe
- ASU Downtown
- ASU Thunderbird Global Management Downtown
- ASU Polytechnic
- ASU West
- ASU SkySong
- ASU Lake Havasu
- ASU Research Park
- ASU Santa Monica
- ASU Washington DC
- ASU China

The four major campuses that make up the Phoenix metropolitan area are the Tempe campus, the Polytechnic campus in Mesa, the West campus, which straddles Phoenix and Glendale, and the Downtown Phoenix campus. The Tempe campus is an open, urban campus located in north Tempe, which is in the center of the Phoenix metropolitan area. This campus is traversed by major surface roads that carry heavy commuter traffic loads as well as by the main east/west valley freeway, SR 202. A heavily used Southern Pacific Rail Line cuts across the southern portion of the campus. The northern end of the campus falls under the final approach pathway of Sky Harbor International Airport, the nation's 6th busiest airport. Future growth includes the Novus and Maribelle projects, which will open the campus up to new experiences with a 365 venue, along with an active retirement community.

The Tempe campus, due to its centralized location, is host to thousands of visitors who attend conferences, meetings and special events at campus theaters, museums, conference centers, and sports stadiums. The Tempe campus regularly hosts high-profile visitors, including the more recent 2016 debates involving Presidential hopefuls at two of the campuses, Tempe and Downtown. Other past visitors have included: U.S. Presidents, Vice-Presidents, members of the U.S. Congress, Supreme Court Justices, foreign dignitaries, and controversial writers and speakers.

The ASU Polytechnic campus is located on the eastern edge of the metropolitan area and adjacent to the cities of Mesa, Gilbert, and the Gila River Indian Community. Adjacent to this campus is the Williams Gateway Airport. This airport is an FAA-designated reliever airport to Phoenix's Sky Harbor and slated to become a regional passenger terminal.

The ASU West campus is located in the west valley and is adjacent to the cities of Phoenix and Glendale. This campus is also host to conferences, art museums and lectures by high profile visitors.

A major expansion to ASU occurred in 2009 with the addition of the Phoenix Downtown Campus. Residential and Academic sites have made a footprint in the downtown Phoenix area. The compliment to this growth of this campus has had a positive impact in the area while continuing to enrich the future growth of education in Downtown Phoenix.

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 one (1) year(s) with the possibility of four (4) 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 specified in the Pricing Schedule. Note: Alternative terms cannot be in lieu of the term stated above.

SECTION III – PRE-PROPOSAL CONFERENCE

No pre-proposal conference will be held.

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 Road 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

   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 Ave 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.

Should: Indicates something that is recommended but not mandatory. If the proposer fails to provide recommended information, the University may, at its sole option, ask the proposer to provide the information or evaluate the proposal without the information.

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. Arizona State University is also a member of the Strategic Alliance for Volume Expenditures ($AVE) cooperative purchasing group. $AVE includes the State of Arizona, many Phoenix metropolitan area municipalities, and many K-12 unified school districts. Under the $AVE Cooperative Purchasing Agreement, and with the concurrence of the proposer, a member of $AVE may access a contract resulting from a solicitation done by the University. If you **do not** want to grant such access to a member of $AVE, **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.

22. Administrative Fee. Licensor will pay ASU an Administrative Fee in the amount of 1% of the gross funds received by Licensor from 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 Agreement. The Administrative Fee will apply to any and all Deliverables provided by Licensor that reference the Agreement or the RFP as the supporting documentation to meet competitive bidding requirements. The Administrative Fee will be calculated based on all sales transacted, minus all taxes and any returns or credits. Licensor will submit the Administrative Fee, along with a quarterly usage report documenting all contract sales, to the ASU Chief Procurement Office

within 30 days following the end of each calendar quarter. Each quarterly report at a minimum, will disclose all purchased Deliverables, prices paid, and quantity, by individual purchasing agency, for all sales within the calendar quarter just ended. The Administrative Fee is payable by Licensor, from Licensor's funds, to ASU.

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:

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

Tel: 480-965-3849
E-mail: Lorenzo.Espinoza@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

1. Overview
   a. Arizona State University Police Department is looking to purchase a fully integrated turnkey system that includes a Computer Aided Dispatch System, Records Management System, Report Writing, Mobile Field Reporting, Training Management system, Property Module, and connectivity to local, county, and state agency systems. The vendor selected will be responsible for the implementation of all selected components, project management, training, data migration, and providing a complete installation that meets the performance requirements as stated in the final contract.

   b. ASU expects awarded Contractor to perform the planning, design, implementation, and support of the CAD/RMS system. The solution must be multi-agency/disciplinary products that can support Law Enforcement based operations, as well as integrate with Fire and EMS dispatching. The Contractor is expected to provide software, hardware, and related services, as further described under Specifications/Scope of Work of this RFP.

   c. The proposer may provide either a cloud-based solution or a hosted/virtual environment as part of their proposal. ASU will determine during the evaluation of proposals what is most advantageous to the University.

   d. The solution's mandatory minimum integrations is listed in the "Interface Functional Requirements" in item 2.i under General System Requirements.

      The solution should also leverage other capabilities and should integrate to various other applications and work within our ASU technology environment and innovative strategies forward.

      Currently, ASU utilizes the applications referenced in 2.i and is interested in solutions with integrations to any or all of these applications or more, which may be annotated in the attached spreadsheet under "Interface Functional Requirements".

   e. <u>**INSTRUCTIONS TO PROPOSERS FOR SECTION V**</u>: Please fill in details about how your application, technologies, and/or services will provide the following features/functionalities/services, including examples of previous projects (if applicable). The proposer may request a Word Document version of Section V. <u>**Please reply directly underneath each item below in Section V for ease of evaluation.**</u>

______________ Place an "X" on the line acknowledging this section.

f. The proposer should request from ASU Purchasing Lorenzo.Espinoza@asu.edu the following documents:

- Word Document for Appendix 1 – RFP Checklist/Cover Page
- Word Document for Section V Specifications/Scope of Work
- Word Document for Section VII Qualifications
- Excel Document for Attachments 1-7 (Referenced in Section V)
- Excel Document for Attachment A Pricing Schedule (Referenced in Section IX Pricing Schedule)
- Word Document for Section XIII Supplier Sustainability Questionnaire
- Word Document for Section XI – Proposer Inquiry Form
- PDF Document for Section XIII – Mandatory Certifications

_____________ Place an "X" on the line acknowledging this section.

2. General System Requirements

a. This section delineates in detail the specific functions required of the system requested. It does not describe how a proposed system is to implement these functions, as each vendor's system will be unique in that respect. Proposers shall also list all exceptions to the functions specified in this section. Failure to do so may cause for disqualification, a lower evaluation score, or the University may direct the vendor, if selected, to implement the missing features at no cost to the University.

b. All proposers must place a check or an "X" to the appropriate letter as indicated below in the response column of the following Attachments 1-7, found in sections 2.c-i:

S = Standard in software. The requirement is met by vendor's base product.

- Please explain any line items that are not an "out of the box" standard but are part of your overall proposal; specifically, why the particular line item is not an "out of the box" standard. Additionally, please identify what potential effect this may have upon meeting a January 13, 2020 implementation date. (Required for any items marked "M", "A", or "U") Your proposed solution will be evaluated based on the value of each of these items combined and will not negatively impact the proposal.

M = Modifications needed, at no additional cost. Base product has this feature or function, but some modification will be required to meet the specific requirement. Explain any modifications required in each exhibit of your proposal and note the reference number in the reference column in the table. Cost, if any, must be itemized in the Pricing Schedule.

A = Modifications needed at additional cost. The vendor's base product does not contain this function or feature, but it will be added to meet this requirement. Cost, if any, must be itemized in the Pricing Schedule.

U = Unable to meet the requirement

____________ Place an "X" on the line acknowledging this section.

c. CAD System Functional Requirements

- Key to the Computer Aided Dispatch portion of the system is incident handling. Since this is a particularly critical function, it is important that its implementation be as complete and easy to use as possible.
- Please see the attached Excel Spreadsheet Attachment 1 - CAD System Functional Requirements that must be completed in order to be considered for this RFP.

____________ Place an "X" on the line acknowledging this section.

d. Field Reporting Functional Requirements

- Please see the attached Excel Spreadsheet Attachment 2 - Field Reporting Functional Requirements that must be completed in order to be considered for this RFP.

____________ Place an "X" on the line acknowledging this section.

e. Global Functional Requirements

- Please see the attached Excel Spreadsheet Attachment 3 - Global Functional Requirements that must be completed in order to be considered for this RFP.

____________ Place an "X" on the line acknowledging this section.

f. Mapping Functional Requirements

- Please see the attached Excel Spreadsheet Attachment 4 - Mapping Functional Requirements that must be completed in order to be considered for this RFP.

____________ Place an "X" on the line acknowledging this section.

g. RMS Functional Requirements

- Please see the attached Excel Spreadsheet Attachment 5 - RMS Functional Requirements that must be completed in order to be considered for this RFP.

____________ Place an "X" on the line acknowledging this section.

h. Mobile Functional Requirements

- Please see the attached Excel Spreadsheet Attachment 6 - Mobile Functional Requirements that must be completed in order to be considered for this RFP.

____________ Place an "X" on the line acknowledging this section.

i. Interface Functional Requirements

- Please see the attached Excel Spreadsheet Attachment 7 - Interface Functional Requirements that must be completed in order to be considered for this RFP.
- Included in Attachment 7 – Interface Functional Requirements allows the proposer to list additional integrations that are offered/available from your proposal.

____________ Place an "X" on the line acknowledging this section.

3. Compatibility and IT Requirements/Specifications

a. Does the proposer confirm that all user-facing (non-administrative) aspects of the Application are browser-based via HTTPS protocol (e.g. browser does not require additional software plugin to access Application via browser) and the application is updated to support new versions of browsers as they are released? Please describe browsers and versions supported. If not applicable, please describe your proposed solution in a hosted/virtual environment.

Answer:

b. Does the application support the American with Disabilities Act/Section 508?

____________ Yes

____________ No

c. Is the system accessible from a mobile device in a user-friendly format (e.g. Responsive web design)?

____________ Yes

____________ No

If yes, please provide links or samples of the responsive web design.

Answer:

d. Does the mobile device usage features include offline mode for relevant modules (e.g. for tablet-based inspection of high-containment areas with no WIFI access)?

Answer:

e. Does the system feature a refresh option or warning message for auto logout due to inactivity; or else saves session to resume upon login?

____________ Yes

____________ No

If yes, please provide screen shots to demonstrate this capability.

Answer:

f. Does the proposer's application support Shibboleth for federated identity integration (i.e. single sign-on)? If not currently supported, willingness to adopt this support (Reference: http://shibboleth.net/) or to meet the requirement via CAS, InCommon, or provision of SSO using federated identity management system?

   Answer:

g. Does the application features extensible web services (e.g. REST/SOAP/custom API) to allow inbound and outbound integrations with other systems?

   Answer:

h. Does the application allow uploading data from file (e.g. Excel)? Please describe and list the different file types/formats for exported reports.

   Answer:

i. The proposer will provide technical documentation of the application. Preferably, the system data model/dictionary, and API documentation are made available to assist in the full, correct, and efficient utilization of the application, including accurate report generation and data analysis.

   Answer:

j. Does the application use ANSI SQL-compliant database backend (e.g. MSSQL/MySQL)? Direct access to database, via a virtual environment or an on-premise hosted database is to be provided. If this is not possible, capacity to replicate data to an ASU data warehouse environment could meet this requirement provided the Application frontend administrative features can sufficiently interact with the backend environment to meet the use cases detailed throughout this RFP.

   Answer:

k. The proposer must describe their applications Administrative/Power User roles capable of configuring granular access permissions for other users.

   Answer:

4. Hardware Requirements
   a. The proposer must describe the necessary topology and architecture of the recommended solution as it would be best served for ASU. The proposer should provide detailed plans on how they will perform steps needed to upgrade the current systems and networks, work with ASU to locate services to the cloud, or operate in a SaaS model for their solution. The current ASU hardware situation can be found in Section II Background.

Answer:

5. Project Management, Training, Support, and Implementation
    a. The successful proposer must provide training and installation support to ensure all new users thoroughly understand the product and become effective as quickly as possible. Thorough and complete online training should be available at no cost. The successful proposer must provide a detailed work plan on how installation, implementation, and training is provided, and an estimated lead-time for installation, implementation, and training should be provided.

        Answer:

    b. The proposer must name in the proposal a project manager with their resume to be assigned as a single point of contact to the University to coordinate and direct the vendor's activities and communications between the University and the proposer.

        Answer:

    c. The proposer must conduct User Acceptance Testing at minimum 60 days prior to training sessions to allow ASU Police Department subject matter experts (that may include but not limited to dispatchers, records personnel, officers, managers, etc.) to familiarize themselves with the software. Through trial and review, the system component process should meet mutually agreed-upon requirements. Final User acceptance Testing (UAT) is based on the specifications of the end-user. ASU Police Department's CAD/RMS Project team will work with the successful proposer to develop the acceptance criteria and the state will have final approval of acceptance criteria. The vendor shall then conduct formal training sessions to familiarize all department personnel in operation of the system. The vendor shall describe the training program proposed, the number of days of training included, and the number of training days proposed to each class of user: dispatchers, records personnel, officers, administrators, and system support personnel.

6. Service Level Agreements (SLAs)
    a. Describe your firm's tiered service levels, including guaranteed incident response and resolution times with associated pricing.

        Answer:

    b. Describe your firm's details on guaranteed uptime.

        Answer:

    c. Describe your firm's email/videoconference/telephone support/hours of operation.

        Answer:

    d. Describe your firm's ability for 24/7 monitoring of application and cloud infrastructure with notification triggers (if applicable).

        Answer:

e. Describe your firm’s Disaster Recovery Plan to your proposed software product.

Answer:

f. Describe your firm’s policies to Downtime & Schedule Maintenance/Updates notifications. The proposer should indicate whether versioning notes detailing changes made to the application are available to customers. In the event data is mirrored to an ASU data warehouse environment, Proposer will provide advance notice describing upcoming ERD (e.g. database schema) changes so that integration can be modified in advanced.

Answer:

g. If proposer’s price for services is tied to any Service Level Agreements (SLAs) outside of the referenced items above, specify those terms. SLAs shall be listed in terms of support, problem resolution and escalation procedures.

Answer:

7. Security Requirements

a. Acknowledgement of Section XIV ASU’s Security Review Process. Note: ASU’s Security Review Process of the RFP is intended for proposers to understand ASU’s security review processes for all software or software developed for the project – website or otherwise. The proposer must understand and agree to ASU security assessment requirements if awarded this contract. This section is included only as reference.

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

b. Describe in detail delivered security elements such as, but not limited to, the encryption of sensitive data in transport, data at rest, 3rd party security scanning, etc.

Answer:

c. Does the proposer meet industry standards, such as SOC2 Type II reports, compliance with FERPA and HIPAA statutes, and GDPR (General Data Protection Regulation) compliance?

____________ Yes

____________ No

Additional information (if applicable):

d. Does the proposer protect confidential data and session activity both within the application and in transit?

____________ Yes

____

No

e. Does the proposer have the ability to encrypt data and session activity?

____________ Yes

____________ No

f. Does the proposer support mass notifications for users during emergencies, including any third party product integrations?

____________ Yes

____________ No

g. The proposer must describe in detail delivered security elements such as, but not limited to, the encryption of sensitive data in transport, data at rest, 3rd party security scanning, etc.

Answer:

h. The proposer must detail their auditing capabilities to help reduce compliance risk (e.g. capture data describing administrative changes made).

Answer:

8. Transitions In/Out Plan
   a. 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. The proposer must detail below in this section a standard or typical transition plan to describe any information on their firm's transition in/out services.

Answer:

b. 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.

c. 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.

d. 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.

9. Value-Added Services

a. Please provide a 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 enhance of ASU's reputation as an innovative, foundational model for the New American University
- Commitment to provide significant financial and non-financial support for the University and its signature programs.
- Any other goods or services your company provides

b. The proposer should describe what value added benefits, services, or programs may contribute to the overall evaluation of your proposal. The proposer should provide their response to this section in the space below.

Answer:

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. The proposer may request a Word Document version of Section VII upon request to ASU Purchasing. Please reply directly underneath each item below in Section VII for ease of evaluation.

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. Provide a brief narrative describing the history of your firm. Identify the number of years in the industry, the number of employees in your firm, the Ownership and if the company has ever filed for bankruptcy, been in loan default, or if there are pending liens, claims or lawsuits against the firm. If so, please describe.

2. The proposer must provide demonstrated experience in consulting and/or implementing large, scalable technology solutions at large institutions, similar to size and scope of ASU. Higher education experience is preferred similar to the size and scope of ASU.

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, with the section that will have responsibility for performing this project clearly noted along will resumes of key team members dedicated to this project.

4. The proposer must provide their white paper that describes specifications of their system/software, security measure, and other technical information that informs concisely about the complexity of their product.

5. The proposer shall provide a Gantt chart (a preliminary project schedule) to identify the estimated timelines of the project, the roles and responsibilities between the awarded proposer and ASU, and any additional resources needed for the project. This project plan must include an installation timeline and proposed project milestones and matches as close as possible to all components outlined within Section V Specifications/Scope of Work. The Gantt chart must estimate a project kickoff from April 1, 2019 to January 13, 2020 for full implementation.

6. Submit two (2) past and three (3) present client references comparable in size to ASU and in scope of this RFP (including training plan samples). 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. Include the name, title, telephone number, and e-mail address of the individual at the client organization who is most familiar with this engagement.

7. The proposer must provide a statement of their review and acceptance of ASU's Terms and Conditions included in this RFP under Section XII. **Note: all exceptions with justification and alternative language MUST be submitted with the proposal.** In no event is a Proposer to submit its own standard contract terms and conditions or a previously negotiated ASU contract as a response to this section.

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

8. If a subcontractor is proposed, provide a history on previous work completed together by the proposer and subcontractor. Include the following for each project in which the proposer and subcontractor have worked together:

a. Agency (provide a University police department if applicable)
b. Project date
c. Applications installed
d. Responsibilities of each party.

9. The proposer must summarize all litigation (regardless of disposition/status) involving the proposer as a plaintiff or defendant within the past five years. If the proposer has been ordered by a Court not to disclose a summary of the case, list this fact.

10. The proposer must describe their company’s affiliation with APCO (Association of Public-Safety Communications Officials) and NENA (National Emergency Number Association) and how the company leverages APCO/NENA standards, guidelines, and best practices.

11. The proposer must describe their company’s affiliation with public safety organizations such as IACP (International Association of Chiefs of Police), CALEA (Commission on Accreditation for Law Enforcement Agencies), etc., and how the company leverages industry standards, guidelines, and best practices.

12. The proposer must describe their company’s affiliation with Homeland Security and how the company leverages Federal standards, guidelines, and best practices.

13. The federal government has taken the lead in developing standards for facilitating information sharing among local, state, and federal first responders and emergency operations managers. Describe the ability of the proposed system and the company’s ability to adhere to these standards.

14. The proposer must describe their company’s compliancy with the National Information Exchange Model (NIEM) standards. List all specifications, functionality, and features related to the proposed system. http://www.niem.gov

SECTION VIII – EVALUATION CRITERIA

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

1. Response Specifications/Scope of Work (45%)
2. Response Pricing Schedule (25%)
3. Response Proposer Qualifications (20%)
4. Sustainability Efforts/Sustainability Questionnaire (10%)

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 "Attachment A" Pricing sheet for software fees and costs.

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 (Exception for any Excel file types – please label appropriately).

- 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 (Maximum 20 pages not including resumes, CVs, and/or Organizational Charts).

4. Section V – Specifications/Scope of Work. Also, include Attachments 1-7 in both PDF and Excel format in soft/digital copy.

5. Section IX – Pricing Schedule. Also, include Attachment A-Pricing Schedule in both PDF and Excel format in soft/digital copy.

6. Exceptions, justification, and alternate language to 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 Lorenzo.Espinoza@asu.edu.

PROJECT NAME: Computer Aided Dispatch, Records Management System, & Mobile Data System for the ASU Police Department

PROPOSAL NUMBER: 341904

INQUIRY DEADLINE: 3:00 P.M., MST, February 7, 2019

QUESTIONS ON:______ORIGINAL PROPOSAL or______ADDENDUM NO. _______________

DATE: __________________________________

WRITER: ____

COMPANY: ____

E-MAIL ADDRESS: ____

PHONE:_________________________________ FAX: ______________________________

QUESTIONS:

____

____

____

____

____

____

____

____

____

____

SECTION XII – AGREEMENT - TERMS & CONDITIONS

Arizona State University Licensing Agreement for Computer Aided Dispatch, Records Management System, and Mobile Data System

This Agreement is made between the Arizona Board of Regents for and on behalf of Arizona State University (ASU) and ___________(Licensor), effective as of__________(the Effective Date). The Agreement will apply to the following: written offers, purchase orders, and other documents issued by ASU to Licensor for the furnishing of a non-exclusive, non-transferable license (the License) to access and use Licensor's licensed materials as and to the extent described in the Agreement.

1. **Licensed Materials and Services.** The License is described with specificity on the Order Form attached as Exhibit A (the Order Form) and the Statement of Work attached as Exhibit B. The parties may sign one or more additional Order Forms, each of which will reference this Agreement, and when signed and attached to Exhibit A, will become part of the definition of Order Form. In connection with the License, Licensor will provide the services to ASU, and will meet the service level requirements as and when set forth in the Service Level Agreement, attached as Exhibit C, and on each Order Form (the Services). The Services and the License are collectively defined as the Deliverables.

2. **Compensation.** ASU will pay Licensor for the Deliverables as and when set forth on Exhibit A. Unless described with specificity on Exhibit A, ASU must receive all Deliverables prior to payment. Licensor will be solely responsible for all expenses it incurs in connection with its obligations under this Agreement. ASU will make payments to Licensor in Licensor's legal name as set forth in the opening paragraph.

3. **Term and Termination.**

   a. The License and the obligations of the parties will commence on the Effective Date and, unless sooner terminated, expire one (1) year after the Effective Date (the Term) with the option to renew up to four (4) successive one-year terms. The total Term will not exceed five (5) years. Following the initial Term, the Agreement may be extended by mutual written agreement.

   b. ASU may terminate this Agreement or any Order Form, in whole or in part, with or without cause, upon thirty (30) days written notice to Licensor. Subject to the provision of any Transition Services (as defined below), upon termination, Licensor will refund to ASU all prepaid amounts for Deliverables not delivered or performed. If the Agreement is terminated pursuant to this section, subject to the provision of any Transition Services, ASU will pay Licensor, as full compensation under the Agreement: (1) the portion of the Deliverables delivered or performed and accepted prior to the termination based on the unit prices in the Agreement, or, if no unit prices are provided, the pro rata amount of the total order price based on the amount delivered or performed; and (2) a reasonable amount, not otherwise recoverable from other sources by Licensor, and as approved by ASU, with respect to the undelivered, unperformed, or unacceptable portion of the Deliverables. In no event will commendation paid previously under the Agreement together with compensation paid under this section exceed the total Agreement price.

   c. ASU may terminate the Agreement, in whole or in part, if Licensor defaults on any of its obligations in the Agreement and fails to cure such default within seven (7) days after receiving notice of default from ASU. In the event of such a default, ASU may procure the Deliverables from other sources and Licensor will be liable to ASU for any excess costs ASU incurs.

   d. ASU may terminate the Agreement at any time if Licensor files a petition in bankruptcy, or is adjudicated bankrupt; or if a petition in bankruptcy is filed against Licensor and not discharged within thirty (30) days; or if Licensor becomes insolvent or makes an assignment for the benefit of its creditors or an arrangement to any bankruptcy law; or if a receiver is appointed for Licensor or its business.

4. **Transition.** Upon termination of the Agreement or termination of any Order Form (regardless of the reason for termination), the parties will work in good faith to transition the termination Services to ASU or its designees, with minimum interruption to ASU's business. At ASU's option, Licensor will continue to provide Services and will provide transition support at rates consistent with the terms of the Agreement for a period no longer than 180 days following the termination date (the Transition Period). Licensor will provide the post-termination Services (the Transition Services) at least at the same levels of quality and timeliness of performance as Services were provided prior to termination, in a professional manner, with high quality, and in accordance with industry standards. The parties may, by written agreement, modify the Transition Services to be provided and the length of the Transition Period.

5. **Independent Contractor.** Licensor is an independent contractor. Neither Licensor not any of Licensor's owners, officers, directors, managers, members, employees, agents, contractors, or subcontractors (collectively, with Licensor, the Licensor Parties) will be employees, agents, partners, or joint venturers of ASU. None of the Licensor Parties will be eligible for any benefits from ASU, including worker's compensation coverage, nor will ASU make deductions from any amounts payable to Licensor for taxes. Taxes for any amounts paid to Licensor will be Licensor's sole responsibility. Licensor is responsible to ASU for the compliance with this Agreement by the Licensor Parties.

6. **Data Use, Ownership, and Privacy.** As between the parties, ASU will own, or retain all of its rights in, all data and information that ASU provides to Licensor, as well as all data and information managed by Licensor on behalf of ASU, including all output, reports, analyses, and other materials relating to, derived from, or generated pursuant to the Agreement, even if generated by Licensor, as well as all data obtained or extracted through ASU's or Licensor's use of such data and information (collectively, ASU Data). ASU Data also includes all data and information provided directly to Licensor by ASU students and employees, and includes personal data, metadata, and user content.

   ASU Data will be ASU's Intellectual Property (as defined below) and Licensor will treat it as ASU Confidential Information. Licensor will not use, access, disclose, license, or provide to third parties, any ASU Data, except: (i) to fulfill Licensor's obligations to ASU hereunder; or (ii) as authorized in writing by ASU. Without limitation, Licensor will not use any ASU Data, whether or not aggregated or de-identified, for product development, marketing, profiling, benchmarking, or product demonstrations, without, in each case, ASU's prior written consent. Licensor will not, directly or indirectly: (x) attempt to re-identify or de-aggregate de-identified or aggregated information; or (y) transfer de-identified or aggregated information to any third party unless that third party agrees not to attempt re-identification or de-aggregation. For ASU Data to be considered de-identified, all direct and indirect personal identifiers must be removed, including names, ID numbers, dates of birth, demographic information, location information, and school information. Upon request by ASU, Licensor will deliver, destroy, and/or make available to ASU, any or all ASU Data.

   Notwithstanding the foregoing, if the Agreement allows Licensor to provide aggregated and de-identified data to third parties, then Licensor may provide such data solely to the extent allowed in the Agreement, and, unless otherwise stated herein, only if such data is aggregated with similar data of others (i.e., is not identified as ASU, ABOR, or Arizona-specific).

7. **Intellectual Property Ownership.** All Intellectual Property that Licensor or any of the Licensor Parties make, conceive, discover, develop or create, either solely or jointly with any other person or persons including ASU, specifically for or at the request of ASU in connection with the Agreement (Contract IP), will be owned by ASU. To the extent any Contract IP is not considered work made for hire for ASU (or if ownership of all rights therein does not otherwise vest exclusively in ASU), Licensor hereby irrevocably assigns, and will cause the Licensor Parties to so assign, without further consideration, to ASU all right, title and interest in and to all Contract IP, including all copyright rights of ownership. Intellectual Property means all ASU Data, any and all inventions, designs, original works of authorship, formulas, processes, compositions, programs, databases, data, technologies, discoveries, ideas, writings, improvements, procedures, techniques, know-how, and all patent, trademark, service mark, trade secret, copyright and other intellectual property rights (and goodwill) relating to the foregoing. Licensor will make full and prompt disclosure of

the Contract IP to ASU. Licensor will, and will cause the Licensor Parties, as and when requested by ASU, do such acts, and sign such instruments to vest in ASU the entire right, title and interest to the Contract IP, and to enable ASU to prepare, file, and prosecute applications for, and to obtain patents and/or copyrights on, the Contract IP, and, at ASU's expense, to cooperate with ASU in the protection and/or defense of the Contract IP.

8. **Licensor's Intellectual Property.** Licensor will retain ownership of its pre-existing Intellectual Property, including any that may be incorporated into the Contract IP, provided that Licensor informs ASU in writing before incorporating any pre-existing Intellectual Property into any Contract IP. Licensor hereby grants to ASU a perpetual, irrevocable, royalty-free, worldwide right and license (with the right to sublicense), to freely use, make, have made, reproduce, disseminate, display, perform, and create derivative works based on such pre-existing Intellectual Property as may be incorporated into the Contract IP or otherwise provided to ASU in the course of performing under the Agreement.

9. **Warranties of Licensor.** In addition to any implied warranties, Licensor warrants to ASU that: (1) the Deliverables will be free from any defects in design, workmanship, materials, or labor; (2) all of the Services will be performed in a professional and workmanlike manner and in conformity with highest and best industry standards by persons reasonably suited by skill, training and experience for the type of services they are assigned to perform; (3) Licensor will comply, and will be responsible for ensuring Licensor Parties comply with all applicable laws, rules, and regulations in the performance of the Agreement; (4) Licensor owns or has sufficient rights in the Deliverables that they do not infringe upon or violate any Intellectual Property of any third parties, and are free and clear of any liens and encumbrances; (5) any data, code, or software developed or delivered by Licensor to ASU will not contain any viruses, worms, Trojan Horses, or other disabling devices or code; (6) all sensitive data, personal data, and personally identifiable data, as those terms may be defined in applicable laws, rules and regulations (PII) provided by Licensor to ASU was obtained legally and Licensor has obtained all requisite permissions from the individuals whose PII is being provided for (a) Licensor to provide the PII to ASU, and (b) ASU to use the PII for the purposes and in the jurisdictions set forth in the Agreement; (7) the prices of Deliverables in the Agreement are the lowest prices at which these or similar goods or services are sold by the Licensor to similar customers. In the event of any price reduction between execution of the Agreement and delivery of the Deliverables, ASU shall be entitled to such reduction; and (8) all Deliverables delivered by Suppler will conform to the specifications, drawings, and descriptions set forth in the Agreement, and to the samples furnished by the Licensor, if any. In the event of a conflict among the specifications, drawings and description, the specifications will govern.

10. **Debarment and Suspension.** Licensor represents and warrants that neither it nor any of its subcontractors supplying the Deliverables have either directly or indirectly or through subcontractors, been suspended, debarred, or otherwise excluded from participation in or penalized by any federal or state procurement, non-procurement, or reimbursement program. Licensor affirms that it has confirmed the above statement by checking The System for Award Management (SAM) within 180 days prior to commencing work under the Agreement. Licensor will provide immediate written notice to ASU upon learning that it or any of its subcontractors are under any investigation or proposed action that could result in such exclusion, suspension, or debarment.

11. **Notices.** All notices and communications required or permitted under this Agreement will be in writing and will be given by personal delivery against receipt (including private courier such as FedEx), or certified U.S. Mail, return receipt requested. All notices and communications will be sent to the addresses below or such other addresses as the parties may specify in the same manner.

To ASU:
Manager, Police Communications
ASU Police Department
Arizona State University
Mailing Address:
a. PO Box 871812
b. Tempe, AZ 85287-1812

With a copy to:
Chief Procurement Officer
Purchasing and Business Services
Arizona State University
Mailing Address:
PO Box 875212
Tempe, AZ 85287-5212

Delivery Address:
c. 325 E. Apache Blvd.
d. Tempe, AZ 85287-1812

Delivery Address:
1551 S. Rural Rd.
Tempe, AZ 85287

To Licensor:
____
____
____
____

With a copy to:
____
____
____
____

Notices, if delivered, and if provided in the manner set forth above, will be deemed to have been given and received on the date of actual receipt or on the date receipt was refused. Any notice to be given by any party may be given by legal counsel for such party.

12. **Nondiscrimination.** The parties will comply with all applicable laws, rules, regulations, and executive orders governing equal employment opportunity, immigration, and nondiscrimination, including the Americans with Disabilities Act. **If applicable, the parties will abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, national origin, protected veteran status or disability.**

13. **Conflict of Interest.** If within three (3) years after the execution of the Agreement, Licensor hires as an employee or agent any ASU representative who was significantly involved in negotiating, securing, drafting, or creating the Agreement, then ASU may cancel the Agreement as provided in Arizona Revised Statutes (ARS) § 38-511.

14. **Arbitration.** The parties agree to arbitrate disputes filed in Arizona Superior Court that are subject to mandatory arbitration pursuant to ARS § 12-133.

15. **Dispute Resolution.** If a dispute arises under the Agreement, the parties will exhaust all applicable administrative remedies provided for under Arizona Board of Regents Policy 3-809.

16. **Records.** To the extent required by ARS § 35-214, Licensor will retain all records relating to the Agreement. Licensor will make those records available at all reasonable times for inspection and audit by ASU or the Auditor General of the State of Arizona during the term of the Agreement and for five (5) years after the completion of the Agreement. The records will be provided at Arizona State University in Tempe, Arizona, or another location designated by ASU on reasonable notice to Licensor.

17. **Failure of Legislature to Appropriate.** In accordance with ARS § 154, if ASU's performance under the Agreement depends on the appropriation of funds by the Arizona Legislature (Legislature), and if the Legislature fails to appropriate the funds necessary for performance, then ASU may provide written notice of this to Licensor and cancel the Agreement without further obligation of ASU. Appropriation is a legislative act and is beyond the control of ASU.

18. **Weapons, Explosive Devices, and Fireworks.** ASU's Weapons, Explosives, and Fireworks Policy prohibits the use, possession, display or storage of any weapon, explosive device or fireworks on all land and buildings owned, leased, or under the control of ASU or its affiliated entities, in all ASU residential facilities (whether managed by ASU or another entity), in all ASU vehicles, and at all ASU or ASU affiliate sponsored events and activities, except as provided in ARS § 12-781, or unless written permission is given by ASU's Police Chief or a designated representative. Licensor will notify all persons or entities who are employees, officers, subcontractors, consultants, agents, guests, invitees or licensees of Licensor of this policy and Licensor will enforce this policy against all such persons and entities.

19. **Advertising, Publicity, Names and Marks.** Licensor will not do any of the following, without, in each case, ASU's prior written consent: (i) use any names, service marks, trademarks, trade names, logos, or other identifying names, domain names, or identifying marks of ASU (ASU Marks), including online, advertising, or promotional purposes; (ii) issue a press release or public statement regarding the Agreement; or (iii) represent or imply any ASU endorsement or support of any product or service in any public or private communication. Any use of ASU Marks must comply with ASU's requirements, including using the ® indication of a registered mark.

20. **Information Security.** All systems containing ASU Data must be designed, managed, and operated in accordance with information security best practices and in compliance with all applicable laws, rules, and regulations. To diminish information security threats, Licensor will (either directly or through its third party service providers) meet the following requirements:

    a. Access Control. Control access to ASU's resources, including sensitive ASU Data, limiting access to legitimate business needs based on an individual's job-related assignment. Licensor will, or will cause the system administrator to, approve and track access to ensure proper usage and accountability, and Licensor will make such information available to ASU for review, upon ASU's request.

    b. Incident Reporting. Report information security incidents immediately to ASU (including those that involve information disclosure incidents, unauthorized disclosure of ASU Data, network intrusions, successful virus attacks, unauthorized access or modifications, and threats and vulnerabilities).

    c. Off Shore. Direct Services that may involve access to secure or sensitive ASU Data or personal client data or development or modification of software for ASU, will be performed within the border of the United States. Unless stated otherwise in the Agreement, this requirement does not apply to indirect or "overhead" services, redundant back-up services or services that are incidental to the performance of the Agreement. This provision applies to work performed by subcontractors at all tiers and to all ASU Data.

    d. Patch Management. Carry out updates and patch management for all systems and devices in a timely manner and to the satisfaction of ASU. Updates and patch management must be deployed using an auditable process that can be reviewed by ASU upon ASU's request.

    e. Encryption. All systems and devices that store, process or transmit sensitive ASU Data must use an industry standard encryption protocol for data in transit and at rest.

    f. Notifications. Notify ASU immediately if Licensor receives any kind of subpoena for or involving ASU Data, if any third party requests ASU Data, or if Licensor has a change in the location or transmission of ASU Data. All notifications to ASU required in this Information Security paragraph will be sent to ASU Information Security at infosec@asu.edu, in addition to any other notice addresses in the Agreement.

    g. Security Reviews. Complete SOC2 Type II or substantially equivalent reviews in accordance with industry standards, which reviews are subject to review by ASU upon ASU's request. Currently, no more than two (2) reviews per year are required.

    h. Scanning and Penetration Tests. Perform periodic scans, including penetration test, for unauthorized applications, services, code and system vulnerabilities on the networks and systems included in the Agreement in accordance with industry standards and ASU standards (as documented in NIST 800-115 or equivalent). All web-based applications (e.g., HTTP/HTTPS accessible URLs, APIs, and web services) are required to have their own web application security scan and remediation plan. Licensor must correct weaknesses within a reasonable period of time, and Licensor must provide proof of testing to ASU upon ASU's request.

i. ASU Rights. ASU reserves the right (either directly or through third party service providers) to scan and/or penetration test any purchased and/or leased software regardless of where it resides.

j. Secure Development. Use secure development and coding standards including secure change management procedures in accordance with industry standards. Perform penetration testing and/or scanning prior to releasing new software versions. Licensor will provide internal standards and procedures to ASU for review upon ASU request.

21. End User Licenses. The terms of this section apply if the License include software or other computer programs or applications that require acceptance of a clickwrap, click-through, end user license, or other similar agreement (End User Agreement) prior to the use of the software. If Licensor requires ASU's individual users to accept an End User Agreement, the terms of the End User Agreement that conflict or are inconsistent, with the terms of the Agreement or ASU's Privacy Policy will be null and void.

22. Background Checks. Licensor will exclude from any direct participation in Licensor's performance under the Agreement, any unqualified persons. In addition, at the request of ASU, Licensor will, at Licensor's expense, conduct reference checks and employment, education, SSN trace, National Sex Offender Registry, and criminal history record checks (collectively, Screenings) on requested persons employed or contracted by Licensor to perform work under the Agreement. Licensor will maintain as part of the records Licensor is required to maintain hereunder, all Screening information and all documentation relating to work performance for each employee or contractor who performs work hereunder. Licensor will abide by all applicable laws, rules and regulations including the Fair Credit Reporting Actand any equal opportunity laws, rules, and regulations.

23. Insurance Requirements. Without limiting any liability of or any other obligation of Licensor, Licensor 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 Licensor, its agents, representatives, employees or subcontractors, as described in Exhibit D.

24. Gratuities. Licensor will not give or offer any gratuities, in the form of entertainment, gifts or otherwise, or use an agent or representative of Licensor to give or offer a gratuity, to any officer or employee of the State of Arizona with a view towards securing an agreement or securing favorable treatment with respect to the awarding or amending, or the making of any determinations with respect to the performing of such Agreement. If ASU determines that Licensor has violated this section, ASU may, by written notice to Licensor, cancel the Agreement. If the Agreement is cancelled by ASU pursuant to this section, ASU will be entitled, in addition to any other rights and remedies, to recover or withhold the amount of the costs incurred by Licensor in providing gratuities.

25. Privacy; Educational Records. Student educational records are protected by the U.S. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) and its implementing regulations (FERPA). Licensor will not require any ASU students or employees to waive any privacy rights (including FERPA or the European Union's General Data Protection Regulation [GDPR]) as a condition for receipt of any educational services, and any attempt to do so will be void. Licensor will comply with FERPA and will not access or make any disclosures of student educational records to third parties without prior notice to and consent from ASU or as otherwise provided by law. If the Agreement requires or permits Licensor to access or release any student records, then, for purposes of the Agreement only, ASU designates Licensor as a "school official" for ASU under FERPA, as that term is used in FERPA. In addition, any access or disclosures of student educational records made by Licensor or any Licensor Parties must comply with ASU's definition of legitimate educational purpose in SSM 107-01. If Licensor violates the terms of this section, Licensor will immediately provide notice of the violation to ASU.

26. **Data Protection.** Licensor will ensure that all services undertaken pursuant to the Agreement are performed in compliance with applicable privacy and data protection laws, rules, and regulations. If Licensor will serve as a Processor of ASU Data that includes Personal Data of Data Subjects in the European Union, Licensor will cooperate with ASU to comply with the GDPR with respect to such Personal Data and Data Subjects. This includes ensuring that all Data Subjects have signed appropriate Consents, and signing and complying with all documents and agreements reasonably requested by ASU, including any data processing agreements. All capitalized terms in this section not otherwise defined in the Agreement are defined in the GDPR.

27. **Academic Freedom and Accreditation.** ASU will maintain ultimate authority over all curriculum. Nothing in the Agreement will limit ASU's academic freedom or require ASU to violate any of the policies, standards, and requirements of the Arizona Board of Regents or any accrediting entities.

28. **Price Adjustment.** ASU normally considers price changes at the end of one contract period and the beginning of another. Price change requests will be supported by evidence of increased costs to Licensor. ASU will not approve price increases that will merely increase gross profitability of Licensor at the expense of ASU. Price change requests will be a factor in the contract extension review process. ASU will determine whether any requested price increase or an alternate option is in the best interest of ASU.

29. **Authorized Presence Requirements.** As required by ARS § 41-4401, ASU is prohibited from awarding a contract to any contractor or subcontractor that fails to comply with ARS § 23-214(A) (verification of employee eligibility through the e-verify program). Licensor warrants that it and its subcontractors comply fully with all applicable immigration laws, rules, and regulations that relate to their employees and their compliance with ARS § 23-214(A). A breach of this warranty will be a material breach of the Agreement that is subject to penalties up to and including termination of the Agreement. ASU retains the legal right to inspect the papers of any contractor or subcontractor employee who works hereunder to ensure that the contractor or subcontractor is complying with the above warranty.

30. **Nondisclosure and Trade Secrets.** Licensor may receive (or has received) from ASU and otherwise be exposed to confidential and proprietary information relating to ASU's business practices, strategies, and technologies, ASU Data, as well as confidential information of ASU necessary to perform and/or provide the License (collectively, ASU Confidential Information). ASU Confidential Information may include, but is not limited to, confidential and proprietary information supplied to Licensor with the legend "ASU Confidential and Proprietary," or other designations of confidentiality. As between Licensor and ASU, the ASU Confidential Information is the sole, exclusive, and valuable property of ASU. Accordingly, Licensor will not reproduce or otherwise use any of the ASU Confidential Information except in the performance or provision of the License, and will not disclose any of the ASU Confidential Information in any form to any third party, either during or after the Term, except with ASU's prior written consent. Upon termination of the Agreement, Licensor will cease using, and will return to ASU, all originals and all copies of the ASU Confidential Information, in all forms and media, in Licensor's possession or under Licensor's control. In addition, Licensor will not disclose or otherwise make available to ASU any confidential information of Licensor or received by Licensor from any third party.

    Licensor will have no obligation to maintain as confidential ASU Confidential Information (other than ASU Data) that Licensor can show: (i) was already lawfully in the possession of or known by Licensor before receipt from ASU; (ii) is or becomes generally known in the industry through no violation of the Agreement or any other agreement between the parties; (iii) is lawfully received by Licensor from a third party without restriction on disclosure or use; (iv) is required to be disclosed by court order following notice to ASU sufficient to allow ASU to contest such order; or (v) is approved in writing by ASU for release or other use by Licensor.

31. **Confidentiality.** ASU, as a public institution, is subject to ARS §§ 39-121 to 39-127 regarding public records. Any provision regarding confidentiality is limited to the extent necessary to comply with Arizona law.

32. **Indemnification and Liability Limitations.** Because ASU is a public institution, any indemnification, liability limitation, releases, or hold harmless provisions are limited as required by Arizona law, including Article 9, Sections 5 and 7 of the Arizona Constitution and ARS §§ 35-154 and 41-621. ASU's liability under any claim for indemnification is limited to claims for property damage, personal injury, or death to the extent caused by acts or omissions of ASU.

33. **Indemnification by Licensor.** Licensor will indemnify, defend, save and hold harmless the State of Arizona, its departments, agencies, boards, commissions, universities, and its and their officials, agents and employees (collectively, Indemnitee) for, from, and against any and all claims, actions, liabilities, damages, losses or expenses (including court costs, attorneys' fees, and costs of claim processing, investigation, and litigation) for bodily injury or personal injury (including death), or loss or damage to tangible or intangible property to the extent caused, or alleged to be caused, by (i) the negligent or willful acts or omissions of Licensor, or any of its Licensor Parties; (ii) a breach of the Agreement; or (iii) failure to comply with any applicable law, rule, or regulation. Licensor will be responsible for primary loss investigation, defense and judgment costs where this indemnification is applicable.

34. **Responsibility.** Each party is responsible for the negligent or willful acts or omissions of its employees and contractors when acting under such party's direction and supervision. ASU recognizes an obligation to pay attorneys' fees or costs only when assessed by a court of competent jurisdiction. Notwithstanding the terms of the Agreement or any other document: (i) other than for employees and contractors acting under ASU's direction and supervision, ASU is not responsible for any actions of any third parties, including its students; and (ii) no person may bind ASU unless they are an authorized signatory in PUR-202.

35. **Americans with Disabilities Act and Rehabilitation Act.** To the extent applicable, Licensor will comply with all applicable provisions of the Americans with Disabilities Act, the Rehabilitation Act of 1973, and all applicable federal regulations, as amended from time to time (ADA Laws). All electronic and information technology and products and services to be used by ASU faculty, staff, students, program participants, or other ASU constituencies must be compliant with ADA Laws. Compliance means that a disabled person can acquire the same information, engage in the same interactions, and enjoy the same services as a nondisabled person, in an equally effective and integrated manner, with substantially equivalent ease of use.

36. **Assignment.** Licensor may not transfer or assign the Agreement or any of Licensor's rights or obligations thereunder, either directly or indirectly, or by operation of law, without ASU's prior written consent, and any attempt to the contrary will be void.

37. **Affirmation of Rights.** All rights and licenses granted to this Agreement are, and will be, for purposes of Section 365(n) of the United States Bankruptcy Code and/or similar or comparable section of the United States Bankruptcy Code (as modified, amended, replaced or renumbered from time to time) (the Code), executory licenses of rights to "intellectual property", as defined under Section 101 (35A) of the Code. The parties will retain and may fully exercise all of their respective rights and elections under the Code. Accordingly, ASU will retain and may fully exercise all of its rights and elections under the Code. Upon the commencement of bankruptcy proceedings by or against either party under the Code, the other party will be entitled to retain all of its license rights and use rights granted under this Agreement.

38. **Availability.** If during the Term, for any reason, Licensor no longer supports or provides any or all of the License, Licensor will continue to allow ASU to (i) use the License at no additional charge, and (ii) receive necessary documentation and code to support the License. This includes providing a current copy of (or access to) the source code for such License. Notwithstanding the foregoing, if Licensor is legally precluded from supporting or providing the License due to third party claims of infringement, Licensor may either procure for ASU the right to continue using the

License, or replace or modify the License or infringing portion thereof so that they are no longer infringing, provided however, the replacements or modifications must provide the essential functions and functionality of the License.

39. **Business Continuity Plan.** If requested by ASU, Licensor will provide to ASU, within 30 days after such request, a comprehensive plan for continuing the performance of its obligations during a Public or Institutional Emergency (the Business Continuity Plan). The Business Continuity Plan, at a minimum, will address the following: 1) identification of response personnel by name; 2) key succession and performance responses in the event of sudden and significant decrease in workforce; and 3) contingency plans for the Licensor to continue the performance of its obligations under the Agreement, despite the emergency. In the event of a Public or Institutional Emergency, Licensor will implement the applicable actions set forth in the Business Continuity Plan and will make other commercially practicable efforts to mitigate the impact of the event. For clarification of intent, being obliged to implement the plan is not of itself an occurrence of force majeure, and Licensor will not be entitled to any additional compensation or extension of time by virtue of having to implement it, unless otherwise agreed to by ASU in writing. A Public or Institutional Emergency will mean a natural or manmade event that creates a substantial risk to the public, that causes or threatens death or injury to the general public, or that causes a significant disruption to the day-to-day business operations of ASU.

40. **Rights to Inventions Made Under an Agreement.** If this Agreement is a “funding agreement” under 37 CFR 401.3, the parties agree to incorporate by this reference the standard patent rights clause found in 37 CFR 401.14 and any implementing regulations issued by the awarding agency.

41. **No Boycott of Israel.** To the extent required by ARS § 35-393.01, Licensor certifies it is not currently engaged in a boycott of Israel and will not engage in a boycott of Israel during the Term.

42. **Title IX Obligation.** Title IX protects individuals from discrimination based on sex, including sexual harassment. ASU fosters a learning and working environment built on respect and free of sexual harassment. ASU’s Title IX Guidance is available online. Licensor will: (i) comply with ASU’s Title IX Guidance; (ii) provide ASU’s Title IX Guidance to any Licensor Parties reasonably expected to interact with ASU students or employees, in person or online; and (iii) ensure that all Licensor Parties comply with ASU’s Title IX Guidance.

43. **Foreign Corrupt Practices Act/ UK Bribery Act/Local Anti-Corruption Law Compliance.** Licensor warrants that it is familiar with the U.S. laws prohibiting corruption and bribery under the U.S. Foreign Corrupt Practices Act and the United Kingdom laws prohibiting corruption and bribery under the UK Bribery Act. In connection with Licensor’s work under the Agreement, Licensor will not offer or provide money or anything of value to any governmental official or employee or any candidate for political office in order to influence their actions or decisions, to obtain or retain business arrangements, or to secure favorable treatment in violation of the Foreign Corrupt Practices Act, the UK Bribery Act, or any other local anti-corruption law, either directly or indirectly. Any breach of the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, or other local anti-corruption law, will be a material breach of the Agreement.

44. **Export Controls.** If any of the Deliverables are export-controlled under the U.S. Export Administration Regulations, U.S. International Traffic in Arms Regulations, or through the sanctions and embargoes established through the Office of Foreign Assets Control (collectively, the Export Control Laws), Licensor will provide ASU with written notification that identifies the export-controlled Deliverables and such Deliverables export classification. None of the work undertaken pursuant to the Agreement will require either party to take or fail to take any action that would cause a violation of any of the Export Control Laws. The parties will cooperate to facilitate compliance with applicable requirements of the Export Control Laws.

45. **Payment Card Industry Data Security Standard.** For e-commerce business and/or payment card transactions, Licensor will comply with the requirements and terms of the rules of all applicable payment card industry associations or organizations, as amended from time to time (PCI Security Standards), and be solely responsible for security and

maintaining confidentiality of payment card transactions processed by means of electronic commerce up to the point of receipt of such transactions by a qualified financial institution.

Licensor will, at all times during the Term, be in compliance with the then current standard for Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS) for software, and PIN Transaction Security (PCI PTS) for hardware. Licensor will provide attestation of compliance to ASU annually by delivering to ASU current copies of the following: (i) Licensor's "Attestation of Compliance for Onsite Assessments - Service Providers;" (ii) an attestation that all ASU locations are being processed and secured in the same manner as those in Licensor's "PCI Report on Compliance;" and (iii) a copy of Licensor's PCI Report on Compliance cover letter. Licensor will notify ASU immediately if Licensor becomes non-compliant, and of the occurrence of any security incidents (including information disclosure incidents, network intrusions, successful virus attacks, unauthorized access or modifications, and threats and vulnerabilities).

Licensor's services must include the following:

a. Licensor maintains its own network operating on its own dedicated infrastructure. Licensor's network includes a firewall that (i) includes access control rules that separate Licensor's PCI network from ASU, and (ii) restricts any communication between Licensor's network devices and ASU systems.
b. Licensor treats the ASU network as an untrusted network and no unencrypted cardholder data traverses or otherwise is stored on ASU's network, and ASU has no ability to decrypt cardholder data.
c. All devices must be SRED (secure reading and exchange of data), EMV (Europay, MasterCard and VISA) and PTS POI compliant.

46. **Assignment of Anti-Trust Overcharge Claims.** In actual economic practice, overcharges resulting from anti-trust violations are borne by the ultimate purchaser. Therefore, Licensor hereby assigns to ASU any and all claims for such overcharges.

47. **Parking.** Licensor will obtain all parking permits and/or decals required while performing any work on ASU premises. If needed, Licensor should contact ASU Parking and Transit, http://cfo.asu.edu/pts.

48. **Campus Deliveries and Mall Access.** Licensor will familiarize itself with ASU parking, campus delivery options, and loading zones. Not all campus buildings are directly accessible and some require Licensor to unload at lots or loading areas that may not be adjacent to the delivery or work location. As a result, Licensor must then transport Deliverables by using electric style golf carts, dolly, or other manual device across pedestrian malls. Many campuses include features and pedestrian malls that may have limited access for Licensor vehicle and carts. Walk-Only Zones prohibit access to all wheeled traffic during enforcement times, and deliveries or work requiring vehicular or cart access may need to be arranged outside of enforcement times. For details about parking permits, supplier permits, loading zones, mall access, and pedestrian mall restrictions, go to http://cfo.asu.edu/pts. For additional information, go to http://walk.asu.edu.

49. **Health Insurance Portability and Accountability Act.** To the extent applicable, Licensor will abide by all laws and regulations that protect the privacy of healthcare information to which Licensor obtains access under the Agreement. Certain portions of the Administrative Simplification section of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as codified at 42 U.S.C. § 1320d through d-8, and the federal privacy regulations as contained in 45 CFR Part 164 may apply to Licensor and ASU, and their relationships and operation under the Agreement. If necessary, Licensor and ASU will enter into a standard Business Associate Agreement, and any other required HIPAA agreements. To the extent the terms thereof relate to Licensor's performance under the Agreement, the provisions of the Business Associate Agreement will control.

50. **Governing Law and Venue.** The Agreement will be governed by the laws of the State of Arizona without regard to any conflicts of laws principles. ASU's obligations hereunder are subject to the regulations/policies of the Arizona Board

of Regents. Any proceeding arising out of or relating to the Agreement will be conducted in Maricopa County, Arizona. Each party consents to such jurisdiction, and waives any objection it may now or hereafter have to venue or to convenience of forum.

51. **Survival.** All provisions of the Agreement that anticipate performance after the termination of the Agreement, and all provisions necessary or appropriate to interpret and enforce such provisions, will survive termination of the Agreement.

52. **Modifications.** The Agreement may be modified or rescinded only by a writing signed by both parties or their duly authorized agents.

53. **Interpretation-Parol Evidence.** This Agreement is intended by the parties as a final expression of their agreement and is intended to be a complete and exclusive statement of the terms of their agreement. No course of prior dealings between the parties and no usage of the trade will be relevant to supplement or explain any term used in the Agreement. Acceptance or acquiescence in a course of performance rendered under the Agreement will not be relevant to determine the meaning of the Agreement even though the accepting or acquiescing party has knowledge of the nature of the performance and opportunity for objection.

54. **Essence of Time.** Time will be of the essence as to matters contemplated by the Agreement.

55. **Small Business.** If subcontracting (Tier 2 and higher) is necessary, Licensor will make commercially reasonable efforts to use Small Business (SB) and Small Diverse Business (SDB) in the performance of the Services. ASU may request a report at each annual anniversary date and at the completion of the Agreement indicating the extent of SB and SDB participation.

56. **Third Party Arrangements.** From time to time, ASU may enter into arrangements with third parties that may require Licensor to work cooperatively with and/or connect and use infrastructure with third parties. On a case-by-case basis, ASU and Licensor will work cooperatively, timely, and in good faith to take such actions as may be necessary or appropriate to give effect to ASU's third party agreements. Licensor will not be bound to terms and conditions of a third party that are different from this Agreement unless expressly agreed in writing. If the third party terms and conditions conflict with this Agreement's terms, impact Licensor's ability to meet service level agreements of this Agreement, or may cause Licensor to incur additional costs, then the parties will enter into good faith negotiations for an amendment to this Agreement prior to Licensor agreeing to compliance with the third party terms and conditions.

57. **Provision of Deliverables to ASU Related Entities.** ASU has, and expects to enter into additional, service and management contracts with a number of third parties (Related Entities) to deliver some or all of the Deliverables to ASU students. These Related Entities include, for example, third party managers or owners of ASU student residence halls. At ASU's option, Licensor will provide the Deliverables to ASU's current and future Related Entities consistent with the terms of the Agreement.

58. **Administrative Fee.** Licensor will pay ASU an Administrative Fee in the amount of 1% of the gross funds received by Licensor from 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 Agreement. The Administrative Fee will apply to any and all Deliverables provided by Licensor that reference the Agreement or the RFP as the supporting documentation to meet competitive bidding requirements. The Administrative Fee will be calculated based on all sales transacted, minus all taxes and any returns or credits. Licensor will submit the Administrative Fee, along with a quarterly usage report documenting all contract sales, to the ASU Chief Procurement Office within 30 days following the end of each calendar quarter. Each quarterly report at a minimum, will disclose all purchased Deliverables, prices paid, and quantity, by individual purchasing agency, for all sales within the calendar quarter just ended. The Administrative Fee is payable by Licensor, from Licensor's funds, to ASU.

59. **Federal Funding Provisions.** If the Agreement involves the use of United States federal funds, including from a government grant or funds from a subcontract at any tier relating to a federal government grant, the following terms apply to the Agreement:

60. **Government Subcontract Provisions.** If this order is a subcontract under a U.S. government prime contract, the clauses referenced below of the Federal Acquisition Regulations (FAR) and the Defense Federal Acquisition Regulations (DFAR), or the Armed Services Procurement Regulations (ASPR) are incorporated into the Agreement by this reference. Each regulation contains criteria for determining applicability of the regulation to a particular contract.

Federal Acquisition Regulations (FAR) **

52.202-1 Definitions
52.203-3 Gratuities
52.203-5 Covenant Against Contingent Fees
52.203-6 Restrictions on Subcontractor Sales to the Government
52.203-7 Anti-Kickback Procedures
52.203-12 Limitation on Payments to Influence Certain Federal Transactions
52.204-2 Security Requirements
52.209-6 Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended or Proposed for Debarment
52.211-15 Defense Priority and Allocation Requirements
52.214-27 Price Reduction For Defective Cost or Pricing Data
52.215-1 Instructions to Offerors—Competitive Acquisition.
52.215-2 Audit and Records - Negotiation
52.215-12 Subcontractor Cost or Pricing Data
52.215-13 Subcontractor Cost or Pricing Data – Modifications
52-215-14 Integrity of Unit Prices
52-219-8 Utilization of Small Business Concerns
52-219-9 Small Business Subcontracting Plan
52.222-1 Notice to the Government of Labor Disputes
52.222-4 Contract Work Hours and Safety Standards Act Overtime Compensation
52.222-6 Davis-Bacon Act [Construction Wage Rate Requirements]
52.222-20 Walsh Healey Public Contracts Act [Contracts for Materials, Supplies, Articles, and Equipment Exceeding $15,000.]
52.222-21 Prohibition of Segregated Facilities
52.222-26 Equal Opportunity
52.222-35 Equal Opportunity for Veterans
52.222-36 Equal Opportunity for Workers with Disabilities
52.222-37 Employment Reports on Veterans
52.222-40 Notification of Employee Rights Concerning Payment of Union Dues or Fees
52.222-41 Service Contract Act of 1965, as Amended
52.222-50 Combating Trafficking in Persons
52.223-3 Hazardous Material Identification and Material Safety Data
52.223-6 Drug-Free Workplace
52.225-1 Buy American Act – Supplies
52.225-13 Restrictions on Certain Foreign Purchases
52.227-1 Authorization and Consent (Alt I in all R&D)
52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement
52.227-3 Patent Indemnity
52.227-10 Filing of Patent Applications--Classified Subject Matter
52.227-11 Patent Rights – Ownership by the Contractor (Alt I-V)

52.227-13 Patent Rights - Ownership by the Government
52.227-14 Rights in Data – General
52.233-1 Disputes
52.242-1 Notice of Intent to Disallow Costs
52.242-15 Stop-work order
52.243-1 Changes - Fixed Price (43.205 (a) (1) Alts may apply)
52.243-2 Changes - Cost Reimbursement (43.205 (b) (1) Alts may apply)
52.244-2 Subcontracts
52.244-5 Competition in Subcontracting
52.244-6 Subcontracts for Commercial Items
52.245-2 Government Property – Installation Operation Services
52.246-15 Certificate of Conformance
52.247-63 Preference for U.S. Flag Air Carriers
52.247-64 Preference for U.S. Flag Commercial Vessels
52.249.1 Termination for Convenience of the Government (Fixed Price) less than simplified acquisition threshold
52.249-2 Termination for Convenience of the Government (Fixed Price) more than simplified acquisition threshold
52.249.4 Termination for Convenience of the Government (Services)
52.249-5 Termination for the Convenience of the Government (Educational and Other Nonprofit Institutions)
52.249-14 Excusable Delays

Defense Federal Acquisition Regulation Supplement (DFARS) **
DFAR CIT. TITLE
252.203-7001 Prohibition on Persons convicted of Fraud or Other Defense-Contract-Related Felonies
252.222-7000 Restrictions on Employment of Personnel
252.225-7000 Buy American Act and Balance of Payments program
252.227-7013 Rights in Technical Data and Computer Software
252.227-7016 Rights in Bid or Proposal Information
252.227-7018 Rights in Noncommercial Technical Data and Computer Software
252.227-7019 Validation of Asserted Restrictions – Computer Software
252.227-7037 Validation Technical Data
252.243-7001 Pricing of Agreement Modifications
252.244-7000 Subcontracts for Commercial Items and Commercial Components

**Full text of the FAR clauses can be found at https://www.acquisition.gov/browsefar
**Full text of the DFAR clauses can be found at http://www.farsite.hill.af.mil/vmdfara.htm

IN WITNESS THEREOF, the parties have signed this Agreement as of the Effective Date.

Arizona Board of Regents for and on behalf of Arizona State University	**Licensor**
By:________________________________	**By**:________________________________
Name:______________________________	**Name**:______________________________
Title:______________________________	**Title**:______________________________
Date Signed:_________________________	**Date Signed**:_________________________

Exhibit A – Order Form
Exhibit B – Statement of Work
Exhibit C – Service Level Agreement
Exhibit D – Insurance Requirements

EXHIBIT A – ORDER FORM No. 1

This Order Form is subject to and made in accordance with the Arizona State University Licensing Agreement for Computer Aided Dispatch, Records Management System, and Mobile Data System between__________(Licensor) and the Arizona Board of Regents for and on behalf of Arizona State University (ASU) effective______(the Agreement). All capitalized terms not defined herein have the meaning in the Agreement. To the extent any provisions of this Order Form conflict with the provisions of the Agreement, the provisions of the Agreement will control. Any other terms in an Order Form provided by Licensor or on Licensor's website are expressly rejected.

ASU	Licensor
Arizona Board of Regents for and on behalf of Arizona State University	
Department:	Representative:
Shipping Address:	Billing Address:

Effective Date	Term	Delivery Method	Payment Terms
			Net-30 upon receipt of invoice

License Description	Quantity	Price

Services Description	Quantity	Price

Additional Terms

1. If in this Exhibit A ASU agrees to reimburse Licensor 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 in this Exhibit A ASU agrees to reimburse Licensor for any expenses, Licensor 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.

List any Attachments (including number of pages of each):

1. Exhibit B – Statement of Work

2. Exhibit C – Service Level Agreement

Arizona Board of Regents for and on behalf of Arizona State University

By:___________________________________

Name:________________________________

Title:__________________________________

Date Signed:___________________________

Licensor

By:__________________________________

Name:_______________________________

Title:_________________________________

Date Signed:__________________________

EXHIBIT B – SERVICE LEVEL AGREEMENT

This Service Level Agreement (SLA) is made in accordance with the Arizona State University Licensing Agreement for Computer Aided Dispatch, Records Management System, and Mobile Data System between_______(Licensor) and the Arizona Board of Regents for and on behalf of Arizona State University (ASU) effective___________(the Agreement). To the extent any provision in this SLA conflicts with any provision of the Agreement, the provision of the Agreement will control.

Arizona Board of Regents for and on behalf of Arizona State University

By:_________________________________

Name:______________________________

Title:_________________________________

Date Signed:__________________________

Licensor

By:_________________________________

Name:______________________________

Title:_________________________________

Date Signed:__________________________

EXHIBIT C – STATEMENT OF WORK

This Statement of Work (SOW) is made in accordance with the Arizona State University Licensing Agreement for Computer Aided Dispatch, Records Management System, and Mobile Data System between______(Licensor) and the Arizona Board of Regents for and on behalf of Arizona State University (ASU) effective___________(the Agreement). To the extent any provision in this SOW conflicts with any provision of the Agreement, the provision of the Agreement will control.

Arizona Board of Regents for and on behalf of Arizona State University	**Licensor**
By:__________________________________	**By**:_________________________________
Name:_______________________________	**Name**:______________________________
Title:_________________________________	**Title**:_______________________________
Date Signed:___________________________	**Date Signed**:_________________________

EXHIBIT D – INSURANCE REQUIREMENTS

Without limiting any liabilities or any other obligation of Licensor, Licensor 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 Licensor, 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 Licensor from liabilities that might arise out of the performance of the work under the Agreement by Licensor, its agents, representatives, employees, or subcontractors. These insurance requirements may change if Licensor is a foreign entity, or with foreign insurance coverage.

Depending upon the final scope of work, these insurance limits may be increased.

A. Minimum Scope and Limits of Insurance. Licensor's insurance coverage will be primary insurance with respect to all other available sources. Licensor 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 Licensor."

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 Licensor.

2. Automobile Liability. If Licensor 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 Licensor is not an individual then coverage will be a combined single limit of $1,000,000. If Licensor 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 Licensor, involving vehicles owned, leased, hired, or borrowed by Licensor."

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 Licensor.

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 Licensor.

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) Licensor is creating any code for ASU; 3) Licensor receives, stores, or analyzes ASU Data (including if the data is not online); 4) Licensor 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	$5,000,000
• Annual Aggregate	$5,000,000

a. This insurance will cover Licensor’s liability for acts, errors and omissions arising out of Licensor’s operations or services, including loss arising from unauthorized access, or use that results in identity theft or fraud. This insurance should also include Network Security, Privacy Liability, and Cyber Liability.

b. If the liability insurance required by the Agreement is written on a claims-made basis, Licensor 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 Licensor 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, Licensor 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 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 Licensor 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, Licensor 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. Licensor's certificate(s) may include all subcontractors as insureds under its policies as required by the Agreement, or Licensor 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

ASU will issue a Purchase Order(s) for goods and/or services awarded under this RFP.
(Fillable PDF versions of mandatory certifications are located on-line under <u>Supplier Forms</u>: <u>http://cfo.asu.edu/purchasing-forms</u>. ORIGINAL signatures are REQUIRED for either version.)

<u>CONFLICT OF INTEREST CERTIFICATION</u>

____
(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.

____
(Firm)

____
(Email Address)

____
(Signature required)

____
(Print name)

____
(Print title)

____
(Address)

____

____
(Phone)

____
(Fax)

____
(Federal Taxpayer ID Number)

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)

______________________________ ______________________________
(Signature required) (Phone)

______________________________ ______________________________
(Print name) (Fax)

______________________________ ______________________________
(Print title) (Federal Taxpayer ID Number)

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)

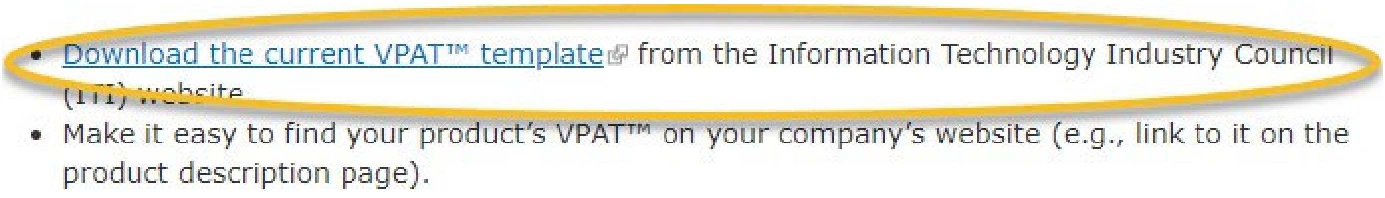
A Voluntary Product Accessibility Template (VPAT™) is a document that explains how information and communication technology (ICT) products such as software, hardware, electronic content, and support documentation meet (conform to) the Revised 508 Standards for IT accessibility. VPATs™ help Federal agency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

The Supplier Sustainability Questionnaire is used to help ASU understand how sustainable a supplier is. Sustainability is an important goal for the university, and as such, we expect our suppliers to help us support this goal. There are two different questionnaires posted, one is for large companies while the other is for small businesses. A company is considered to be large when there are more than 100 fulltime employees or over 4 million dollars in annual revenue generated.

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?

SECTION XIV – SECURITY REVIEW (REFERENCE DOCUMENT)

Security Review Form
Form version: 2018-10-19

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.

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

☐ This project is not using Planview.

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

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?

☐	**High**	We don't know who is responsible for the security design of the entire system.
☐	**High**	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.
☐	**Medium**	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.

□	**Medium**	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. However the vendor has not provided evidence of compliance with the ISO language.
□	**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

Number of Records	ex: 5000	Are direct services performed in the US?	ex: 5000
Estimated Yearly Addition	ex: 500	Is data stored in the US?	Yes/No
Are records purged?	Yes/No	Are data or systems accessible outside the US?	Yes/No

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

Regulated Data

□ PCI regulated (credit card data)

□ FERPA regulated (student data)

□ GDPR regulated (European Union user data)

□ HIPAA regulated (health data)

□ ITAR (import, export, defense-related technical data or foreign students)

□ Other Regulated (CJIS, COPPA, GLBA, etc.)

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.
- Google gives preference to https pages in its search results: see http://googleonlinesecurity.blogspot.in/2014/08/https-as-ranking-signal_6.html

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.
□	**Medium**	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.
□	**Low**	Sensitive data is encrypted on disk, but not on backups. There is no applicable regulation requiring encryption at rest.
□	**Addressed**	All sensitive data is encrypted at every location where it is stored, including user devices and backups.
□	**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 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.

Additional information (optional)

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?

□	**Unknown**	***RESEVED FOR SECURITY ARCHITECT SELECTION ONLY.*** 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 "Unknown" because there may be systems or connections that are not reviewed because they are not detailed on the diagram.
□	**Unknown**	***RESEVED FOR SECURITY ARCHITECT SELECTION ONLY.*** 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 "Unknown" because there may be systems or connections that are not reviewed because they are not detailed on the diagram.
□	**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

□	**Unknown**	Some new or changed servers have not yet been scanned or penetration tested.
□	**High**	A scan or penetration test reported one or more high severity issues that have not yet been addressed.
□	**High**	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).
□	**Medium**	A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).
□	**Addressed**	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).
□	**Addressed**	This project has no new servers and no changes to existing servers (other than servers inside a vendor's "cloud" and the vendor has signed ISO language).

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?

□	**Unknown**	At present we don't know if there will be development or QA instances of the web site(s).
□	**Medium**	Only a production instance exists. There is no place to test code or changes without impacting live systems and data.
□	**Low**	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.
□	**Addressed**	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.
□	**Addressed**	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).

□	**Unknown**	Some web sites have not yet been scanned or penetration tested.
□	**High**	A scan or penetration test reported one or more high severity issues that have not yet been addressed.
□	**High**	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).
□	**Medium**	A scan or penetration test reported one or more medium severity issues that have not yet been addressed (but no highs).
□	**Low**	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.
□	**Addressed**	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.

Additional information (optional)

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.

Additional information (optional)

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.
□	**Medium**	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.
□	**Low**	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.)
□	**Addressed**	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.
□	**Addressed**	None of the systems in this project have access to a database containing sensitive data.
□	**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?

□	**High**	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.
□	**High**	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.
□	**High**	One or more systems maintain an independent user authentication technique instead of standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS.
□	**Medium**	The login page uses https encryption and standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS, but subsequent pages revert back to http.
□	**Low**	Ordinary users are authenticated using standard ASU enterprise "single-sign-on" systems, but privileged users, such as site owners or administrators, are authenticated using a separate mechanism.
□	**Addressed**	All systems that require users to identify themselves use standard ASU enterprise "single-sign-on" authentication systems such as WebAuth or CAS.
□	**Addressed**	Access is in compliance with the ASU Privileged account standard: https://docs.google.com/file/d/0B7bqVGx3GJQbaC10bEl0ZndjVVE/
□	**Addressed**	Because all data is public, no user authentication is needed. Administrator access is controlled through existing mechanisms outside the scope of this project.

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?

□	**High**	One or more servers initiate or accept connections with their peers, but do not verify or otherwise restrict which servers can connect.
□	**High**	When a server logs in to another server, a password or other secret is transmitted across a network connection without encryption.
□	**Medium**	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 "black list" identifying which addresses are not allowed to connect.
□	**Low**	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 "white list" specifically identifying which addresses are allowed to connect, and denying all others by default.

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

Vendor	**Date vendor signed contract with ISO language**

Additional information (optional)

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.

Additional information (optional)

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.
□	**Addressed**	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.
□	**Addressed**	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 web site associated with this project has a "Tier 1" rating. (The Web Application Security Standard at 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.
□	**Low**	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.
□	**Addressed**	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.
□	**Addressed**	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.)

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 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?

□	**HIGH**	No logging is performed on any system
□	**High**	Some systems do not recognize and log typical attacks, or other unexpected or undesired events.
□	**Medium**	Potential security events are logged, but there is no human or automated review of those logs to alert on possible problems.
□	**Medium**	Potential security events are logged, but the logs do not fully comply with the ASU System Audit Requirements Standard http://links.asu.edu/systemauditrequirementsstandard.
□	**Low**	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.
□	**Addressed**	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?

□	**High**	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.
□	**Medium**	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.
□	**Low**	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 ofvalid signatures.

□	**Addressed**	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:

Additional information (optional)

Has the new software developed or purchased in this project undergone vulnerability scanning or penetration testing by an

entity other than the developer?

□	**High**	No vulnerbility scanning or penetration testing has been conducted
□	**High**	One or more components of new software (other than web sites) have not been vulnerability scanned or penetration tested.
□	**Medium**	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.
□	**Low**	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).
□	**Addressed**	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.
□	**Addressed**	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.
□	**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.)

Additional information (optional)

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?

□	**Medium**	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.)
□	**Medium**	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.)

□	**Medium**	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.
□	**Medium**	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.
□	**Low**	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.)
□	**Low**	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.)
□	**Low**	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.)
□	**Low**	Users are required to enable or install other plug-ins or media players not listed above. (Please describe in notes below.)
□	**Addressed**	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.
□	**Addressed**	The project will not use any of the technologies listed in this section.

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.)

□		
□		
□		

Additional information (optional)

Risk Score

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

Risk Rating	**Unknown**	**High**	**Medium**	**Low**	**Addressed**
Count of boxes checked					

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.

SECTION XIV – SECURITY ARCHITECTURE DIAGRAM (REFERENCE DOCUMENT #2)

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 moreapplicable.
    - 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 thereare 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 alldo 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/Fully_qualified_domain_name

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 theserver 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

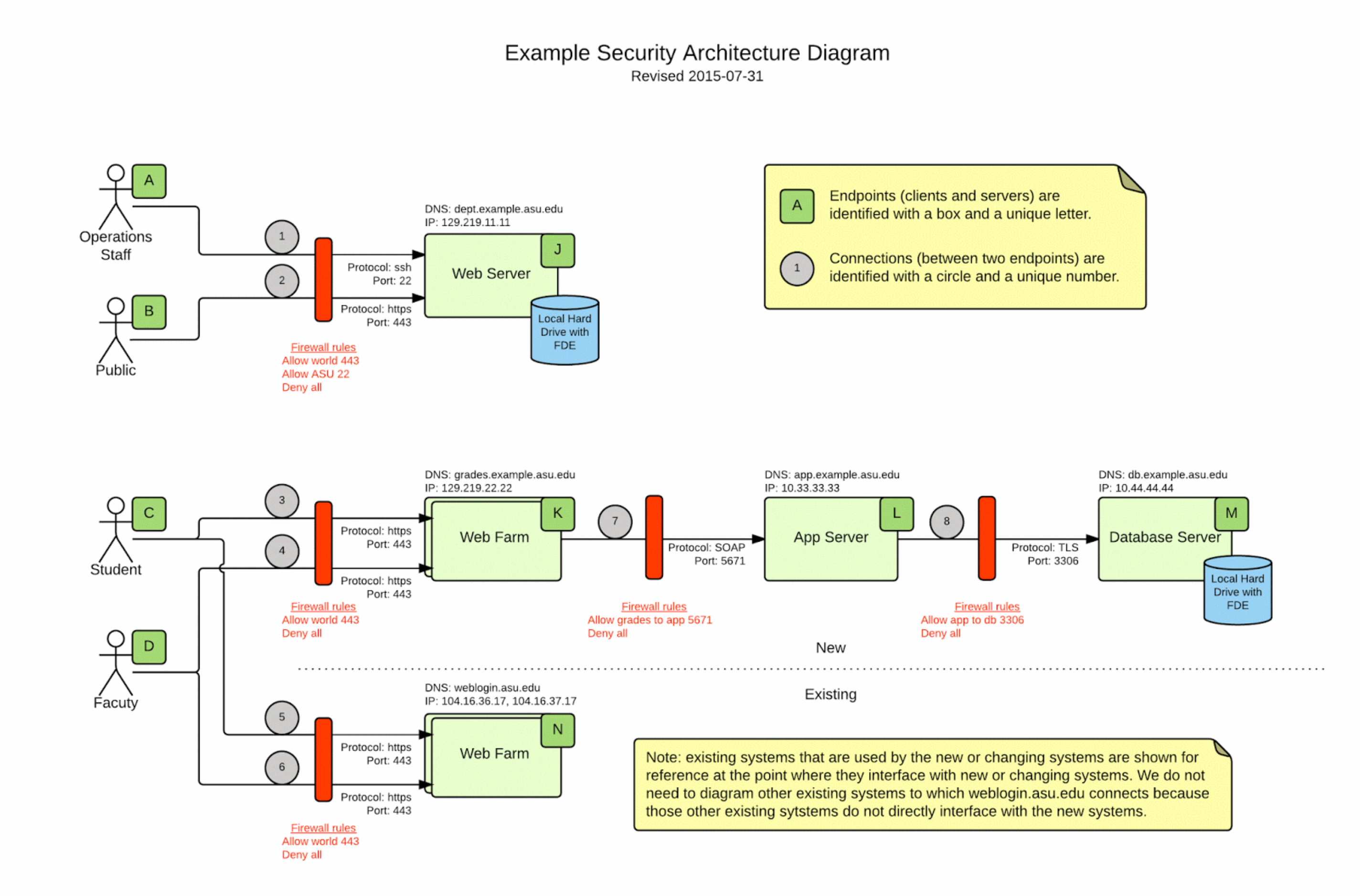
It may also help to distinguish existing endpoints, to which you will merely connect, from new endpoints that will be created as part of your project.

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.

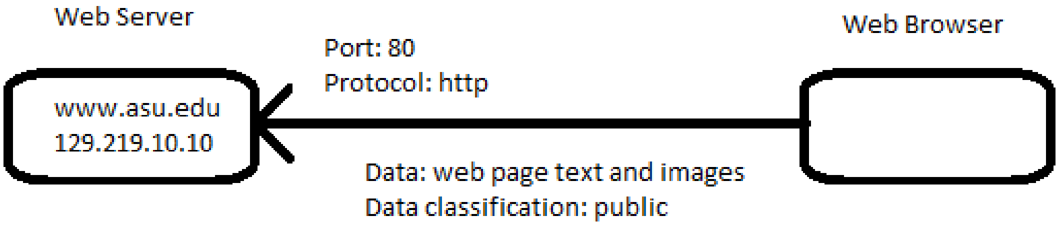
It is not necessary to show disk drives that are physically within a single server. However network shares are most likely part of a file server, and the file server should also be shown as a distinct endpoint.

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):

□	Section 1	RFP Checklist/Cover Page, Mandatory Certifications, Voluntary Product Accessibility Template (VPAT), & Supplier Sustainability Questionnaire.
□	Section 2	Proposer Qualifications, Section VII (Maximum 20 pages not including resumes, CVs, and/or Organizational charts).
□	Section 3	Response to the Specifications/Scope of Work, Section V. Also Include: • Attachments 1-7 (Provide both PDF and Excel files in soft/digital copy)
□	Section 4	Price Schedule, Section IX. Also include: • Attachment A Pricing Schedule
□	Section 5	Exceptions to Terms and Conditions, Section XII
□	Section 6	Confidential/Proprietary Justification Letter with Sealed documents, if applicable. Section IV, page 9, item 9.

In addition, the proposer must provide their review and acknowledgement of the following documents provided in this RFP (please mark off each document to acknowledge that you have reviewed the below documents in the RFP)

□	RFP 341904 (PDF Document)
□	All RFP Addendums (PDF Document)
□	Attachment 1 (Excel Document)
□	Attachment 2 (Excel Document)
□	Attachment 3 (Excel Spreadsheet)
□	Attachment 4 (Excel Spreadsheet)
□	Attachment 5 (Excel Document)

□	Attachment 6 (Excel Document)
□	Attachment 7 (Excel Document, within the RFP 341901 Document)
□	Attachment A – Pricing Schedule (Excel Document)

After carefully reviewing all the terms and conditions, the authorized undersigned agrees to furnish such goods/services in accordance with the specifications/scope of work.

Firm (CO.) Name	By (Signature)	Title

Date	Email Address	Phone #