THE
UNIVERSITY
OF RHODE ISLAND
DIVISION OF
ADMINISTRATION
AND FINANCE

THINK BIG WE DO™

PURCHASING DEPARTMENT
10 Tootell Road, Suite 3, Kingston, RI 02881 USA p: 401.874.2171 f: 401.874.2306 uri.edu/purchasing

BID/PROPOSAL

COMMODITY: **CAMPUS MOBILE APP** DATE: **1/2/2020**

FORMAL BID NO. ______ PUBLIC BID NO. ______ RFP NO. **100859**

BIDS ARE TO BE RECEIVED IN URI PURCHASING DEPARTMENT BY: DATE: **1/30/2020** TIME: **2:00 PM**
Eastern Time

BUYER: **RYAN PINCINCE/rlc** RP SURETY REQUIRED: YES: ______ NO: **X**

PRE-BID/PROPOSAL CONFERENCE: DATE: ______ TIME: ______

MANDATORY: YES: ______ NO: ______

LOCATION: ______

Questions concerning this solicitation must be received by the URI Purchasing Department at URIPurchasing@uri.edu no later than DATE: 1/14/2020 **TIME:** 12:00 PM **Please reference the Bid/RFP No. on all correspondence. Questions received, if any, will be posted on the internet as an addendum to this solicition at the conclusion of the question period. It is the responsibility of all interested parties to download this information.**

For Bid Solicitation Information visit: http://web.uri.edu/purchasing/bid-information/

BE SURE ALL INFORMATION SHOWN BELOW IS CORRECT.
FEDERAL EMPLOYER IDENTIFICATION NUMBER MUST BE INCLUDED.

COMPANY NAME: ______ FEIN: ______
STREET AND NUMBER: ______
CITY, STATE & ZIP CODE: ______

No offer will be considered that is not accompanied by the attached University of Rhode Island Bidder Certification Form/Contract Offer <u>completed</u> and <u>signed</u> by the offeror.

______ ______
Print Name and Title Telephone Number/Facsimile Number

______ ______
Signature Date E-mail address

THIS BID WILL NOT BE HONORED UNLESS SIGNED

The University of Rhode Island is an equal opportunity employer committed to the principles of affirmative action.

University of Rhode Island Bidder Certification Form

ALL OFFERS ARE SUBJECT TO THE REQUIREMENTS, PROVISIONS AND PROCEDURES CONTAINED IN THIS CERTIFICATION FORM. Offerors are expected to read, sign and comply with all requirements. Failure to do so may be grounds for disqualification of the offer contained herein.

Rules for Submitting Offers

This Certification Form must be attached in its entirety to the front of the offer and shall be considered an integral part of each offer made by a vendor to enter into a contract with the University of Rhode Island. As such, submittal of the entire Bidder Certification Form, signed by a duly authorized representative of the offeror attesting that he/she (1) has read and agrees to comply with the requirements set forth herein and (2) to the accuracy of the information provided and the offer extended, is a mandatory part of any contract award.

To assure that offers are considered on time, each offer must be submitted with the specific Bid/RFP/LOI number, date and time of opening marked in the upper left hand corner of the envelope. Each bid/offer must be submitted in separate sealed envelopes.

A complete signed (in ink) offer package must be delivered to the University of Rhode Island Purchasing Office by the time and date specified for the opening of responses in a sealed envelope.

Bids must be submitted on the URI bid solicitation forms provided, indicating brand and part numbers of items offered, as appropriate. Bidders must submit detailed cuts and specs on items offered as equivalent to brands requested WITH THE OFFER. Bidders must be able to submit samples if requested.

Documents misdirected to other State locations or which are not present in the University of Rhode Island Purchasing Office at the time of opening for whatever cause will be deemed to be late and will not be considered. For the purposes of this requirement, the official time and date shall be that of the time clock in the reception area of the University of Rhode Island Purchasing Office. Postmarks shall not be considered proof of timely submission.

RIVIP SOLICITATIONS. To assure maximum access opportunities for users, public bid/RFP solicitations shall be posted on the RIVIP for a minimum of seven days and no amendments shall be made within the last five days before the date an offer is due. Except when access to the Web Site has been severely curtailed and it is determined by the Purchasing Agent that special circumstances preclude extending a solicitation due date, requests to mail or fax hard copies of solicitations will not be honored. When the result of an internet solicitation is unsuccessful, the University of Rhode Island will cancel the original solicitation and resolicit the original offer directly from vendors.

PRICING. Offers are irrevocable for sixty (60) days from the opening date (or such other extended period set forth in the solicitation), and may not be withdrawn, except with the express permission of the University Purchasing Agent. All pricing will be considered to be firm and fixed unless otherwise indicated. The University of Rhode Island is exempt from Federal excise taxes and State Sales and Use Taxes. Such taxes shall not be included in the bid price. PRICES QUOTED ARE FOB DESTINATION.

DELIVERY and PRODUCT QUALITY. All offers must define delivery dates for all items; if no delivery date is specified, it is assumed that immediate delivery from stock will be made. The contractor will be responsible for delivery of materials in first class condition. Rejected materials will be at the vendor's expense.

PREVAILING WAGE, OSHA SAFETY TRAINING and APPRENTICESHIP REQUIREMENTS. Bidders must comply with the provisions of the Rhode Island labor laws, including R.I. Gen. Laws §§ 37-13-1 et seq. and occupational safety laws, including R.I. Gen. Laws §§ 28-20-1 et seq. These laws mandate for public works construction projects the payment of prevailing wage rates, the implementation and maintenance of occupational safety standards, and for projects with a minimum value of $1 Million, the employment of apprentices. The successful Bidder must submit certifications of compliance with these laws from each of its subcontractors prior to their commencement of any work. Prevailing wage rates, apprenticeship requirements, and other workforce and safety regulations are accessible at www.dlt.ri.gov.

PUBLIC RECORDS. Offerors are advised that all materials submitted to the University for consideration in response to this solicitation will be considered without exception to be Public Records pursuant to Title 38 Chapter 2 of the Rhode Island General Laws, and will be released for inspection immediately upon request once an award has been made. Offerors are encouraged to attend public bid/RFP openings to obtain information; however, bid/RFP response summaries may be reviewed after award(s) have been made by visiting the Rhode Island Vendor Information Program (RIVIP) at www.purchasing.ri.gov, Solicitation Opportunities +, Other Solicitation Opportunities or appearing in person at the University of Rhode Island Purchasing Office Mondays through Fridays between 8:30 am – 3:30 pm. Telephone requests for results will not be honored. Written requests for results will only be honored if the information is not available on the RIVIP.

Award will be made the to the responsive and responsible offeror quoting the lowest net price in accordance with specifications, for any individual item(s), for major groupings of items, or for all items listed, at the University's sole option.

BID SURETY. Where bid surety is required, bidder must furnish a bid bond or certified check for 5% of the bid total with the bid, or for such other amount as may be specified. Bids submitted without a required bid surety will not be considered.

SPECIFICATIONS. Unless specified "no substitute", product offerings equivalent in quality and performance will be considered (at the sole option of the University) on the condition that the offer is accompanied by detailed product specifications. Offers which fail to include alternate specifications may be deemed nonresponsive.

VENDOR AUTHORIZATION TO PROCEED. When a purchase order, change order, contract/agreement or contract/agreement amendment is issued by the University of Rhode Island, no claim for payment for services rendered or goods delivered contrary to or in excess of the contract terms and scope shall be considered valid unless the vendor has obtained a written change order or contract amendment issued by the University of Rhode Island Purchasing Office PRIOR to delivery.

Any offer, whether in response to a solicitation for proposals or bids, or made without a solicitation, which is accepted in the form of an order OR pricing agreement made in writing by the University of Rhode Island Purchasing Office, shall be considered a binding contract.

REGULATIONS, GENERAL TERMS AND CONDITIONS GOVERNING STATE AND BOARD OF GOVERNORS FOR HIGHER EDUCATION CONTRACTS. This solicitation and any contract or purchase order arising from it are issued in accordance with the specific requirements described herein, and the State's Purchasing Laws and Regulations and other applicable State Laws, including the Board of Governors for Higher Education General Terms and Conditions of Purchase. The regulations, General Terms and Conditions are incorporated into all University of Rhode Island contracts and can be viewed at: www.ribghe.org/procurementregs113006.pdf and www.purchasing.ri.gov.

ARRA SUPPLEMENTAL TERMS AND CONDITIONS. Contracts and sub-awards funded in whole or in part by the American Recovery and Reinvestment Act of 2009. Pub.L.No. 111-5 and any amendments thereto, such contracts and sub-awards shall be subject to the Supplemental Terms and Conditions for Contracts and Sub-awards funded in whole or in part by the American Recovery and Reinvestment Act of 2009. Pub.L.No. 111-5 and any amendments thereto located on the Division of Purchases website at www.purchasing.ri.gov.

EQUAL EMPLOYMENT OPPORTUNITY. Compliance certificate and agreement procedures will apply to all awards for supplies or services valued at $10,000 or more. Minority Business Enterprise policies and procedures, including subcontracting opportunities as described in Title 37 Chapter 14.1 of the Rhode Island General Laws also apply.

PERFORMANCE BONDS. Where indicated, successful bidder must furnish a 100% performance bond and labor and payment bond for contracts subject to Title 37 Chapters 12 and 13 of the Rhode Island General Laws. All bonds must be furnished by a surety company authorized to conduct business in the State of Rhode Island. Performance bonds must be submitted within 21 calendar days of the issuance of a tentative notice of award.

DEFAULT and NON-COMPLIANCE Default and/or non-compliance with the requirements and any other aspects of the award may result in withholding of payment(s), contract termination, debarment, suspension, or any other remedy necessary that is in the best interest of the state/University of Rhode Island.

COMPLIANCE Vendor must comply with all applicable federal, state and local laws, regulations and ordinances.

SPRINKLER IMPAIRMENT AND HOT WORK. The Contractor agrees to comply with the practices of the State's Insurance carrier for sprinkler impairment and hot work. Prior to performing any work, the Contractor shall obtain the necessary information for compliance from the Risk Management Office at the Department of Administration or the Risk Management Office at the University of Rhode Island.

Each bid proposal for a *public works project* must include a "public copy" to be available for public inspection upon the opening of bids. **Bid Proposals that do not include a copy for public inspection will be deemed nonresponsive.**

For further information on how to comply with this statutory requirement, see R.I. Gen. Laws §§ 37-2-18(b) and (j). Also see State of Rhode Island Procurement Regulation 5.11 at http://www.purchasing.ri.gov/rulesandregulations/rulesAndRegulations.aspx

ALL CONTRACT AWARDS ARE SUBJECT TO THE FOLLOWING DISCLOSURES & CERTIFICATIONS

Offerors must respond to every disclosure statement. A person authorized to enter into contracts must sign the offer and attest to the accuracy of all statements.

Indicate Yes (Y) or No (N):

____1 State whether your company, or any owner, stockholder, officer, director, member, partner, or principal thereof, or any subsidiary or affiliated company, has been subject to suspension or debarment by any federal, state, or municipal government agency, or the subject of criminal prosecution, or convicted of a criminal offense with the previous five (5) years. If so, then provide details below.

____2 State whether your company, or any owner, stockholder, officer, director, member, partner, or principal thereof, or any subsidiary or affiliated company, has had any contracts with a federal, state or municipal government agency terminated for any reason within the previous five (5) years. If so, then provide details below.

____3 State whether your company or any owner, stockholder, officer, director, member, partner, or principal thereof, or any subsidiary or affiliated company, has been fined more than $5000 for violation(s) of Rhode Island environmental laws by the Rhode Island Department of Environmental Management within the previous five (5) years. If so, then provide details below.

____4 I/we certify that I/we will immediately disclose, in writing, to the University Purchasing Agent any potential conflict of interest which may occur during the course of the engagement authorized pursuant to this contract.

____5 I/we acknowledge that, in accordance with (1) Chapter §37-2-54(c) of the Rhode Island General Laws "no purchase or contract shall be binding on the state or any agency thereof unless approved by the Department [of Administration] or made under general regulations which the Chief Purchasing Officer may prescribe," and (2) RIGL section §37-2-7(16) which identifies the Board of Governors for Higher Education as a public agency and gives binding contractual authority to the University Purchasing Agent, including change orders and other types of contracts and under State Purchasing Regulation 8.2.1.1.2 any alleged oral agreement or arrangements made by a bidder or contractor with any agency or an employee of the University of Rhode Island may be disregarded and shall not be binding on the University of Rhode Island.

____6 I/we certify that I or my/our firm possesses all licenses required by Federal and State laws and regulations as they pertain to the requirements of the solicitation and offer made herein and shall maintain such required license(s) during the entire course of the contract resulting from the offer contained herein and, should my/our license lapse or be suspended, I/we shall immediately inform the University of Rhode Island Purchasing Agent in writing of such circumstance.

____7 I/we certify that I/we will maintain required insurance during the entire course of the contract resulting from the offer contained herein and, should my/our insurance lapse or be suspended, I/we shall immediately inform the University of Rhode Island Purchasing Agent in writing of such circumstance.

____8 I/we certify that I/we understand that falsification of any information herein or failure to notify the University of Rhode Island Purchasing Agent as certified herein may be grounds for suspension, debarment and/or prosecution for fraud.

____9 I/we acknowledge that the provisions and procedures set forth in this form apply to any contract arising from this offer.

____10 I/we acknowledge that I/we understand the State's Purchasing Laws (§37-2 of the General Laws of Rhode Island) and Purchasing Regulations and General Terms and Conditions available at the Rhode Island Division of Purchases Website (http://www.purchasing.ri.gov) and the Board of Governors Website (www.ribghe.org/procurementregs113006.pdf) apply as the governing conditions for any contract or purchase order I/we may receive from the University of Rhode Island, including the offer contained herein.

____11 I/we certify that the bidder: (i) is not identified on the General Treasurer's list, created pursuant to R.I. Gen. Laws § 37-2.5-3, as a person or entity engaging in investment activities in Iran described in § 37-2.5-2(b); and (ii) is not engaging in any such investment activities in Iran.

____12 If the product is subject to Department of Commerce Export Administration Regulations (EAR) or International Traffic in Arms Regulations (ITAR), please provide the Export Control Classification Number (ECCN) or the US Munitions List (USML) Category:______________________

____13 I/we certify that the above information is correct and complete.

IF YOU HAVE ANSWERED "YES" TO QUESTIONS #1 – 3 OR IF YOU ARE UNABLE TO CERTIFY YES TO QUESTIONS #4 – 11 and 13 OF THE FOREGOING, PROVIDE DETAILS/EXPLANATION IN AN ATTACHED STATEMENT. INCOMPLETE CERTIFICATION FORMS SHALL BE GROUNDS FOR DISQUALIFICATION OF OFFER.

Signature below commits vendor to the attached offer and certifies (1) that the offer has taken into account all solicitation amendments, (2) that the above statements and information are accurate and that vendor understands and has complied with the requirements set forth herein.

Vendor's Signature:____________________________________ Bid Number:______________ Date:____________
(Person Authorized to enter into contracts; signature must be in ink) (if applicable)

____
Print Name and Title of Company official signing offer Telephone Number

SECTION 1: INTRODUCTION

The Rhode Island Council on Postsecondary Education/University of Rhode Island is soliciting proposals for the University of Rhode Island from qualified OFFERORS to provide a vendor-hosted, full-featured, low-code rapid mobile application development platform and tools in accordance with the terms of this Request for Proposal ("RFP") and the General Terms and Conditions of Purchase indicated in the attached URI Bidder Certification Form.

The initial contract period will begin approximately February 1, 2020 for three years. Contracts may be renewed for up to three additional 12-month periods based on vendor performance and the availability of funds.

This is a Request for Proposals, not a Request for Quotes. Responses will be evaluated on the basis of the relative merits of the proposal, in addition to cost; there will be no public opening and reading of responses received by the University of Rhode Island Purchasing Department pursuant to this solicitation, other than to name those offerors who have submitted proposals.

Instructions and Notifications to Offerors

1. Potential offerors are advised to review all sections of this RFP carefully and to follow instructions completely, as failure to make a complete submission as described elsewhere herein may result in rejection of the proposal.

2. Alternative approaches and/or methodologies to accomplish the desired or intended results of this RFP are solicited. However, proposals which depart from or materially alter the terms, requirements, or scope of work defined by this RFP may be rejected as being non-responsive.

3. All costs associated with developing or submitting a proposal in response to this RFP or for providing oral or written clarification of its content shall be borne by the vendor. The University assumes no responsibility for these costs even if the RFP is cancelled or continued.

4. Proposals are considered to be irrevocable for a period of not less than 180 days following the opening date, and may not be withdrawn, except with the express written permission of the University of Rhode Island Purchasing Director.

5. All pricing submitted will be considered to be firm and fixed unless otherwise indicated in the proposal.

6. It is intended that an award pursuant to this RFP will be made to a prime vendor, or prime vendors in the various categories, who will assume responsibility for all aspects of the work. Subcontracts are permitted, provided that their use is clearly indicated in the vendor's proposal, and the subcontractor(s) to be used is identified in the proposal.

7. The purchase of goods and/or services under an award made pursuant to this RFP will be contingent on the availability of appropriated funds.

8. Vendors are advised that all materials submitted to the University of Rhode Island Purchasing Department for consideration in response to this RFP may be considered to be public records, as defined in R. I. Gen. Laws § 38-2-1, *et seq*., and may be released for inspection upon request, once an award has been made.

   Any information submitted in response to this RFP that a vendor believes are trade secrets or commercial or financial information which is of a privileged or confidential nature should be clearly marked as such. The vendor should provide a brief explanation as to why each portion of information that is marked should be withheld from public disclosure. Vendors are advised that the University of Rhode Island Purchasing Department may release records marked confidential by a vendor upon a public records request if the University determines the marked information does not fall within the category of trade secrets or commercial or financial information which is of a privileged or confidential nature.

9. Interested parties are instructed to peruse the Division of Purchases website on a regular basis, as additional information relating to this solicitation may be released in the form of an addendum to this RFP.

10. By submission of proposals in response to this RFP vendors agree to comply with R. I. General Laws § 28-5.1-10 which mandates that contractors/subcontractors doing business with the State of Rhode Island exercise the same commitment to equal opportunity as prevails under Federal contracts controlled by Federal Executive Orders 11246, 11625 and 11375.

    Vendors are required to ensure that they, and any subcontractors awarded a subcontract under this RFP, undertake or continue programs to ensure that minority group members, women, and persons with disabilities are afforded equal employment opportunities without discrimination on the basis of race, color, religion, sex, sexual orientation, gender identity or expression, age, national origin, or disability.

    Vendors and subcontractors who do more than $10,000 in government business in one year are prohibited from engaging in employment discrimination on the basis of race, color, religion, sex, sexual orientation, gender identity or expression, age, national origin, or disability, and are required to submit an "Affirmative Action Policy Statement."

    Vendors with 50 or more employees and $50,000 or more in government contracts must prepare a written "Affirmative Action Plan" prior to issuance of a purchase order.

    a. For these purposes, equal opportunity shall apply in the areas of recruitment, employment, job assignment, promotion, upgrading, demotion, transfer, layoff, termination, and rates of pay or other forms of compensation.

    b. Vendors further agree, where applicable, to complete the "Contract Compliance Report" (http://odeo.ri.gov/documents/odeo-eeo-contract-compliance-report.pdf), as well as the "Certificate of Compliance" (http://odeo.ri.gov/documents/odeo-eeo-certificate-of-compliance.pdf and submit both documents, along with their Affirmative Action Plan or an Affirmative Action Policy Statement, prior to issuance of a purchase order. For public works projects vendors and all subcontractors must submit a "Monthly Utilization Report" (http://odeo.ri.gov/documents/monthly-employment-utilization-report-form.xlsx) to the ODEO/State Equal Opportunity Office, which identifies the workforce actually utilized on the project.

For further information, contact the Rhode Island Equal Employment Opportunity Office, at 222-3090 or via e-mail at Krystal.Waters@doa.ri.gov .

11. In accordance with R. I. Gen. Laws § 7-1.2-1401 no foreign corporation has the right to transact business in Rhode Island until it has procured a certificate of authority so to do from the Secretary of State. This is a requirement only of the successful vendor(s). For further information, contact the Secretary of State at (401-222-3040).

12. In accordance with R. I. Gen. Laws §§ 37-14.1-1 and 37-2.2-1 it is the policy of the State to support the fullest possible participation of firms owned and controlled by minorities (MBEs) and women (WBEs) and to support the fullest possible participation of small disadvantaged businesses owned and controlled by persons with disabilities (Disability Business Enterprises a/k/a "DisBE")(collectively, MBEs, WBEs, and DisBEs are referred to herein as ISBEs) in the performance of State procurements and projects. As part of the evaluation process, vendors will be scored and receive points based upon their proposed ISBE utilization rate in accordance with 150-RICR-90-10-1, "Regulations Governing Participation by Small Business Enterprises in State Purchases of Goods and Services and Public Works Projects". As a condition of contract award vendors shall agree to meet or exceed their proposed ISBE utilization rate and that the rate shall apply to the total contract price, inclusive of all modifications and amendments. Vendors shall submit their ISBE participation rate on the enclosed form entitled "MBE, WBE and/or DisBE Plan Form", which shall be submitted in a separate, sealed envelope as part of the proposal. ISBE participation credit will only be granted for ISBEs that are duly certified as MBEs or WBEs by the State of Rhode Island, Department of Administration, Office of Diversity, Equity and Opportunity or firms certified as DisBEs by the Governor's Commission on Disabilities. The current directory of firms certified as MBEs or WBEs may be accessed at http://odeo.ri.gov/offices/mbeco/mbe-wbe.php. Information regarding DisBEs may be accessed at www.gcd.ri.gov.

For further information, visit the Office of Diversity, Equity & Opportunity's website, at http://odeo.ri.gov// and *see* R.I. Gen. Laws Ch. 37-14.1, R.I. Gen. Laws Ch. 37-2.2, and 150-RICR-90-10-1. The Office of Diversity, Equity & Opportunity may be contacted at, (401) 574-8670 or via email Dorinda.Keene@doa.ri.gov

13. Complete a separate Higher Education Cloud Vendor Assessment Tool.: The Higher Education Cloud Vendor Assessment Tool (HECVAT) may be accessed electronically at https://security.uri.edu/forms/sig/ and will need to be completed by each vendor. The "HECVAT" is intended to simplify and speed up the process of gathering the information to assess the controls used by your organization to protect the University's data, comply with the terms of the Agreement and to provide an operationally stable, protected and recoverable service. Your printed completed copy of the HECVAT, provided with your RFP response, will be reviewed and approved for compliance by the Chief Information Security Officer prior to the Technical Review. HECVATs not approved will not proceed to the Technical Review.

14. Complete a separate IT Security Services Security Checklist for Mobile Apps: The Security Checklist for Mobile Apps is attached to this RFP and will need to be completed by each vendor. The checklist does not aim to be a comprehensive list of security requirements. Rather, it focuses on peculiarities of mobile application security, as well as common security mistakes that developers make. The goal of following the checklist is to avoid major pitfalls when coding mobile apps. Your printed completed copy of the Security Checklist, provided with your RFP response, will be reviewed and approved for compliance by the Chief Information Security Officer prior to the Technical Review. Checklists not approved will not proceed to the Technical Review.

Restrictions on Communications – No Bidder-initiated contact, other than normal business activities not associated with this procurement, will be allowed after the issuance of this RFP between Bidders and University employees or their agents regarding this solicitation, except with express permission of the University Purchasing Department. Any such other contact may be considered improper and may disqualify a Bidder from further consideration. The appropriate channel to direct any communications, concerns or questions regarding the RFP is through the email address provided herein.

If a Bidder fails to notify the University of Rhode Island Purchasing Department contact person of an error in this RFP which was known or reasonably should have been known to the Bidder, the Bidder shall submit a response at the Bidder's own risk. If awarded the contract, the Bidder shall not be entitled to additional compensation or performance time by reason of the error or its later correction.

SECTION 2: BACKGROUND

The University of Rhode Island (URI) seeks an innovative partner who will provide and host the University's campus mobile application development platform and position its brand as a leader in the mobile app space.

The University of Rhode Island is the state's only public land grant research institution. Founded in 1892, the University's main campus is in Kingston, Rhode Island with 3 additional satellite campuses in the state. The University maintains an extensive website with social media integration (Facebook, Twitter, Instagram, YouTube). The University also contracts with various vendors, including its Student Information and HR Systems (PeopleSoft 9.2 Campus Solutions and HCM, respectively) and Learning Management System (Sakai, transitioning to D2L Brightspace in 2020).

Content creation at URI is managed in a distributed fashion, where many individual subject-matter experts contribute pages to our web presence. The mobile platform must allow for many content creators with regulated access to specific portions of the mobile content, with different administrative rights to create and edit this content. Similarly, app users will have access to publicly available information, plus specific information tailored to their campus role(s).

The initial audiences for the mobile app are the prospective and undergraduate students on the Kingston campus, with initial rollout to be timed with accepted student notification in April 2020. Other audiences to follow include graduate students, alumni, faculty, staff and other URI campuses. A primary goal is to provide personalized content based upon the student's demographic, geographic, academic, or other activities.

Vendors bidding must demonstrate an excellent service history with the ability to be flexible, innovative and technologically advanced. The vendor must fully support all aspects of the mobile platform, clearly identifying when and where subcontractors are used to provide this support. The vendor must have a clearly defined Service Level Agreement that includes acceptable guaranteed system availability.

SECTION 3: SCOPE OF WORK AND REQUIREMENTS

General Scope of Work

The University of Rhode Island seeks to obtain a rapid mobile application development platform and support services to be provided by a qualified vendor. The selected platform will assist the University in meeting its goal of creating a 21st century 24/7 learning environment by implementing applications of technology that promote innovation, engagement, efficiency and effectiveness.

The solution must have capability to deploy native apps, mobile web apps, and full web apps for desktop. It must have the ability to integrate internal and external apps, and external links, within the delivered functionality. The solution must serve relevant, personalized content in real-time.

The mobile application should run on Android and iOS at minimum, both smartphones and tablets, and take advantage of features of each platform and OS. A mobile-enabled, responsive HTML5 website is a desirable added feature. The system must provide an easy-to-use app assembly and publishing tool for business or non-technical users. The authentication mechanism should support modern authentication authorities and provide the granularity to restrict the users to specific modules and rights.

The proposed platform must already be used in Higher Education and provide integration, as appropriate, with existing University software. The initial deployment will include read-only integration of PeopleSoft Campus Solutions version 9.2, with full integration of PeopleSoft CS and HCM, and D2L Brightspace Learning Management System to follow.

The initial implementation should provide a comprehensive experience tailored for various student personas, plus a New Student Orientation module template.

In addition, the vendor must also provide ongoing technical support services for all service delivery of the system to URI, including ongoing live environment support, performance monitoring, data security and procedures, patches, fixes and upgrades.

Specific Activities / Tasks

Each proposal should contain the following information at a minimum:

A. General Requirements

Req. Nbr	Description

A.1	A proven track record in providing low- or no-code mobile development platforms to other higher education institutions in the United States, particularly medium to large size research institutions, as determined by the overall vendor responses to this RFP.
A.2	A clear, well-defined, mutually agreed Service Level Agreement which defines: • Guaranteed hours of system availability for live environments as well as test and/or training environments • Policy, plan and procedures for maintenance service times by the vendor to include process of planning and testing system maintenance with URI including patches, fixes and upgrades; the process of mutually determining an appropriate time for the platform to be upgraded or modified in any way; communication before, during and after system maintenance; test and approval processes; areas of responsibility for both vendor and URI, and other required information to be determined. • Policy for keeping URI's mobile platform current with patches, fixes and feature upgrades.
A.3	24/7 service support with clearly defined procedures for reporting and resolving problems of all categories, such as system down to sporadic tool failure. These procedures must include voice and web contact methods and identify how, when and under what circumstances URI will work directly with a support technician to resolve a problem as opposed to a trouble ticketing procedure. Use of subcontracted resources for support must be identified and clearly explained including time zone differences, procedural difference, quality assurances and accountability.
A.4	Clearly defined points of contact describing responsibilities such as for direct account support, technical support, emergency support, off-business hours support, project management.
A.5	The ability to provide a test platform with URI data to be used for implementing new releases, tools, and training URI staff.
A.6	Clearly identified features that will be available within the platform, each supported and maintained by bidder.
A.7	Adherence to the URI Brand Visual Standards Guide as set by the University's Communications & Marketing department, branding the app accordingly.

B. Company Organization and History

Req. Nbr	Description
B.1	Provide a brief overview of your company and history of your organization, including any relationship(s) with a parent, subsidiary or affiliated company.
B.2	Describe your organizational philosophy/approach to client services.
B.3	Provide your most recent ratings for each of the agencies listed below: A.M. Best Standard & Poor's Fitch Moody's
B.4	How long has your company been providing and supporting mobile application development platforms to higher education institutions in the United States?
B.5	Provide a description of your data center and support staff offices, including the following: • Describe the physical environment(s) and location(s) of your Data Center(s). • Describe the physical environment and location of your support staff offices.

B.6	What fiduciary responsibility does your organization assume for this project?
B.7	How do you ensure that your record-keeping system is in compliance with all regulations?
B.8	Who is your compliance officer/consultant or legal counsel?
B.9	Provide at least three college/university references where you have provided or are currently providing a mobile application platform for a higher education institution for a minimum of two years. References must include name and address of institution, dates of service, and institution's contact person's name, telephone number and email
B.10	Please list all platform upgrades and versions over the past three years, detailing the functionality (new features) added with each of these upgrades.
B.11	Is your company currently for sale or involved in any transaction to expend or to become acquired by another business entity? If yes, please explain the impact both in organizational and directional terms.

C. Technical Requirements Overview

Req. Nbr	Description
	System Requirements
C.1	The mobile framework shall allow the campus to deliver apps that run natively on Apple iOS and Google Android, for both phone and tablet devices. Support must also include a mobile web version, which is optimized for both small and large devices, including tablets and desktop. Explain how this is done.
C.2	Does your solution require any additional software or other solution(s) for complete functionality? If so, provide a list.
C.3	The system shall have ability to release new modules or features to users without re-submitting native app versions to app stores over and again. Explain how this is done.
C.4	Describe how your solution supports production, test, and training environments. Describe acceptance and migration to production.
C.5	Describe your support for group and role-based security, hierarchical administration, multi-group membership, data element access control.
C.6	Can your solution provide programmable source code, and the ability to support the development, extension, or customization of standard modules at the source level, which may be implemented directly by URI. If so, please explain how this customization works, and what training is provided.
C.7	Vendor shall supply an extensible middleware platform that is designed to aggregate data from web services, including web services that will not be provided under this project. Explain how this is done.
C.8	Platform should allow the combining of data sources and deep-linking of modules for a seamless user experience. Explain how this is done.
C.9	Are there other use cases for your platform that are available to URI? If so, please describe.
C.10	Does your solution offer vendor integrations? If so, please describe the vendor community, and the ability to share extensions.
	Accessibility Requirements
C.11	The mobile platform and products created by the platform shall deliver applications that are accessible to users with disability. The product must meet or attempt to meet accessibility standards as described by the Federal 508 guidelines as it pertains to web software. Describe the accessibility features in regard to page display and the functionality of your product.

C.12	Describe how your organization designs and tests for accessibility as part of the mobile app design and development.
C.13	The vendor must provide a VPAT (https://www.section508.gov/sell/vpat) or equivalent reporting template and supporting documentation as necessary.
	Analytics
C.14	Download analytics must be available for viewing and measuring.
C.15	Analytics on feature usage and engagement must be available.
C.16	Analytics tools should be available for departments to use to reach out to users.
C.17	Describe all data captured and how that data can be accessed and/or distributed.
C.18	Describe the parameters available for analysis (e.g., time periods, locations, devices, platforms, etc.)

D. Features

Req. Nbr	Description
D.1	What is included your base product?
D.2	What is considered add-on? Please enumerate options that are available.
D.3	The initial implementation should include a prebuilt New Student Orientation template. Please describe its features.
D.4	Describe how the solution determines the appropriate persona upon opening the app (e.g., automatic via internal/external information, self-selection)? Will the app remember the persona, or must the user select it each time the app is opened?
D.5	Is your solution able to automatically switch to a different persona once an event persona is no longer relevant or available (e.g., orientation, move-in week)? If so, please describe.
D.6	Can you your solution automatically select the appropriate campus version of the app based on the geolocation of the device. If so, please explain.
D.7	Describe how the app will interact with external social, image, and video feeds (e.g., Twitter, Facebook, Vimeo, YouTube, Flickr, Instagram). Describe how the user can filter these feeds.
D.8	The app must have an athletics feed, showing scores and game day information. URI currently has two sources, Presto Sports and AYC Media. Can your solution combine both sources into one feed? If so, please explain how this is done.
D.9	Describe how your solution incorporates live webcam feeds. Can multiple feeds exist on the same page?
D.10	Can the solution add personalized, live content to existing screens? If so, please describe.
D.11	The app must have a calendar of events.
D.12	The solution must support browsing or searching for events. Describe how the app would integrate multiple calendar feeds, and display weekly or monthly views, in addition to adding events to a native calendar.
D.13	Is event category filtering available? If so, please describe.
D.14	Can your solution display the user's class schedule and feed it into the calendar? If so, please describe.
D.15	The app must display dining options with daily menus, hours, map locations, and dining hall webcam feeds.

D.16	The platform must utilize campus maps, extended with customized layers, points of interest, landmarks, and custom directions, and embed these customized capabilities directly into the workflow of the app. Explain how this is done.
D.17	URI currently has Google-based customized campus maps for real time wayfinding on campus. Please describe the method(s) your solution uses to incorporate custom map data into the map. If your solution can use URI's current API-based data layers, please describe.
D.18	Can your solution display the user's class schedule, pinpoint the classroom's locations in the map, and route the student directly to the classroom? If so, please describe.
D.19	The app must have a customizable news feed. Describe how your solution consumes news (and other) feeds and displays the content.
D.21	Describe how your solution supports the Admissions process.
D.22	Does your solution include a QR code reader and or generator? If so, please describe.
D.23	Does your solution support full site cross module search? If so, please describe.
D.24	Describe how your platform harnesses the capabilities of beacon technology.
D.25	Does your solution currently include features related to, or integrating with Artificial Intelligence (AI), Augmented Reality (AR), or Virtual Reality (VR)? If so, please describe.
	Messaging/Push Notifications
D.25	Please describe the methods of communication your solution provides (e.g., push, banner, email, etc.). How is each managed and administered?
D.26	Can external systems access the alert and messaging system? If so, please explain.
D.27	Does your solution allow for targeted messages to subpopulations of users (e.g., specific class or dorm, role-based messages, etc.)? If so, please describe.
D.28	Does your solution provide the ability to deliver messages to specific named users?
D.29	Does your solution offer the ability to schedule messages? If so, please describe.
D.30	Does your solution allow URI to control message-related authoring and approval permissions across the organization? If so, please describe.
D.31	Describe options for multiple/repeat notifications.
D.32	Does your solution provide push notifications based on GPS beacons and/or geofences? If so, please give examples.
D.33	Can users control their communication experience (e.g., scheduling, digest, opt-in, opt-out)?
D.34	Please describe the analytics associated with the communication solution.

E. Integration

Req. Nbr	Description
E.1	Can custom integrations be added to your solution using core technology, and without needing to resubmit to the app stores?
E.2	Describe how your solution would integrate URI data (whether data feed, web service, etc.) into the app. Would a vendor-specified data format be required, or could current URI System data sources be used?
E.3	Describe your solution's ability to present the course catalog.
E.4	The solution must connect with the University's LMS system (Sakai/D2L Brightspace), and provide personalized course information, announcements, grades, and course assignments by integrating directly with the LMS's web services for URI.

E.5	The solution must implement web services that integrate with PeopleSoft Campus Solutions version 9.2, including search classes, add/drop/enroll classes, balances, and view grades. Describe all options available for integration with PeopleSoft.
E.6	Describe your solution's ability to provide and search our campus directory.
E.7	Does your solution have the capability to support a curated interactive, multi-stop mobile walking tour, with the added ability for URI staff to easily author a mobile tour without requiring technical skills? If so, please describe.
E.8	Please describe the platform's integration abilities with the following 3rd party software (e.g., full integration, integration via API, link, etc.): • YouVisit – Virtual Tour • CBORD – Dining Services • Localist – Events • Slate – Admissions • Starfish – Academic Success • Handshake – Jobs/Internships • Campus Labs – Student Success • CampusBird – Maps, Virtual Tours • EMS – Facility Reservations • IMLeagues – Intramural Sports & Group exercise registration/sign in
E.9	Can push notifications form any of the above 3rd party software be integrated into your platform? If so, please describe each.
E.10	If any of the above 3rd party software is integrated within your platform, and data is created using the app (e.g., voting within CampusLabs), how is that data returned to the 3rd party system?
E.11	The app must include the real-time shuttle location map data: https://uri.transloc.com/. Describe how your solution would accomplish this.
E.12	Can your solution be used to reserve or view availability of campus resources (e.g., library study rooms, labs, etc.)? If so, please describe.
E.13	Can your solution integrate internally developed apps, such as the URI Roommate database (https://commuters.apps.uri.edu/roommate_database/)? If so, please describe.
E.14	Can your solution include a stream of WRIU https://www.wriu.org/ and/or the student station http://riu2.org/? If so, please describe.
E.15	Describe your ability to include videos and live streaming from our campus newspaper, The Good Five Cent Cigar (https://rhodycigar.com/newscast/)
E.16	Students have requested the ability to add money to their Ram Account and have the funds available immediately. Describe how the connection to https://www.ri.gov/URI/ramacct/ would work, and whether an additional login would be necessary.
E.17	Students have requested the ability to make an appointment with Health Services. Describe how the connection to https://uri.medicatconnect.com/login.aspx would work, and whether an additional login would be necessary.
E.18	Does your solution have the capability to allow students to register for events, buy tickets or pay club dues? If so, is the payment system PCI compliant? Please describe.
E.19	Does your solution integrate with any payment gateways? If so, please describe.
E.20	Does your solution integrate with any student ID card providers? If so, please describe.

F. Platform Management

Req. Nbr	Description
F.1	The system shall provide an app assembly and publishing tool for business or non-technical users. This tool should make it very easy to combine multiple modules, new content and media, and responsive web pages into a complete app experience. Publishing and updating the application should be possible at any time, in real time, without returning to the app store.
F.2	The system shall provide an administration console that allows both IT personnel and non-technical users on campus to add to the mobile solution. Does your solution provide the ability to customize the core modules? If so, please describe.
F.3	The solution must allow for campus branding in accordance with the branding standards and approval set by URI's Communication and Marketing Department, including logos, word marks, colors and fonts. Please explain how this is done.
F.4	The solution must offer a large variety of user interface styles. Please include screen style options (including ones branded with the University of Rhode Island colors and theme if possible). Also include examples of other customer apps, and the unique branding, styles, looks, and user interface systems that can be implemented. Include examples of phone, tablet, and desktop (HTML5) content.
F.5	The solution must enable non-technical users to modify the app's style and colors without the need to understand CSS or HTML. Please explain how this is done.
F.6	The system must allow dynamic and portable edits to the core modules (e.g., the headers or footers). Such edits should be able to include: links to other modules or responsive web pages, video, text, phone numbers. These edits must be available to non-technical administrators, so that modifications to the system can be produced at will by the URI staff, for immediate availability on all channels. Please explain how this is done.
F.7	Can your solution automatically generate themes based on user input of a selection of colors? If so, please explain.
F.8	The system shall support multi-campus and/or multi-persona versions of the mobile app. This feature must be configurable through an administration console and not require custom implementation. The administrators must be able to create new campus locations or personas as needed. Describe how this is done.
F.9	The solution shall allow the ability to brand different campus locations and/or personas with a separate theme including a different logo, color, fonts spacing and font sizes for each campus. Each of these different campus locations and user interfaces must be easily available through a common mobile app, using the multi-site feature described above. Please explain how this is done.
F.10	Does your solution allow for decentralized ownership: multiple levels of administrative roles to be delegated, with permissions set to control access? If so, please describe.
F.11	Does your solution use separate user interfaces to support different access roles (e.g., staff, student, prospect, alumni/donors, administrators, etc.)? If so, please describe.

G. Security

Req. Nbr	Description
G.1	Since the app will display or update student specific data, it shall have secure authentication that interacts with campus authentication methods. The interaction between the device and the authentication mechanism shall be encrypted. Describe

	how authentication is implemented in your platform, including whether it supports SSO authentication with AD, LDAP, and/or SAML.
G.2	Can access and administration capabilities be based on user role or other attributes provided by authentication data sources, such as SAML attributes?
G.3	Can your solution use SAML attributes to dynamically generate personalized versions of the app screens and tiles based on the user's credentials? If so, please explain.
G.4	Does your solution support biometric authentication? If so, please describe
G.5	Is authentication optional to use the solution?
G.6	Is authentication using locally-generated accounts allowed?

H. Implementation Plan and Training

Req. Nbr	Description
H.1	The Vendor must provide a comprehensive project work plan, including an approximate timeline of implementation.
H.2	List recommended URI staffing resources needed during the implementation of your solution, showing roles, activities and hours of effort typically needed.
H.3	List recommended URI staffing resources needed for the operational lifetime of this solution, showing roles, activities and hours of effort typically needed.
H.4	Describe the training options you have available for both IT staff working within the system as well as any resources available for our non-technical administrators. How is the training delivered? Is there an additional cost for any training?

I. Miscellaneous

Req. Nbr	Description
I.1	Provide any additional information you feel may be relevant to your proposal or any other service that would be included.

SECTION 4: PROPOSAL

A. Technical Proposal

It is the intent of URI to award a contract to the respondent deemed to be the most qualified and responsible firm, who submits the best overall proposal based on an evaluation of all proposal responses. Selection shall be based on URI assessment of the respondent's ability to provide a vendor-hosted, full-featured, low-code rapid mobile application development platform and tools, as determined by the technical committee elected to evaluate proposals. The offeror should specifically address each of the following elements:

1. **Firm Experience and Qualifications (Section 3, Tables A&B) (10 Points):** The Firm's past performance working with higher education clients of similar size and complexity to URI on similar projects will be evaluated. Successful completion, timeliness and degree of customer satisfaction for each project will be taken into consideration. In evaluating the Firm's past performance, the University will consider references submitted by the Firm and may consider information for other sources. The vendor shall provide narrative statements for each table entry.

2. **Software Features and Technical Requirements (Section 3, Tables C,D,E,F,G,I) (45 Points):** The proposed software platform will be evaluated to determine the extent to which it meets both the functional and technical requirements set forth in Section 3 of this RFP. The proposal shall address each table entry with a narrative description of the features currently in the platform. Future development plans for features not yet available will not be considered as qualified for scoring.

3. **Implementation Plan and Training (Section 3, Table H) (15 Points):** The Firm's proposed project approach will be evaluated to determine how well it outlines the required tasks and provides a methodology for successfully accomplishing the project objectives, including implementation, training and support. The Firm's outline and description for evaluating the project objectives must include a high-level overview of the phases of implementation and approximate timelines based on prior implementation efforts. The vendor shall provide narrative statements for each table entry.

B. Cost Proposal

Provide a proposal cost proposal to include the following on the attached Appendix B Cost Proposal Form

1. Total and annual costs of a three-year proposal that addresses the base product and required features outlined in the Scope of Work section of this RFP as well as any related costs necessary to provide your solution (including but not limited to all hardware, software, setup, training, additional professional development classes, project management services, customer support, warranty, updates and maintenance).

2. Pricing for potential product/services mentioned in Section 3 of the RFP but not included above. Include any discounts available to the University.

3. The terms, conditions, and nature of the license and the renewal costs. Include how the cost model is calculated (e.g., total users, total apps, etc.), using an estimate of 15,000 undergraduate students.

C. ISBE Proposal

See Appendix A for information and the MBE, WBE, and/or Disability Business Enterprise Participation Plan form(s). Bidders are required to complete, sign and submit these forms with their overall proposal in a sealed envelope. Please complete separate forms for each MBE, WBE and/or Disability Business Enterprise subcontractor/supplier to be utilized on the solicitation.

SECTION 5: EVALUATION AND SELECTION

Proposals will be reviewed by a Technical Review Committee ("TEC") comprised of staff from URI/State Agencies. The TEC first shall consider technical proposals.

Technical proposals must receive a minimum of 60 (85.7%) out of a maximum of 70 points to advance to the cost evaluation phase. Any technical proposals scoring less than 60 points shall not have the accompanying cost or ISBE participation proposals opened and evaluated. The proposal will be dropped from further consideration.

Technical proposals scoring 60 points or higher will have the cost proposals evaluated and assigned up to a maximum of 30 points in cost category bringing the total potential evaluation score to 100 points. After total possible evaluation points are determined ISBE proposals shall be evaluated and assigned up to 6 bonus points for ISBE participation.

The University of Rhode Island reserves the right to select the vendor(s) or firm(s) ("vendor") that it deems to be most qualified to provide the goods and/or services as specified herein; and, conversely, reserves the right to cancel the solicitation in its entirety in its sole discretion.

Proposals shall be reviewed and scored based upon the following criteria:

Criteria	Possible Points
Firm Experience and Qualifications (Section 3, Tables A&B)	10 Points
Software Features and Technical Requirements (Section 3, Tables C,D,E,F,G,I)	45 Points
Implementation Plan and Training (Section 3, Table H)	15 Points
Total Possible Technical Points	**70 Points**
Cost proposal*	30 Points
Total Possible Evaluation Points	**100 Points**
ISBE Participation**	6 Bonus Points
Total Possible Points	**106 Points**

<u>* Cost Proposal Evaluation</u>:

The vendor with the lowest cost proposal shall receive one hundred percent (100%) of the available points for cost. All other vendors shall be awarded cost points based upon the following formula:

(lowest cost proposal / vendor's cost proposal) x available points

For example: If the vendor with the lowest cost proposal (Vendor A) bids $65,000 and Vendor B bids $100,000 for monthly costs and service fees and the total points available are thirty (30), Vendor B's cost points are calculated as follows:

$65,000 / $100,000 x 30= 19.5

<u>ISBE Participation Evaluation</u>**:

A. <u>Calculation of ISBE Participation Rate</u>

1. <u>ISBE Participation Rate for Non-ISBE Vendors</u>. The ISBE participation rate for non-ISBE vendors shall be expressed as a percentage and shall be calculated by dividing the amount of non-ISBE vendor's total contract price that will be subcontracted to ISBEs by the non-ISBE vendor's total contract price. For example if the non-ISBE's total contract price is $100,000.00 and it subcontracts a total of $12,000.00 to ISBEs, the non-ISBE's ISBE participation rate would be 12%.

2. <u>ISBE Participation Rate for ISBE Vendors</u>. The ISBE participation rate for ISBE vendors shall be expressed as a percentage and shall be calculated by dividing the amount of the ISBE vendor's total contract price that will be subcontracted to ISBEs and the amount that will be self-performed by the ISBE vendor by the ISBE vendor's total contract price. For example if the ISBE vendor's total contract price is $100,000.00 and it subcontracts a total of $12,000.00 to ISBEs and will perform a total of $8,000.00 of the work itself , the ISBE vendor's ISBE participation rate would be 20%.

B. <u>Points for ISBE Participation Rate</u>:

The vendor with the highest ISBE participation rate shall receive the maximum ISBE participation points. All other vendors shall receive ISBE participation points by applying the following formula:

(Vendor's ISBE participation rate ÷ Highest ISBE participation rate

X Maximum ISBE participation points)

For example, assuming the weight given by the RFP to ISBE participation is 6 points, if Vendor A has the highest ISBE participation rate at 20% and Vendor B's ISBE participation rate is 12%, Vendor A will receive the maximum 6 points and Vendor B will receive (12% ÷ 20%) x 6 which equals 3.6 points.

<u>General Evaluation</u>:

Points shall be assigned based on the vendor's clear demonstration of the ability to provide the requested goods and/or services. Vendors may be required to submit additional written information or be asked to make an oral presentation before the Technical Review Committee to clarify statements made in the proposal.

SECTION 6: QUESTIONS

Questions concerning this solicitation may be e-mailed to the University of Rhode Island Purchasing Department at URIPurchasing@uri.edu no later than the time and date indicated on page 1 of this solicitation. Please reference the reference **RFP # 100859** on all correspondence. Questions should be submitted in a Microsoft Word attachment in a narrative format with no tables. Answers to questions received, if any, shall be posted on the Division of Purchases' website as an addendum to this solicitation. It is the responsibility of all interested parties to monitor the Division of Purchases website for any procurement related postings such as addenda. If technical assistance is required, call the Help Desk at (401) 574-8100.

SECTION 7: PROPOSAL CONTENTS

A. Proposals shall include the following:

1. **Bid/Proposal Cover Page**, completed and signed, in ink (first page of RFP document)
2. One completed and signed **URI Bidder Certification Form** (include in the Technical Proposal original copy only). *Do not include in copies of the Technical or Cost proposal.*

3. ✉ **Technical Proposal** - describing the qualifications and background of the applicant and experience with and for similar projects, and all information described earlier in this solicitation. The technical proposal is limited to one hundred (100) pages (this excludes any appendices and as appropriate, resumes of key staff that will provide services covered by this request).

    a. One (1) Electronic copy on a CD-R, marked "Technical Proposal - Original".

    b. One (1) printed paper copy, marked "Technical Proposal -Original" and signed.

    c. Six (6) printed paper copies

4. ✉ **Cost Proposal** - A separate, signed and sealed cost proposal reflecting the hourly rate, or other fee structure, proposed to complete all of the requirements of this project. *Do not include any copies in the Technical proposals.*

    a. One (1) Electronic copy on a CD-R, marked "Cost Proposal -Original".

    b. One (1) printed paper copy, marked "Cost Proposal -Original" and signed.

    c. One (1) printed paper copy

5. ✉ **ISBE Proposal** - Two (2) completed original and copy versions, signed and sealed Appendix A. MBE, WBE, and/or Disability Business Enterprise Participation Plan. Please complete separate forms for each MBE/WBE or Disability Business Enterprise subcontractor/supplier to be utilized on the solicitation. *Do not include any copies in the Technical proposals.*

6. ✉**Higher Education Cloud Vendor Assessment Tool (HECVAT)** –

    a. One (1) Electronic copy on a CD-R, marked “HECVAT”

    b. One (1) printed paper copy

7. ✉**IT Security Services Security Checklist for Mobile Apps** –

    a. One (1) Electronic copy on a CD-R, marked “Security Checklist”

    b. One (1) printed paper copy

B. Formatting of proposal response contents should consist of the following:

1. Formatting of CD-Rs – Separate CD-Rs are required for the technical proposal and cost proposal. All CD-Rs submitted must be labeled with:

    a. Vendor’s name

    b. RFP #

    c. RFP Title

    d. Proposal type (e.g., technical proposal or cost proposal)

    e. If file sizes require more than one CD-R, multiple CD-Rs are acceptable. Each CD-R must include the above labeling and additional labeling of how many CD-Rs should be accounted for (e.g., 3 CD-Rs are submitted for a technical proposal and each CD-R should have additional label of ‘1 of 3’ on first CD-R, ‘2 of 3’ on second CD-R, ‘3 of 3’ on third CD-R).

    Vendors are responsible for testing their CD-Rs before submission as the URI Purchasing Department’s inability to open or read a CD-R may be grounds for rejection of a Vendor’s proposal. All files should be readable and readily accessible on the CD-Rs submitted with no instructions to download files from any external resource(s). If a file is partial, corrupt or unreadable, the URI Purchasing Department may consider it “non-responsive”. USB Drives or any other electronic media shall not be accepted. Please note that CD-Rs submitted, shall not be returned.

2. Formatting of written documents and printed copies:

a. For clarity, the technical proposal shall be typed. These documents shall be single-spaced with 1" margins on white 8.5"x 11" paper using a font of 12 point Calibri or 12 point Times New Roman.

b. All pages on the technical proposal are to be sequentially numbered in the footer, starting with number 1 on the first page of the narrative (this does not include the cover page or table of contents) through to the end, including all forms and attachments. The Vendor's name should appear on every page, including attachments. Each attachment should be referenced appropriately within the proposal section and the attachment title should reference the proposal section it is applicable to.

c. The cost proposal shall be typed using the template referenced in section 4.

d. Printed copies are to be only bound with removable binder clips.

SECTION 8: PROPOSAL SUBMISSION

Interested vendors must submit proposals to provide the goods and/or services covered by this RFP on or before the date and time listed on the cover page of this solicitation. Responses received after this date and time, as registered by the official time clock in the reception area of the University of Rhode Island Purchasing Department, shall not be accepted.

Responses should be mailed or hand-delivered in a sealed envelope marked "RFP # 100859 to

MAIL TO:

UNIVERSITY OF RHODE ISLAND
PO BOX 1773
PURCHASING DEPARTMENT
KINGSTON, RI 02881

COURIER:

UNIVERSITY OF RHODE ISLAND
PURCHASING DEPARTMENT
10 TOOTELL RD.
KINGSTON, RI 02881-2010

NOTE: Proposals received after the above-referenced due date and time will not be considered. Proposals misdirected to other University locations or which are otherwise not presented in the URI Purchasing Department by the scheduled due date and time will be determined to be late and will not be considered. Proposals faxed, or emailed, to the URI Purchasing Department will not be considered. The "official" time clock is located in the reception area of the URI Purchasing Department. **(Please be advised that FedEx/UPS do not always arrive by 10:30 am, you would be smart to send your submission to arrive at least one day early)**

SECTION 9: CONCLUDING STATEMENTS

Notwithstanding the above, the University of Rhode Island reserves the right to award on the basis of cost alone, to accept or reject any or all proposals, and to award it in its best interest.

Proposals found to be technically or substantially non-responsive at any point in the evaluation process will be rejected and not considered further.

The University may, at its sole option, elect to require presentation(s) by offerors clearly in consideration for award

If a Vendor is selected for an award, no work is to commence until a purchase order is issued by the University of Rhode Island Purchasing Department.

APPENDIX A. PROPOSER ISBE RESPONSIBILITIES AND MBE, WBE, AND/OR DISABILITY BUSINESS ENTERPRISE PARTICIPATION FORM

A. Proposer's ISBE Responsibilities (from 150-RICR-90-10-1.7.E)

1. Proposal of ISBE Participation Rate. Unless otherwise indicated in the RFP, a Proposer must submit its proposed ISBE Participation Rate in a sealed envelope or via sealed electronic submission at the time it submits its proposed total contract price. The Proposer shall be responsible for completing and submitting all standard forms adopted pursuant to 105-RICR-90-10-1.9 and submitting all substantiating documentation as reasonably requested by either the Using Agency's MBE/WBE Coordinator, Division, ODEO, or Governor's Commission on Disabilities including but not limited to the names and contact information of all proposed subcontractors and the dollar amounts that correspond with each proposed subcontract.

2. Failure to Submit ISBE Participation Rate. Any Proposer that fails to submit a proposed ISBE Participation Rate or any requested substantiating documentation in a timely manner shall receive zero (0) ISBE participation points.

3. Execution of Proposed ISBE Participation Rate. Proposers shall be evaluated and scored based on the amounts and rates submitted in their proposals. If awarded the contract, Proposers shall be required to achieve their proposed ISBE Participation Rates. During the life of the contract, the Proposer shall be responsible for submitting all substantiating documentation as reasonably requested by the Using Agency's MBE/WBE Coordinator, Division, ODEO, or Governor's Commission on Disabilities including but not limited to copies of purchase orders, subcontracts, and cancelled checks.

4. Change Orders. If during the life of the contract, a change order is issued by the Division, the Proposer shall notify the ODEO of the change as soon as reasonably possible. Proposers are required to achieve their proposed ISBE Participation Rates on any change order amounts.
5. Notice of Change to Proposed ISBE Participation Rate. If during the life of the contract, the Proposer becomes aware that it will be unable to achieve its proposed ISBE Participation Rate, it must notify the Division and ODEO as soon as reasonably possible. The Division, in consultation with ODEO and Governor's Commission on Disabilities, and the Proposer may agree to a modified ISBE Participation Rate provided that the change in circumstances was beyond the control of the Proposer or the direct result of an unanticipated reduction in the overall total project cost.

B. MBE, WBE, AND/OR Disability Business Enterprise Participation Plan Form:

Attached is the MBE, WBE, and/or Disability Business Enterprise Participation Plan form. Bidders are required to complete, sign and submit with their overall proposal in a sealed envelope. Please complete separate forms for each MBE, WBE and/or Disability Business Enterprise subcontractor/supplier to be utilized on the solicitation.

STATE OF RHODE ISLAND AND PROVIDENCE PLANTATIONS
DEPARTMENT OF ADMINISTRATION
ONE CAPITOL HILL PROVIDENCE,
RHODE ISLAND 02908

MBE, WBE, and/or DISABILITY BUSINESS ENTERPRISE PARTICIPATION PLAN

Bidder's Name:
Bidder's Address:
Point of Contact:
Telephone:
Email:
Solicitation No.:
Project Name:

This form is intended to capture commitments between the prime contractor/vendor and MBE/WBE and/or Disability Business Enterprise subcontractors and suppliers, including a description of the work to be performed and the percentage of the work as submitted to the prime contractor/vendor. Please note that all MBE/WBE subcontractors/suppliers must be certified by the Office of Diversity, Equity and Opportunity MBE Compliance Office and all Disability Business Enterprises must be certified by the Governor's Commission on Disabilities at time of bid, and that MBE/WBE and Disability Business Enterprise subcontractors must self-perform 100% of the work or subcontract to another RI certified MBE in order to receive participation credit. Vendors may count 60% of expenditures for materials and supplies obtained from an MBE certified as a regular dealer/supplier, and 100% of such expenditures obtained from an MBE certified as a manufacturer. This form must be completed in its entirety and submitted at time of bid. **Please complete <u>separate forms</u> for each MBE/WBE or Disability Business Enterprise subcontractor/supplier to be utilized on the solicitation.**

Name of Subcontractor/Supplier:					
Type of RI Certification:	□ MBE □ WBE □ Disability Business Enterprise				
Address:					
Point of Contact:					
Telephone:					
Email:					
Detailed Description of Work To Be Performed by Subcontractor or Materials to be Supplied by Supplier:					
Total Contract Value ($):		Subcontract Value ($):		ISBE Participation Rate (%):	
Anticipated Date of Performance:					

I certify under penalty of perjury that the forgoing statements are true and correct.

Prime Contractor/Vendor Signature	**Title**	**Date**
Subcontractor/Supplier Signature	**Title**	**Date**

Appendix B – Cost Proposal

Item	**Cost**
Base Annual Cost	
Any One-Time Costs *(please itemize)*	
Usage Analytics	
Admin Training (Assume 4 administrators)	
Any Other Costs *(please itemize)*	
Total Year 1 Cost	
Annual Year 2 Cost	
Annual Year 3 Cost	
Any Other Costs *(please itemize)*	
Total Cost	

THE UNIVERSITY OF RHODE ISLAND

OFFICE OF INFORMATION SECURITY

IT SECURITY SERVICES

SECURITY CHECKLIST FOR MOBILE APPS

VERSION HISTORY

Version #	Date	Author	Key Differences
1.0	11/14/2019	Mike Khalfayan	

SECURITY CHECKLIST FOR MOBILE APPS

Table 1: Security Checklist for Mobile App Developers

Description	OS	Type A	Type B
Authentication and Access Control			
□ User authentication must support adequate authentication strength.	All	Required	Required
□ Immutable device identifiers, such as unique device ID (UDID) and International Mobile Station Equipment Identity (IMEI), must not be used as credentials.	All	Required	Required
□ The apps shall mutually authenticate the user and the server.	All	Required	Required
□ The client and server shall properly validate Transport Layer Security (TLS) or similar certificates.	All	Required	Required
□ Apps shall counter bidding-down attacks, including TLS stripping.	All	Required	Required
□ The app shall implement certificate pinning.	All	Required	Recommended
Data Protection			
□ Secret keys and/or passwords must not be hard-coded in the app.	All	Required	Required
□ Encryption keys shall be derived from dynamically set values, such as the user passcode.	All	Required	Required
□ App-level encryption for data at rest shall be used.	All	Required	Required
□ Encryption for data in motion shall be used.	All	Required	Required
□ Sensitive data, including authentication credentials, shall be encrypted, even when stored in the keychain.	All	Required	Recommended

Description		OS	Type A	Type B
□	The mobile app shall prevent sensitive data from leaking via the autosnapshot feature of iOS and similar mechanisms.	All	Required	Recommended
□	The mobile app shall not allow storage, sharing or pasting of sensitive data onto removable or shared media and external resources.	All	Required	Recommended
□	The app shall not enable autocomplete for sensitive text input fields.	All	Required	Required
□	Cached data (e.g., HTTP, camera images and GUI objects) shall be minimized and deleted after exiting the app.	All	Required	Required
□	Sensitive data shall not be stored in the SQLite database on the device; if it’s unavoidable, a tool shall be used to encrypt the database.	All	Required	Recommended
□	The data logged via the keyboard shall not contain credentials, financial information or other sensitive data.	All	Required	Required
□	The strength of cryptography and key lengths shall be in accordance with FIPS 140-2-approved security functions.	All	Required	Recommended
□	The apps shall leverage trusted environments (such as TEE), where available.	All	Recommended	Recommended
Session Management				
□	The session timeout shall be of a reasonable value and configurable.	All	Required	Required
□	Session data shall be deleted when a session is aborted or terminated unexpectedly.	All	Required	Required
□	GET commands shall not be used for querying sensitive data; POST commands should be preferred over HTTPS.	All	Required	Required

Description		OS	Type A	Type B
Error Handling and Logging				
□	The app shall not log sensitive data on the system log or file system.	All	Required	Required
□	The crash and debug logs shall not contain sensitive data.	All	Required	Required
Permissions				
□	Permissions and resources granted to apps (i.e., AndroidManifest.xml, iOS entitlements) shall be limited to what the app needs to operate. (If third-party code is reused, this is valid for the third-party code as well.)	All	Required	Required
Tampering Protection				
□	Method swizzling shall not be adopted. (In rare exceptions, when swizzling needs to be used, thorough security testing against exploits must be provided and documented.)	All	Required	Recommended
□	Third-party libraries used shall be validated (via testing or other means) as free from vulnerabilities and malicious code.	All	Required	Required
□	Apps shall use server-side checks and shall not rely on client-side checks for functions that can be manipulated to steal information or compromise the app.	All	Required	Required
□	The app shall minimize communication with other apps and take appropriate measures when doing so.	All	Required	Required
□	Immutable structures that cannot be overwritten when not in use shall be avoided for sensitive data, and mutable structures shall be preferred.	All	Required	Recommended

Description		OS	Type A	Type B
□	The app shall not support implicit intents for Android.	Android	Required	Recommended
□	The app shall use address space layout randomization (ASLR), where available.	All	Required	Required
□	The app shall validate all input.	All	Required	Required
□	The app shall have the necessary measures in place to avoid race conditions.	All	Required	Required
□	The app shall be able to detect privilege escalation conditions, including jailbreak/rooting and unlocked bootloaders.	All	Required	Optional
□	The app shall perform checks for indicators of compromise.	Android	Recommended	Optional
□	The app code shall be obfuscated.	All	Required	Recommended
Life Cycle				
□	All test data shall be removed from the app container (.ipa, .apk, etc.).	All	Required	Required
□	No debugging flags shall be set in the finalized app.	All	Required	Required
□	The app shall go through application security testing.	All	Required	Required

This security checklist should be used as guidance for developers of the security precautions that are necessary to take in the mobile apps they produce.

The security checklist is divided into seven specific domains:

- Authentication and Access Control
- Data Protection
- Session Management
- Error Handling and Logging
- Permissions
- Tampering Protection

- Life Cycle

Each domain contains a set of requirements and recommendations. Certain requirements are generic, and some are specific to the OS or programming language used.

The checklist provides differentiates between requirements for **Type A** and **Type B** apps. **Type A** are higher-security requirement apps, while **Type B** require less-stringent security. In the columns for **Type A** and **Type B** in the checklist, there are suggested checks for requirements that are mandatory, recommended and optional.

The checklist does not aim to be a comprehensive list of security requirements. Rather, it focuses on peculiarities of mobile application security, as well as common security mistakes that developers make. The goal of following the checklist is to avoid major pitfalls when coding mobile apps. The Rationale section below provides background and rationale for each of the items included in the checklist.

RATIONALE

Authentication and Access Control

User Authentication Must Support Adequate Authentication Strength

This is a generic requirement, and what is considered adequate will depend on the context and regulatory environment. Gartner recommends six-character alphanumeric passcodes for enterprise apps, because they provide sufficient protection against brute-force attacks. In iOS, for example, a six-character alphanumeric passcode will require 1.7 years of brute-force cracking time, whereas a four-digit PIN can be guessed in 40 minutes.[1],[2]

However, many banking apps, for example, offer four-digit PIN codes, and many support biometric authentication on newer devices. Gartner considers fingerprint-based user authentication to be stronger than four-digit passcodes, but no stronger than six-character alphanumeric passcodes. In this context, organizations decide to absorb residual risk in the product. In those cases, a best practice is to strongly associate the device with the mobile application. This practice is called device binding. There are various ways to perform device binding, typically involving the use of device identifiers to associate the device.

Immutable Device Identifiers, Such as Unique Device ID (UDID) and International Mobile Station Equipment Identity (IMEI), Must Not Be Used as Credentials

Although using unique device identifiers (UDIDs) to perform device binding is a best practice, it has been a common pitfall with mobile applications to use device identifiers as security credentials.[3] Identifiers are not considered secret and, as such, they cannot serve as passcodes or authentication credentials. Increasingly, iOS and Android make it harder to leverage these
identifiers, as well as provide alternative methods that allow identifiers for the application to use to be derived.

The Apps Shall Mutually Authenticate the User and the Server

App authentication is usually understood as the need for the mobile client to authenticate itself to the server. However, it is a common attack to tweak and republish apps, redirecting the authentication to a malicious rogue server (a command and control center). Therefore, to avoid rogue server attacks, the server must also authenticate itself to the mobile client.

The Client and Server Shall Properly Validate Transport Layer Security (TLS) or Similar Certificates

This specific recommendation assumes the app is leveraging Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or another protocol. Throughout this research, we assume TLS or SSL is being used as the security transport protocol. Other protocols can be used as well, provided there is a security protocol. Whatever the protocol of choice, certificates must be validated. It is a common mistake not to validate the TLS certificates allowing man-in-the-middle attacks. (We refer to TLS, rather than the older SSL in all this research.)

By validating the certificate, the mobile client verifies that the origin of the credential is legitimate. Usually, TLS certificate validation consists of validating the signature of the certificate.

The App Shall Implement Certificate Pinning

Pinning a certificate consists in only accepting a specific certificate, instead of verifying the general validity of the certificate. Traditional validation is still appropriate in certain situations, such as where interaction with a wide range of servers takes place (see the requirement on TLS certificate validation above).

Certificate pinning is used to prevent man-in-the-middle attacks and fraudulent certificates and can be particularly useful for in-house-developed applications, where the identity of the server is already established and known.

Data Protection

Secret Keys and/or Passwords Must Not Be Hard-Coded in the App

This mistake is one of the most frequent in mobile application development. Secret keys, passwords, passcodes and credentials that are hard-coded in the app are can be easily stolen by attackers who download the app and reverse-engineer it. There are several alternatives to hardcoding passwords. One example is to enroll and deploy certificates that can serve as material for authentication.

Encryption Keys Shall Be Derived From Dynamically Set Values, Such as the User Passcode

To avoid hard-coding of credentials, such as secret keys, they should be derived from dynamically set values. One easy way to do this is by leveraging the user passcode, if one is used to authenticate to the app. A simple passcode will weaken the encryption key, so that the key material used should encompass other values that are independent of the key.

App-Level Encryption for Data at Rest Shall Be Used

Data at rest should be confidentiality protected. Mobile devices provide device-level encryption. Application-level encryption is provided natively by the OS or offered by the application. Entities with very high security requirements (typically verticals such as government, defense, and, depending on the context, healthcare, finance and insurance) may opt to use stand-alone encryption, while most other apps can use native mechanisms.

When using OS-native encryption mechanisms to encrypt application data, it is essential to ensure that the appropriate protection class is used. For example, when using iOS default encryption, NSFileProtectionComplete should be used. This class will keep the files encrypted when the device is locked, in case of theft or loss. In this case, the strength of encryption depends, in part, on the complexity of the device passcode. Therefore, developers should keep in mind that a weak passcode will lead to weak protection. In consumer-facing apps, the publisher of the app has no control over the strength of the passcode. However, in business-to-employee (B2E) contexts, an organization can enforce this via policy, with a requirement for passcodes of adequate complexity (Gartner recommends six-character alphanumeric passcodes).

Encryption for Data in Motion Should Be Used

Most mobile apps employ TLS as a transport security protocol, which provides encryption for data in motion. In most cases, this is sufficient as a measure for protecting data in motion. Customized solutions may use proprietary methods of encrypting data in motion through encrypted tunnels or other mechanisms. Details can be found in the “Market Guide for Secure Enterprise Data Communications.”

Sensitive Data, Including Authentication Credentials, Shall Be Encrypted, Even When Stored in the Keychain

What is considered sensitive data depends on the context and the specific regulatory environment. A fundamental part of the exercise of developing a secure app will be to identify the sensitive data. That data will have to be encrypted and handled with additional care (for example, it should not be possible to export that data, as discussed in other items on the checklist).

In iOS and Android, there are keychain mechanisms, which are secure storage spaces to store credentials (such as passcodes, secret keys and certificates). In the keychain, several levels of security can be imposed natively. For example, in iOS, the setting kSecAttrAccessibleAlways allows data in the keychain to always be accessed, whereas kSecAttrAccessibleWhenUnlocked allows data in the keychain to be accessed only while the device is unlocked by the user. These settings should be selected with care and should have the maximum security possible.

However, even when these settings are set appropriately, credentials can and should be protected for high-security applications. For example, the keybag in iOS devices stores keys used to protect keychain items.

An alternative to native platform resources to protect credentials is whiteboxing (or white-box cryptography). This method consists of techniques that hide and protect sensitive application data in its own code. (See the “Market Guide for Application Shielding” for more details, as well as a list of providers.)

The Mobile App Shall Prevent Sensitive Data From Leaking via the Autosnapshot Feature of iOS and Similar Mechanisms

To facilitate multitasking, iOS provides snapshots of apps. This allows users to view the app screen without accessing the app itself. It can be convenient when deciding which app to select and use next, but it can lead to data leakage. There is a way to obfuscate the app screen and only show the name of the application. Apps that contain sensitive data should follow this approach.

A similar feature, an overview screen, is available on Android devices; however, we have not determined whether it is possible to similarly obfuscate the screenshot.

The Mobile App Shall Not Allow Storage, Sharing or Pasting of Sensitive Data Onto Removable or Shared Media and External Resources

This recommendation will depend on the specific use case. Unless strictly necessary, it should not be possible to leverage external media that cannot be controlled and monitored. Where this can’t be avoided, the data should be stored in an encrypted form.

The App Shall Not Enable Autocomplete for Sensitive Text Input Fields Autocomplete for sensitive text input, such as passcodes, would lead to that sensitive data being cached and prompted as choices when the user attempts to log in. This is a common pitfall with web and mobile applications and should be avoided.

Cached Data (e.g., HTTP, Camera Images and GUI Objects) Shall Be Minimized and Deleted After Exiting the App

Especially for hybrid and mobile web apps, a major problem is how to protect cached content. There are some inbuilt ways, but the security of the method selected will typically depend on whether the user has set a complex-enough passcode on the device. It is, therefore, recommended to minimize stored data, avoid caching sensitive data and delete the data once it is no longer being used.

Sensitive Data Shall Not Be Stored in the SQLite Database on the Device; If It's Unavoidable, a Tool Shall Be Used to Encrypt the Database

Cached data should be avoided (see previous entry). However, there are use cases and applications where this is unavoidable. The best option in those cases is storing data in SQLite and encrypting it. A tool commonly used in these cases is SQLCipher.

The Data Logged via the Keyboard Shall Not Contain Credentials, Financial Information or Other Sensitive Data

The iOS keyboard caches entries provided by users. This is done to assist with autocompletion and correction functionality. However, sensitive data is exposed to risks when cached on the device, beyond the application back end's control. Gartner recommends disable caching when sensitive data, such as credentials or financial information, is entered.

Android is similar, providing a user dictionary in which words and terms entered are logged. To disable caching, a custom keyboard can be implemented. For select devices when high security is required, the trusted user interface available in the trusted execution environment could be leveraged.[4]

The Strength of Cryptography and Key Lengths Shall Be in Accordance With FIPS 140-2-Approved Security Functions

FIPS 140-2-certified encryption is a regulatory requirement in specific industries and countries. However, it is a good practice to follow the so-called “approved security functions” in FIPS 140-2.[5] This is because security algorithms become outdated with time. Computational power becomes strong enough to break certain shorter-keyed algorithms, and researchers sometimes uncover vulnerabilities that make algorithms breakable (see “Better Safe Than Sorry: Preparing for Crypto-Agility”).

The Apps Shall Leverage Trusted Environments (Such as TEE), Where Available

iOS and Android platforms have been opening up functionality to developers to leverage the hardware-based roots of trust on the device (see “Innovation Insight for Trusted Execution Environments”).

Session Management

The Session Timeout Shall Be of a Reasonable Value and Configurable

This is a generic requirement that will depend on the context. (For details on how to set timeouts, see “Setting PC and Smartphone Timeouts Is a Blunt Instrument for Mitigating Risks, but an Essential One.”)

Session Data Shall Be Deleted When a Session Is Aborted or Terminated Unexpectedly

Abnormal termination of an application operation may leave data cached. Therefore, in case of a crash or an unexpected termination of the application, it should be foreseen that all session data is deleted, even if the app is built to not store any sensitive data in the first place.

GET Commands Shall Not Be Used for Querying Sensitive Data; POST Commands Should Be Preferred Over HTTPS

When dealing with web code, it is safer to use POST requests, rather than GET requests, to query sensitive data. Even when TLS is employed, GET requests can be logged unprotected in locations beyond the application's control, such as the browser history.

Error Handling and Logging

The App Shall Not Log Sensitive Data on the System Log or File System

Data such as passcodes, passwords and other credentials, as well as private information such as identifiers, names, phone numbers and payment information, must not be logged. This prevents attackers that may try to manipulate the app to recover this information.

The Crash and Debug Logs Shall Not Contain Sensitive Data

Logged data stored during crashes is typically sent to the server or stored in the app, and is used to discover bugs in the app. This data shall not contain sensitive data, such as passcodes, passwords and other credentials, as well as private information such as identifiers, names, phone numbers and payment information.

Permissions

Permissions and Resources Granted to Apps (i.e., AndroidManifest.xml, iOS Entitlements) Shall Be Limited to What the App Needs to Operate (If Third-Party Code Is Reused, This Is Valid for the Third-Party Code as Well)

It is often the case that apps request more privileges and access to information than they really require to operate. This makes the app a target for attackers that may try to exploit the application’s permissions to obtain access to the user’s private information. Apps sometimes run with more privileges than needed because developers reuse existing libraries in their apps. These libraries often request certain permissions by default.

Developers shall ensure that their code and the external libraries they leverage do not request unnecessary permissions.

As a concrete example, in Android, MODE_WORLD_WRITEABLE and MODE_WORLD_READABLE modes allow access to any applications, as well as any data format. This could lead to malicious

applications accessing sensitive data. Therefore, Android apps shall not create files with permissions of MODE_WORLD_READABLE or MODE_WORLD_WRITABLE.

Tampering Protection

Method Swizzling Shall Not Be Adopted (in Rare Exceptions, When Swizzling Needs to Be Used, Thorough Security Testing Against Exploits Must Be Provided and Documented)

Method swizzling is a technique that certain developers use in iOS Objective-C and Swift apps (and, to a lesser extent, in Android Java apps). Swizzling is not inherently malicious, and can provide certain performance benefits; however, if used improperly, it could cause security issues. Swizzling with iOS apps consists of dynamically redirecting method invocations. This dynamicity makes it possible for an attacker to redirect to a malicious method, rather than the intended one.

Third-Party Libraries Used Shall Be Tested and Validated as Free From Vulnerabilities and Malicious Code

Developers tend to use third-party libraries that can support the functionality they want to have in the application. These third-party libraries are often the main source of vulnerabilities for applications, either because they have not been written properly, or they hold an excessive number of permissions. Only reputable APIs shall be used, and they shall be validated before use to verify they are not malicious and do not introduce any vulnerabilities.

Apps Shall Use Server-Side Checks and Shall Not Rely on Client-Side Checks for Functions That Can Be Manipulated to Steal Information or Compromise the App

If checks such as verifying a user identity or the integrity of the application are left to the client residing on the mobile app, then there is a risk that the attacker may compromise the client and bypass those controls. Server-side checks require that the client provides proof to the server, which validates the controls; therefore, an attacker cannon bypass them.

The App Shall Minimize Communication With Other Apps and Take Appropriate Measures When Doing So

Apps that are written to freely share data with third-party apps can be a source of leakage, as they can be exploited by attackers. Therefore, if apps are not meant to share data, they should be locked down. For example, in Android, an app that does not share data should report android:exported="false" in the application manifest.

If apps are meant to share data with other apps, precautions should be taken. In the same Android example, if sharing between corporate apps is employed, android:protectionLevel "signature" should be selected, so that the system checks that both apps are signed with the same certificate.

Immutable Structures That Cannot Be Overwritten When Not Used Shall Be Avoided for Sensitive Data, and Mutable Structures Shall Be Preferred

Immutable objects can only be written once and cannot be erased. This is not only inconvenient, but can be dangerous when dealing with sensitive data.

The App Shall Not Support Implicit Intents for Android

An intent in Android programming is a description of an action that an app can perform. There are two possible ways to resolve an intent: explicit and implicit. Implicit intents do not specify the target component (for example, the application recipient of the data) in an explicit manner. In such a case, to identify the recipient Android compares the content of the intent to potential recipient components, thanks to component filters.

Since Android 5.0, the Android platform has been eliminating the option for an implicit intent,[6] because a malicious application could impersonate itself as one able to receive and handle the data from an implicit intent. Information shall be sent only with explicit intents to other components of the Android system.

The App Shall Use Address Space Layout Randomization (ASLR), Where Available

Address space layout randomization (ASLR) is a feature supported on most modern mobile devices. It adds entropy to the way an app is memorized on a device. This randomness makes it harder for an attacker to exploit the app.

The App Shall Validate All Input Received

Input validation consists of verifying that data input in the app is in the expected format and length. This avoids many of the most common attack techniques, such as buffer overflows. These techniques try to take advantage of the lack of input validation to send unforeseen input that can carry out unwanted actions.

In the specific case of an iOS app that has registered a URL scheme, it shall validate the input received from the URL. It should only be able to receive specific input, to avoid directory traversals, buffer overflows and other similar attacks.

The App Shall Have the Necessary Measures in Place to Avoid Race Conditions

Race conditions arise in situations in which a control on a specific condition is conducted to lead to the app taking an action. A typical control can be verifying that the user is authorized to request a specific file or specific information before fetching it. Race conditions occur when the control is performed on one app or one user, but the resource is accessed by a different app or user. An attacker can exploit this to access resources without authorization.

Where the intended resource is shared, race conditions do not solely depend on the specific app. However, there are some precautions that developers can take to minimize risks of race conditions.

Precautions depend on the specific context. When dealing with temporary files that can be overwritten, a typical precaution is to ensure that a temporary file with the same name exists. Another typical action is resource locking for the duration of the intended operation.

The App Shall Be Able to Detect Privilege Escalation Conditions, Including Jailbreak/Rooting and Unlocked Bootloaders

This is a requirement for Type A apps and a recommendation for Type B apps. These sorts of checks are habitually delegated to enterprise mobility management (EMM) tools on workforce devices, while they are employed by the app itself in consumer-facing apps.

These are checks that are performed before or during app operation and come in the form of libraries. The most common form of check is detection of Android rooting or iOS jailbreak. Among the various techniques used to detect this practice is looking for the presence of Cydia on the device (a popular app for jailbroken iOS devices). Another control can be that the app is not running in a debugger.

Controls of this nature may be considered privacy-invasive, because they investigate outside the boundaries of the application. The terms of agreement of the application (or the mobile policy, for enterprise apps) should reflect this and inform the user.

The way to handle these checks will depend on the context. Aborting the app may be acceptable in high-security B2E situations, but customer-facing apps should use this information to categorize the user in terms of risk, rather than denying service.

The App Shall Perform Checks for Indicators of Compromise

Mobile platforms have been providing developers with tools to perform checks of the status of a device, beyond simply checking for jailbreak/rooting detection. Although the functionality is mainly relevant to Android, the main active threats are in Android.[7]

Developers should take advantage of this inbuilt functionality in the Android platform to ensure that the environment the device is running in is not compromised. A few examples are checks to see whether there is malware on the device, verify whether a device is a bot and perform an overall check for indicators of compromise on the device.[8]

The App Code Shall Be Obfuscated

Obfuscation is typically done for consumer-facing apps and apps with sensitive data or intellectual property. Certain commercial app stores will also add their own obfuscation to apps.
Code obfuscation scrambles the code, making it harder for the attacker to understand what the application is doing. This may, for example, be achieved by renaming classes that may give away the application’s functioning.

Obfuscation makes it harder for an application to be attacked and is a dissuasive measure. However, with enough time and effort, the protections of obfuscation can be bypassed, and developers should ensure obfuscation does not replace, but rather augments, all other security protections considered in this checklist.

Life Cycle

All Test Data Shall Be Removed From the App Container (.ipa, .apk, etc.)

At times, developers neglect the removal of test data from the application. For example, during testing, developers sometimes allow certain actions (e.g., key sequences) to bypass authentication to be able to test multiple sets of data rapidly. These constitute vulnerabilities in a production app, and they should be removed beforehand.

No Debugging Flags Shall Be Set in the Finalized App

It’s possible to forbid debuggers from interacting with the app. This makes it harder for an attacker to reverse-engineer an application and to have visibility on background processes.

The App Shall Go Through Application Security Testing

This is a generic requirement. Mobile AST unveils vulnerabilities that could be exploited by hackers or inadvertently leak sensitive information. The security checklist in this Toolkit provides a reminder for developers of the pitfalls to be avoided but cannot replace testing. (For information on how testing works, and which the main vendors are providing such services, see the Mobile use case within the “Critical Capabilities for Application Security Testing.”)

Evidence

1 “iOS Keychain Weakness FAQ,” Fraunhofer Institute for Secure Information Technology (SIT).

2 “Elcomsoft iOS Forensic Toolkit: Enhanced Forensic Access to iPhone/iPad/iPod Devices Running Apple iOS“

3 “Use Whatsapp? Your Phone number Is Your Username and IMEI Is the Password —

Hackable"

[4] "GlobalPlatform: Trusted User Interface Made Simple"

[5] "Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules"

[6] "Android 5.0 Behavior Changes"

[7] "White Paper: Mobile Financial Malware 2017 Threat Report"

[8] "Protect Against Security Threats With SafetyNet"

THE
UNIVERSITY
OF RHODE ISLAND

DIVISION OF
ADMINISTRATION
AND FINANCE

THINK BIG WE DO™

PURCHASING DEPARTMENT
10 Tootell Road, Suite 3, Kingston, RI 02881 USA p: 401.874.2171 f: 401.874.2306 uri.edu/purchasing

Important Notice

Please note that the address for the URI Purchasing Office has changed although we have **not** moved and are still located in the Dining Services Distribution Center building.

Our new address is: 10 Tootell Road

Due to the added extension of Plains Road, the street name where our building resides has been changed and is now considered an extension of Tootell Road.

Also please remember to **always** write the Bid No. and the Bid Date/Time on the upper left-hand side of your envelope:

Bid No: ____________________
Bid Date/Time: ______________

TO **MAIL** YOUR BID:

University of Rhode Island
P.O. Box 1773
Purchasing Department
Kingston, RI 02881

TO **COURIER** YOUR BID:

University of Rhode Island
Purchasing Department
Dining Services Distribution Center
10 Tootell Road
Kingston, RI 02881-2010