THE CITADEL		
	Solicitation Number	**RFP 21018-SB**
	Addendum #	**1**
	Date Issued	**April 8, 2021**
	Procurement Officer	**Scott Brechtel**
	Phone	**843-953-2737**
	E-Mail Address	**sbrechte@citadel.edu**

SOLICITATION TITLE: Grant Management Software

TYPE OF ADDENDUM:

X Change or clarification to the Solicitation's specifications, requirements, or scope of work.

X Questions posed regarding the Solicitation and their respective answers by The Citadel.

QUESTIONS FROM OFFERORS - AMENDMENT (JUN 2017)
THE SOLICITATION IS AMENDED AS PROVIDED HEREIN. INFORMATION OR CHANGES RESULTING FROM QUESTIONS WILL BE SHOWN IN A QUESTION-AND-ANSWER FORMAT. ALL QUESTIONS RECEIVED HAVE BEEN REPRINTED BELOW. THE "STATE'S RESPONSE" SHOULD BE READ WITHOUT REFERENCE TO THE QUESTIONS. THE QUESTIONS ARE INCLUDED SOLELY TO PROVIDE A CROSS-REFERENCE TO THE POTENTIAL OFFEROR THAT SUBMITTED THE QUESTION. QUESTIONS DO NOT FORM A PART OF THE CONTRACT; THE "STATE'S RESPONSE" DOES. ANY RESTATEMENT OF PART OR ALL OF AN EXISTING PROVISION OF THE SOLICITATION IN AN ANSWER DOES NOT MODIFY THE ORIGINAL PROVISION EXCEPT AS FOLLOWS: UNDERLINED TEXT IS ADDED TO THE ORIGINAL PROVISON. STRICKEN TEXT IS DELETED. 02-2A097-1]

□ Other Change:

IMPORTANT NOTICE:

X Contractor is required to acknowledge receipt of this Addendum by signing below and returning a copy with its Offer.

DESCRIPTION OF CHANGES:

All respondents must also complete and return with their proposal a copy of the Security Assessment Questionnaire that is included at the end of this addendum.

Questions & Answers

Q: How many users will need to use this solution?
A: Approximately 30 users will need to use this solution.

Q: How many internal or external users need access to the system?
A: Internal users would be approximately 30.

Q: How many anticipated users of the research grant management software? Please specify how many model administrators, basic data input users, and read-only users.
A:1-3 administrators, 15-20 input users, and 5-7 read only users.

Q: How many applications or applicants are received on a yearly basis?
A: 50

Q: Does the award process have a multi-tier approval workflow?
A: Yes

Q: Are there any other “must have” integration besides Ellucian Banner?
A: No

Q: Does the project have a budget and access to funds?
A: Funds are available to procure this software solution.

Q: What is the timeline to have the new system in production?
A: Fall 2021

Q: Will the Citadel be open to a two separate contracts—one contract for professional services and one contract for software licensing?
A: Possibly, based upon proposals received.

Q: Do you require grants.gov integration and functionality?
A: No

Q: What are your submission numbers, number of proposals, number of awards, etc. on an annual basis? What is the dollar value of these awards?
A: 40-50 applied for each year and approximately 15 received each year. Dollar value is approximately 2-3 million each year.

Q: Many schools find it valuable to implement Conflict of Interest (COI) and/or Protocol modules to supplement pre- and post-award software. Are these components of interest to the Citadel?
A: Possibly, based upon the proposals received.

Q: Our software integrates with Ellucian Banner and we suggest using the Banner system to fulfill several of the financial requirements of this RFP, including real-time tracking, financial summaries, burn rate, and P&L statements. The vast majority of our clients utilize the financial system of Banner and then integrate through API’s into our software. Is this something the Citadel would be amenable to?
A: No

Q: Is the Citadel only using Ellucian Banner for billing and not other financial management (i.e. payroll)? Or does the Citadel already use Ellucian Banner's capabilities to meet the financial requirements outlined in this RFP, including the following:
- Generate financial summaries, burn rate, and P&L statements
- Improve budget spend-down oversight
- Maintain budgets and balances for multi-year sponsored projects
- Track internal commitments with cost accounting functionality
- Compute and encumber projected salaries and benefits for individual budget periods
- Forecast salary coverage
- Generate reports for fiscal oversight of individual funds, research teams, and organizational units
A: We currently use Banner for all things related to grants

Q: How many staff members are dedicated to research and research administration? How many faculty and/or students (or what percentage of the faculty and/or student body) are involved in sponsored research?
A: 1-3 administrators and 10% of faculty and students involved in research

Q: Does the Citadel have an existing relationship with the Ellucian Banner system and can it be integrated with Salesforce? https://www.ellucian.com/solutions/ellucian-ethos
A: We are a Banner Ellucian Customer, but it is unknown if we can integrate with Salesforce.

Q: Do you have API (integration component banner system) that can be used by Salesforce developers?
A: Currently we do not have this option.

Q: What is the Citadel's current total research expenditure?
A: The Citadel receives approximately $2-3 million in research grants per year and expends about the same.

Except as provided herein, all terms and conditions of the Solicitation referenced above remain unchanged and in full force and effect.

SIGNATURE OF PERSON AUTHORIZED TO EXECUTE ON BEHALF OF OFFEROR

By:_____

Printed Name & Title:_____

Offeror Name:_____

Date:_____

SERVICE PROVIDER SECURITY ASSESSMENT QUESTIONNAIRE

Instructions: (1) Attach additional pages or documents as appropriate and make sure answers cross reference to the questions below. (2) As used in this Questionnaire, the phrase "government information" shall have the meaning defined in the clause titled "Information Security." (3) This Questionnaire must be read in conjunction with both of the following two clauses (a) Service Provider Security Assessment Questionnaire – Required, and (b) Service Provider Security Representation.

1. Describe your policies and procedures that ensure access to government information is limited to only those of your employees and contractors who require access to perform your proposed services.

2. Describe your disaster recovery and business continuity plans.

3. What safeguards and practices do you have in place to vet your employees and contractors who will have access to government information?

4. Describe and explain your security policies and procedures as they relate to your use of your contractors and next-tier sub -contractors.

5. List any reports or certifications that you have from properly accredited third-parties that demonstrate that adequate security controls and assurance requirements are in place to adequately provide for the confidentiality, integrity, and availability of the information systems used to process, store, transmit, and access all government information. (For example, an ISO/IEC 27001 compliance certificate, an AICPA SOC 2 (Type 2) report, or perhaps an AICPA SOC 3 report (i.e., a SysTrust or WebTrust seal)). For each certification, describe the scope of the assessment performed. Will these reports / certifications remain in place for the duration of the contract? Will you provide the state with most recent and future versions of the applicable compliance certificate / audit report?

6. Describe the policies, procedures and practices you have in place to provide for the physical security of your data centers and other sites where government information will be hosted, accessed or maintained.

7. Will government information be encrypted at rest? Will government information be encrypted when transmitted? Will government information be encrypted during data backups, and on backup media? Please elaborate.

8. Describe safeguards that are in place to prevent unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access or disclosure of government information.

9. What controls are in place to detect security breaches? What system and network activity do you log? How long do you maintain these audit logs?

10. How will government information be managed after contract termination? Will government information provided to the Contractor be deleted or destroyed? When will this occur?

11. Describe your incident response policies and practices.

12. Identify any third party which will host or have access to government information.

Offeror's response to this questionnaire includes any other information submitted with its offer regarding information or data security.

SIGNATURE OF PERSON AUTHORIZED TO REPRESENT THE ACCURACY OF THIS INFORMATION ON BEHALF OF CONTRACTOR:

By: _____
(authorized signature)

Its: _____
(printed name of person signing above)

_____
(title of person signing above)

Date: _____