THE CITADEL		
	Solicitation Number	**RFP 27008-LB**
	Addendum #	**1**
	Date Issued	**10/21/2026**
	Procurement Officer	**Luke Bollmann**
	Phone	**843-953-6873**
	E-Mail Address	**lbollman@citadel.edu**

SOLICITATION TITLE: RFP 27008-LB Computerized maintenance management system.

TYPE OF ADDENDUM:

☒ Change or clarification to the Solicitation's specifications, requirements, or scope of work.
☒ Questions posed regarding the Solicitation and their respective answers by The Citadel.
☒ Other Change: Submission Deadline Extended until: November 5th, 2026 @ 2:00 PM Eastern Standard time.

QUESTIONS:

Vendor qualifications and evaluation

1. Vendor Qualifications — Section II, Requirement 2.1. Does the requirement for ten years of higher-education CMMS experience apply to the software manufacturer, the prime contractor, or the combined experience of the proposed team?

Answer: Requirement 2.1 requires a minimum of ten years of experience producing, implementing, and maintaining CMMS systems in college/university settings. It also requests the proposed product's history and the project team's experience. Each element of the proposed project team should have 10 years of relevant experience.

2. Can the requirement for deployment at 25 college campuses be satisfied through installations of the proposed software by the manufacturer and its implementation partners?

Answer: No

3. Can the requirement for four successful Ellucian Banner integration references be met through a combination of software manufacturer, prime contractor, and subcontractor references?

Answer: No

4. Must the Banner integration references involve the exact CMMS product and version being proposed, or will integrations using earlier versions of the same product qualify?

Answer: The solicitation requires references for the proposed system that have successfully interfaced with Banner but does not specify a version-matching rule.

5. Are the vendor experience and reference requirements mandatory pass/fail criteria or scored evaluation criteria?

Answer: They are mandatory qualification requirements. Section II expressly states that all vendor requirements are mandatory, and that failure to meet any of them will result in disqualification.

6. May the software publisher and named implementation partner jointly satisfy the experience, campus deployment, and Banner reference requirements?

Answer: No

7. Does the requirement for ten years of higher-education CMMS experience apply to the software manufacturer, the prime contractor, or the combined experience of the proposed team?

Answer: No

8. Can the requirement for deployment at 25 college campuses be satisfied through installations of the proposed software by the manufacturer and its implementation partners?

Answer: No

9. Can the requirement for four successful Ellucian Banner integration references be met through a combination of software manufacturer, prime contractor, and subcontractor references?

Answer: No

10. Must a named implementation/integration subcontractor independently meet the 10-year college CMMS, 25-campus, and eight-reference requirements, or are those requirements assessed against the prime offeror and proposed CMMS product? We are not requesting a waiver.

Answer: Yes, minimum ten years of experience producing, implementing and maintaining CMMS systems in College/University settings.

11. For Requirements 2.1 and 2.2, may an offeror satisfy the mandatory experience, campus-installation, and Ellucian Banner reference thresholds through the proposed CMMS product manufacturer, parent company, or named subcontractor, or must the legal entity submitting the offer independently meet every threshold?

Answer: No

12. Will The Citadel accept a prime contractor/subcontractor delivery model in which [redacted] provides implementation and support while the software manufacturer provides product licensing and escalation support?

Answer: The solicitation does not categorically prohibit this delivery model. However, the offeror must identify its subcontractors and demonstrate that the proposed arrangement satisfies the mandatory qualification, implementation, maintenance, and support requirements. Software licensing must also comply with the separate licensing provisions in Section VII. Acceptance of a particular arrangement is not guaranteed. (RFP § V, p. 29; § III, Requirements 4.1–4.5 and 5.1–5.5, pp. 17–18; § VII, Software Licensing Agreements–Single Solicitation, pp. 46–47.)

13. Given the specific reference requirements in Section II, 2.2, and potential restrictions on public-sector references, will The Citadel be willing and authorized to serve as a reference for the selected vendor after successful implementation?

Answer: The solicitation does not commit The Citadel to serve as a reference for the selected contractor.

14. Evaluation Factors. The Offeror Qualifications factor refers to "converting institutions from existing payment processing, One Card, and/or related systems." Please confirm whether this applies to a CMMS procurement.

Answer: This will be removed from Offeror's Qualifications as it is nonapplicable.

15. Section VI, page 30, refers to payment processing and OneCard experience. Please confirm whether CMMS implementation and maintenance-management experience is intended and whether corrected evaluation language will be issued.

Answer: This will be removed from Offeror's Qualifications as it is nonapplicable.

16. The cost formula example uses 30 points while the stated weight is 10. Please confirm 10 points.

Answer: Cost will be 10/100 of the points as listed under evaluation factors. 30 was used as an example.

17. Please confirm that the October 13 question deadline and October 28 proposal deadline, each stated as 2 PM, use local Eastern time.

Answer: 2:00pm EST.

Existing CMMS and operational requirements

18. Do you have an existing CMMS on campus? If so, are they currently integrated with Banner?

Answer: We currently contract with WebTMA. The solicitation confirms that an existing system is contemplated: Requirement 4.3 requires the contractor to work with Citadel staff to extract data from the current system and import it into the new CMMS. It also requires two-way communication with existing Citadel systems, including Banner. However, it does not identify the incumbent CMMS or confirm whether the current system is already integrated with Banner. (RFP § III, Requirements 3.6 and 4.3, pp. 17–18.)

19. What CMMS or work-order management system is currently used by Facilities Engineering, and what are the primary reasons for replacing it?

Answer: WebTMA, contract period is running out.

20. How many facilities, buildings, maintainable assets, and active work orders are expected to be managed by the new system?

Answer: The solicitation does not specify the number of buildings, assets, or active work orders. It states that Facilities and Engineering receives and processes over 10,000 requests in a typical year. That figure provides a workload indicator but should not be treated as the number of active work orders, buildings, or maintainable assets. (RFP § III, Scope of Operation, p. 15.)

21. Which processes must be supported at go-live: corrective maintenance, preventive maintenance, inspections, asset inventory, space management, inventory, purchasing, or capital planning?

Answer: The solicitation requires a broad CMMS capability set, including work-order management, project management, costing, storeroom/warehouse functions, tool inventory, preventive maintenance, personnel tracking, building information, and equipment information. Specific requirements include customer work requests, work-order tracking, project costs, inventory transactions, and preventive maintenance. Space management, capital planning, and a separate purchasing workflow are not expressly established as standalone requirements in the cited list. (RFP § III, CMMS Requirements and Requirements 8–17, pp. 15, 19–27.)

22. Are there specific reporting, dashboards, key performance indicators, or regulatory compliance requirements that the proposed CMMS must support?

Answer: Yes, the solicitation specifies reporting and dashboard capabilities. Requirements include a built-in report writer, ad hoc reporting, scheduled reports, automatic emailing, exportable billing statements, configurable dashboards, and metrics such as delinquent and active work orders. Additional reporting and regulatory compliance requirements beyond those expressly listed are not specified. (RFP § III, Requirements 7.1–7.5 and 9.1–9.3, pp. 18–20.)

23. Would The Citadel be interested in optional assessment services to evaluate maintenance management processes, reporting, integrations, data structures, and system utilization in order to identify optimization opportunities and implementation priorities?

Answer: No

User counts, mobile access, and licensing

24. How many users require access to the CMMS, by role and license type?

Answer: The solicitation does not provide user counts by role or license type. It does require different administrator-defined access levels, including read-only, read-and-edit, and full system capability, as well as single sign-on through Microsoft Entra ID. Offerors should not assume an official number of users or license tiers. (RFP § III, Requirements 3.4 and 6.1–6.2, pp. 17–18.)

25. Please provide the anticipated numbers of administrators, facilities users, technicians, concurrent users, requestors, buildings, maintainable assets, and annual work orders that offerors should use for licensing and pricing.

Answer: The system must support configurable user access and dashboards, and the implementation plan is expected to account for Citadel staff resources.(RFP § III, Requirements 3.4, 4.4, 6.2, and 9.1, pp. 17–20.)

26. How many users are anticipated, broken down by administrators, supervisors, technicians, requesters, and occasional users?

Answer: No role-by-role user count is specified. The system must support configurable user access and dashboards, and the implementation plan is expected to account for Citadel staff resources.(RFP § III, Requirements 3.4, 4.4, 6.2, and 9.1, pp. 17–20.)

27. Several requirements reference barcode-enabled inventory, warehouse, and tool management processes. Should offerors include technician and warehouse mobile access/licensing as part of the proposed solution, or should mobile functionality be proposed as an optional component? If mobile functionality is required, please provide the approximate number of users who will need mobile access.

Answer: Barcode functions are expressly required for inventory activities such as physical counts, issues, receipts, returns, adjustments, and bin labels. However, the solicitation does not expressly require mobile-device access or provide a mobile-user count. Offerors should demonstrate the required barcode functionality.

28. Does The Citadel require mobile work-order execution, including offline capability for technicians working without reliable network access?

Answer: The solicitation requires web-based work requests and work-order management, but it does not expressly require mobile applications or offline operation.

Project budgets and commercial requirements

29. What is the typical budget range and annual total value of projects the CMMS will manage?

Answer: Facilities Engineering manages a wide range of work, from small in-house service requests to multimillion-dollar projects. Project budgets and expenditures vary depending on the nature and scope of the work.. (RFP § III, Scope of Operation, p. 15.)

30. What is the anticipated budget for software, implementation, and ongoing support over the five-year contract period?

Answer: This depends on what is offered.

31. Does The Citadel prefer subscription-based licensing, perpetual licensing, or will both commercial models be evaluated?

Answer: The Citadel will consider both subscription-based and perpetual licensing models, provided the proposed solution meets the requirements outlined in the RFP. All proposals will be evaluated in accordance with the established evaluation criteria.

32. Should vendors price software licensing, implementation, integration, migration, training, and ongoing support separately?

Answer: The solicitation requires a detailed total cost of ownership, including purchasing, owning, operating, maintaining, and supporting the proposed solution over the potential contract term. It also requires pricing to include the cost of every proposed software product. Separate line-item pricing is a sensible way to demonstrate these costs, but the exact required pricing breakdown should follow the bidding schedule and cost proposal instructions.

33. Can vendors propose optional modules or a phased expansion roadmap beyond the initial Facilities Engineering requirements?

Answer: The solicitation requires the offeror to describe the proposed solution and total cost of ownership. It does not expressly establish an optional-module or phased-expansion evaluation framework. The offeror may describe additional capabilities separately but should not substitute optional functionality for mandatory requirements or alter the solicitation's terms.

Hosting, VMware, and technical architecture

34. Technical Specifications 3.2. Please confirm that an on-premises installation on The Citadel's VMware environment satisfies this requirement. Would a vendor-hosted option also be considered?

Answer: An on-premises system operating in The Citadel's VMware environment is consistent with the express requirement. The solicitation also contemplates remotely hosted applications in Requirement 3.6 but does not expressly waive the VMware requirement for SaaS deployments.

35. Section 3.2 requires the system to operate in a VMware environment, while the second Section 3.6 addresses remotely hosted applications. Will The Citadel accept a vendor-hosted (cloud/SaaS) solution in lieu of an on-premises VMware installation? If on premises is required, please provide The Citadel's VMware, operating system, and database standards.

Answer: We do accept SaaS solutions. If on prem is required, we would prefer either Windows Server 2022 or Red Hat Enterprise Linux 8+9.

36. Hosting — Section 3.2. Will a vendor-hosted SaaS solution be accepted instead of a system operating in The Citadel's VMware and backup/restore environment? If so, what recovery and data-export arrangements are required?

Answer: SaaS is accepted. Recovery and data exports should be in concurrent with Banner along with other systems already in place. See the citadel technology security standards addendum appendix E.

37. Will vendor-hosted SaaS deployments be considered acceptable alternatives to an on-premises deployment?

Answer: SaaS is accepted.

38. Please clarify whether a vendor-hosted commercial SaaS solution is fully acceptable. If so, do the VMware operation and The Citadel backup/restore requirements apply only to institution-hosted solutions, and may a SaaS vendor use its standard CONUS-hosted backup and disaster-recovery architecture?

Answer: SaaS is accepted. AWS/Azure/Google cloud services are accepted. The backup/restore requirements only apply to this if The Citadel hosts this environment.

39. Is The Citadel seeking an on-premises deployment, a vendor-hosted SaaS solution, or are both deployment models acceptable?

Answer: Both deployment models are acceptable.

40. Does the stated VMware compatibility requirement apply to the CMMS application hosting environment, integration components, or both?

Answer: Only applies to the Citadel hosted environment.

41. If SaaS hosting is permitted, what recovery, disaster-recovery, backup, and data-export arrangements are required?

Answer: The solicitation requires detailed procedures to ensure the security and continued availability of remotely hosted data. It does not specify numerical recovery point objectives, recovery time objectives, backup frequency, retention periods, or data-export requirements. Offeror can propose these measures.

Database connectivity and reporting

42. Database Access — Section 3.5. Does "OBDC compliant" mean ODBC compliant? Is direct database connectivity required, or are supported APIs and report exports acceptable?

Answer: This is a typo. ‘ODBC compliant’ would be correct.

Ellucian Banner integration

43. Banner Integration Scope. Please clarify the intended scope of the Ellucian Banner integration, including account validation, budget validation, chargeback processing, project accounting, invoice

processing, purchase requisitions, purchase orders, receiving, and any required inbound or outbound financial or procurement transactions.

Answer: The solicitation expressly requires two-way communication with existing Citadel systems, including Banner, without custom programming by Citadel personnel. Requirement 12.8 specifically requires the ability to validate budget numbers through uploaded data or an interface with a financial system such as Banner. Other requirements address billing codes, cost allocation, invoice processing, and inventory accounting transactions. However, the solicitation does not define a complete Banner interface specification covering every transaction listed in the question. The required inbound and outbound data objects and transaction flows need clarification. (RFP § III, Requirements 3.6, 12.2–12.14, and 13.6, pp. 17, 22–23.)

44. Banner Environment. Which Banner version and modules must integrate with the CMMS, and which APIs or other integration interfaces are available?

Answer: Banner 9

45. Banner Integration Scope. Which business processes and data exchanges are required, in each direction? What transaction volumes and acknowledgment or error-handling mechanisms are expected?

Answer: The solicitation requires two-way system communication and validates budget numbers through uploaded data or a financial-system interface. It also requires validation of system functionality and interfaces before go-live.

46. Which Ellucian Banner products, modules, and versions are currently deployed, including Finance, Human Resources, Procurement, and Fixed Assets?

Answer: Banner 9

47. What specific business transactions must be integrated between Banner and the CMMS, such as purchase orders, requisitions, vendors, labor costs, inventory, or financial account codes?

Answer: Expressly stated requirements include budget validation, cost allocation across accounts, labor and materials costing, invoice processing, and accounting transactions generated by inventory issues. The solicitation does not expressly establish that every example in the question—such as purchase requisitions, purchase orders, or vendor master synchronization—must be integrated with Banner. The full transaction scope requires clarification. (RFP § III, Requirements 12.2–12.14 and 13.6, pp. 22–23.)

48. Does The Citadel have an existing Banner integration framework, API gateway, middleware platform, or established interface specifications available to vendors?

Answer: Requirement 3.6 does require two-way communication with existing Citadel systems without custom programming by Citadel personnel.

49. Are Banner integrations required to operate in real time, near real time, or through scheduled batch processing?

Answer: This is not specified. Explain capabilities in proposal.

50. Will The Citadel provide Banner technical resources, test environments, interface documentation, and support during integration development and testing?

Answer: Yes. Comparable integrations with other ERP systems may be considered. However, the vendor should clearly explain how they would integrate their solution with Banner and identify any requirements or assistance needed from The Citadel.

51. Will equivalent, demonstrated integrations with other enterprise resource planning systems be considered if the proposed solution supports Banner through standard APIs or middleware?

Answer: The solicitation specifically requires the proposed system to be in use at 25 campuses and requires at least eight references, at least half of which have successfully interfaced with Banner. It does not state that equivalent integrations with other ERP systems may substitute for the Banner-reference requirement. Such experience may support a vendor's narrative, but it should not be assumed to satisfy the express Banner requirement without written clarification. (RFP § II, Requirement 2.2, p. 16.)

52. For the Banner integration, what are the full requirements? Requirement 12.8 lists validating budget numbers; are there any others?

Answer: In addition to budget validation, the solicitation specifies two-way communication with existing Citadel systems, labor and material costing, multiple-account billing, invoice processing, and accounting transactions generated by inventory issues. It does not provide a comprehensive Banner interface specification identifying every required exchange. The full list of required Banner transactions should be clarified. (RFP § III, Requirements 3.6, 12.2–12.14, and 13.6, pp. 17, 22–23.)

53. Is the CMMS expected to be the system of record for invoice processing, purchase orders, and blanket purchases, or will it record and track those costs while Banner remains the system of record for accounts payable and purchasing?

Answer: The solicitation requires the CMMS to provide an invoice-processing tool and cost tracking, but it does not explicitly assign the authoritative system-of-record role for accounts payable, purchase orders, or blanket purchases. It also requires budget validation through uploaded data or a financial-system interface. The division of responsibility between Banner and the CMMS must be clarified. (RFP § III, Requirements 12.8 and 12.10–12.14, p. 22.)

Billing and chargeback functionality

54. Billing Configuration — Sections 7.3–7.4. May the contractor configure scheduled reports and billing statements during implementation, provided they are ready to use at go-live without further user configuration?

Answer: The solicitation requires report scheduling and automatic emailing to be available as out-of-the-box functions without special configuration or administrative support from the user. It similarly requires pre-established, exportable billing reports and automated billing statements. Contractor configuration during implementation may be consistent with those requirements, provided the required functions are ready to use at go-live and do not depend on additional user configuration. (RFP § III, Requirements 7.3–7.4, p. 19.)

55. Billing Recipients — Section 7.4. Must billing statements be emailed to external recipients or recipients without CMMS licenses?

Answer: Emails should be sent to anyone that can request a work order or access the platform.

56. Please describe the billing model behind the "push-button billing" requirement: who is billed (internal departments, external customers, or both), the approximate number of billing accounts, the billing frequency, and how charges are expected to reach Banner (for example, journal entry upload).

Answer: The solicitation requires push-button billing, exportable billing reports, scheduled billing, automatically generated statements, and automatic emailing. It also requires work orders to be billable to multiple accounts using percentage or dollar-value splits and requires administrator-definable billing codes. (RFP § III, Requirements 7.4 and 12.2–12.4, pp. 19, 22.)

Existing system, data migration, and historical records

57. Existing CMMS and Migration — Section 4.3. What is the current CMMS, and what data extraction methods are available? Please provide record counts, attachment counts, total data size, and years of history to migrate.

Answer: the existing CMMS is WebTMA. Current data extraction methods are excel, PDF, HTML, and PNG files. The system has been in use since 2011, record count and data size is unknown.

58. Historical Records — Section 4.3. Must historical workflow and audit events be recreated in the new CMMS, or may they be retained in an approved searchable archive?

Answer: The solicitation requires migration of identified existing data and requires active work orders to maintain a complete audit trail of changes. It does not explicitly state whether every historical workflow event must be recreated in the new system or whether a searchable archive is acceptable.

59. Please identify the incumbent CMMS and provide estimated record counts, source formats, attachment volumes, years of history, asset records, inventory records, open work orders, and preventive-maintenance schedules expected to be migrated.

Answer: The solicitation requires the contractor to identify, collect, potentially relabel, extract, and import existing data. It does not supply the requested volumes, formats, or historical period. The implementation team must work with The Citadel to determine these details, but the incumbent system and migration quantities remain unspecified. (RFP § III, Requirements 4.3–4.4, p. 17.)

60. What historical data must be migrated from the existing system, including assets, work orders, preventive maintenance schedules, inventory, and associated documents?

Answer: The solicitation expressly requires migration of existing data such as buildings, floors, rooms, and accounts. The CMMS requirements also address equipment, inventory, work orders, and preventive maintenance.

61. Will The Citadel provide cleansed and validated source data, or is data assessment, cleansing, and transformation expected to be included in the vendor's scope?

Answer: The solicitation expects the contractor to work with Citadel staff to identify, collect, and potentially relabel data. It does not establish that The Citadel will provide fully cleansed data or explicitly allocate every data-cleansing and transformation task. The implementation matrix must identify responsibilities, so the division of work should be documented before implementation. (RFP § III, Requirements 4.3–4.4, p. 17.)

Implementation timeline, testing, and training

62. Does the four-month implementation requirement mean full production deployment of all functionality and integrations, or would a phased implementation with core CMMS capabilities operational within four months be acceptable?

Answer: Product should be operational in four months.

63. What acceptance testing, training, documentation, and operational readiness milestones must be completed before the system is considered fully functional?

Answer: The solicitation requires the contractor to test the validity of data, data relationships, all system functions, and interfaces before go-live, with the stated goal of 100% functionality. It also requires an implementation matrix and ongoing technical support.

Authentication and single sign-on

64. Authentication — Section 6.1. Which authentication and federation protocols are permitted? Will SAML or OpenID Connect single sign-on integrated with The Citadel's identity provider satisfy Section 6.1?

Answer: Requirement 6.1 will be “Software needs to be Microsoft Entra ID SSO login compatible.”

65. What identity management and single sign-on technologies must be supported, such as Microsoft Entra ID, Active Directory, SAML, or OpenID Connect?

Answer: Requirement 6.1 will be “Software needs to be Microsoft Entra ID SSO login compatible.”

Cybersecurity, data residency, and support

66. Support Access and Data Location. Does the continental-U.S. restriction apply to all remote support personnel who access government information?

Answer: See Appendix E

67. Incident and Support Targets. What response and resolution targets apply to routine support, emergency support, and security incidents, in addition to the stated 24-hour security incident notification requirement?

Answer: See Appendix E

68. What cybersecurity requirements apply to the solution, including data encryption, vulnerability management, audit logging, backup, and disaster recovery?

Answer: See Appendix E.

69. Are there specific data residency, accessibility, or security compliance standards that the proposed solution must satisfy?

Answer: Answer: See Appendix E

70. What existing systems beyond Ellucian Banner must integrate with the CMMS, including GIS, building automation, access control, or document management systems?

Answer: There are no additional system integration requirements beyond those identified in the RFP.

Contractual and legal requirements

71. Limitation of Liability — Single Agency. The cap in paragraph (1) reads "[a dollar amount]". Please state the amount. Will the State accept a cap equal to the fees paid or payable in the 12 months before the claim?

Answer: The solicitation does not provide the dollar amount. The limitation-of-liability clause contains a placeholder for the contractor's cap and a separate placeholder for the governmental unit's cap. It also excludes certain claims from the general limitation, including specified indemnification obligations and insured losses. The Procurement Officer must establish the intended amounts and determine whether a trailing-12-month-fees cap will be accepted. The South Carolina Procurement Code does not itself establish the missing contract-specific amount. (RFP § VII, Limitation of Liability–Single Agency, p. 45.)

72. Limitation of Liability (3)(g). As written, the cap does not apply to any loss "covered by a policy of insurance maintained or required … to be maintained." Since the RFP requires $5M/$10M cyber coverage, this effectively removes the cap for most claims. Will the State delete (3)(g), or limit uncapped exposure for data-related claims to the required insurance limits?

Answer: No. The Citadel does not intend to modify the Limitation of Liability provisions outlined in the solicitation. The required insurance coverage limits do not establish a cap on contractual liability.

73. Indemnification — Disclosure of Information and Information Use and Disclosure (h). Will the State accept limiting these obligations to the required cyber insurance limits instead of "without limitation"?

Answer: No. The Citadel does not intend to modify the indemnification or information security provisions outlined in the solicitation. The required cyber insurance limits do not establish a cap on these contractual obligations.

74. Indemnification — Intellectual Property. Will the State limit "IP right" to U.S. patents, copyrights and trade secrets, and exclude claims arising from modification by anyone other than the contractor, combination with items the contractor did not supply, or use of an outdated version after a non-infringing update was provided?

Answer: No. The Citadel does not intend to modify the Intellectual Property Indemnification provisions outlined in the solicitation. Offerors should prepare their proposals in accordance with the stated terms and conditions.

75. Ownership of Data & Materials. Please confirm that this clause covers The Citadel's data and deliverables prepared specifically for The Citadel and does not transfer ownership of the contractor's pre-existing software, its configurations, documentation or general know-how. Those would remain the contractor's and be licensed to The Citadel for the contract term.

Answer: See Appendix E

76. Software Licensing Agreements — Single Solicitation. The "South Carolina Standard Amendment to End User License Agreements for COTS Software – Single Agency" is referenced but not attached. Please provide it.

Answer: The ownership provisions apply as stated in the solicitation. The Citadel's data and materials prepared specifically for The Citadel are subject to those provisions. Any proposed exceptions regarding pre-existing contractor intellectual property or licensing rights must be reviewed and approved by the appropriate contracting authority.

The solicitation's software licensing clause identifies the South Carolina Standard Amendment to End User License Agreements for Commercial Off-The-Shelf Software–Single Agency as an attachment, while the contract-document provision describes it as an exhibit offered for information only. The clause also states that software licensing agreements must be separately executed and that the offeror must provide a requested license agreement within one business day. (RFP § VII, Contract Documents & Order of Precedence–Software Licensing–Single Agency, p. 36; Software Licensing Agreements–Single Solicitation, pp. 46–47.)

77. Insurance — Information Security and Privacy. Will the State accept the cyber/E&O limits on a per-claim and aggregate basis under a combined Tech E&O/Cyber policy?

Answer: The solicitation contains an information-security and privacy insurance clause and invites offerors with concerns about insurance requirements to raise them with the Procurement Officer before opening. It does not expressly confirm that a combined Technology Errors and Omissions/Cyber policy with the proposed per-claim and aggregate limits will be accepted. The Procurement Officer and the State's insurance reviewers must determine whether the proposed policy satisfies the required coverage. (RFP § VII, Contractor's Liability Insurance–Information Security and Privacy, pp. 36–37.)

Proposal submission requirements

78. Do you require a printed version of the redacted document? Or just an electronic version?

Answer: Minimum a redacted copy on the thumb drive is required.

CHANGE OF SPECIFICATIONS

SCOPE OF WORK section 6.1) Software needs to be Microsoft Entra ID SSO login compatible.

APPENDIX E: see below Page 13-19 of addendum 1. This form must be completed and attached to addendum.

Offeror’s Qualifications: Experience converting institutions from existing payment processing, One Card, and/or related systems will not be an evaluation factor.

IMPORTANT NOTICE:

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
Signature:_____

Printed Name & Title:_____

Company Name:_____

Date:_____

APPENDIX E

THE CITADEL | PROCUREMENT SERVICES | INFORMATION TECHNOLOGY SECURITY

THE CITADEL TECHNOLOGY SECURITY STANDARDS ADDENDUM

For Inclusion in a Solicitation, RFP, Contract, or Purchase Order

Solicitation	Offeror
RFP / Solicitation No.: _____	Legal Name: _____
Solicitation Title: _____	Primary Contact: _____
Procurement Officer: _____	Email / Phone: _____

REQUIRED RESPONSE: Complete every applicable requirement and checklist item. Mark each response Yes, Partial, No, or N/A; identify the applicable requirement ID and supporting evidence; explain every Partial, No, N/A, or requested exception; and sign the certification. If the Offeror receives an award, the applicable requirements become contractual obligations unless The Citadel expressly accepts a written exception and incorporates it into the resulting contract or purchase order.

Purpose. This Addendum establishes the minimum technology, cybersecurity, privacy, data-protection, and secure-configuration requirements applicable to an Offeror's proposed products, services, personnel, systems, subcontractors, and subprocessors. The Offeror shall disclose every requirement it cannot fully meet and submit the required exception information with its proposal. If the Offeror receives an award, the applicable requirements and any exceptions expressly accepted in writing by The Citadel become contractual obligations.

1. Applicability and Governing Standard

This Addendum applies when the Offeror, its personnel, its subcontractors, or any system or service used to perform the awarded work will: (1) access a Citadel system; or (2) create, receive, maintain, transmit, store, process, or dispose of Citadel Data. The Offeror shall comply with all federal, State of South Carolina, and other legal, regulatory, contractual, and institutional requirements applicable to the proposed scope, data, technology, and services. The Offeror shall maintain risk-appropriate controls aligned with NIST SP 800-53 Revision 5, including Release 5.2.0, and shall apply the current applicable CIS Benchmark for each technology as the secure-configuration baseline.

Definitions. "Citadel Data" means information created, received, maintained, transmitted, stored, processed, or disposed of for or on behalf of The Citadel. "Offeror" includes the entity submitting the proposal and, where applicable, its personnel, agents, subcontractors, subprocessors, and service providers. "Security Incident" means a suspected or confirmed event that compromises or may compromise the confidentiality, integrity, or availability of Citadel Data, a Citadel system, or a service provided to The Citadel. "Restricted Data" means Citadel Data designated as restricted under The Citadel's applicable data-classification requirements.

2. Mandatory Offeror Requirements

Response Instructions. The Offeror shall provide one response for every requirement. "Yes" means the proposed solution fully complies without exception. "Partial" means it complies with only part of the requirement or requires qualification. "No" means it does not comply. "N/A" means the requirement does not apply to the proposed scope, architecture, data, or service. Every Partial, No, or N/A response must identify the requirement ID and include an explanation, supporting evidence, identified risk, compensating controls, accountable owner, remediation date, and requested exception expiration, as applicable. Silence, an incomplete response, or a reference to future development does not constitute compliance.

ID	Requirement	Minimum Obligation	Offeror Response
01	Authorized use and confidentiality	Use Citadel Data only for the awarded work and minimum necessary purpose. Require personnel confidentiality commitments and restrict access by need-to-know.	☐ Yes ☐ Partial ☐ No ☐ N/A
02	Ownership and prohibited use	Recognize The Citadel's ownership and control of Citadel Data. Do not sell, monetize, advertise against, independently profile, or disclose data for unrelated purposes.	☐ Yes ☐ Partial ☐ No ☐ N/A
03	Education and regulated data	Process education records only under an approved FERPA basis and direct-control terms where applicable. Do not process payment-card, regulated-health, export-controlled, criminal-justice, controlled-unclassified, or classified information unless expressly authorized.	☐ Yes ☐ Partial ☐ No ☐ N/A

04	Artificial intelligence	Do not submit Citadel Data to public or unapproved AI services or use Citadel Data, prompts, outputs, metadata, telemetry, or derived content to train, tune, test, or improve models without prior written authorization. Before approved use, disclose providers, models, purposes, data inputs, retention, training use, human oversight, output use, safeguards, subprocessors, and processing locations. Notify The Citadel before material changes and provide a method to disable AI features or prevent Citadel Data from being used by them when required.	☐ Yes ☐ Partial ☐ No ☐ N/A
05	Location and subprocessors	Disclose processing, storage, backup, support, and remote-access countries and all subprocessors. Apply equivalent written obligations and remain responsible for subcontractor performance.	☐ Yes ☐ Partial ☐ No ☐ N/A
06	Access and authentication	Use unique identities, least privilege, prompt termination, separate administrative accounts, and MFA for privileged, remote, administrative, and cloud-console access.	☐ Yes ☐ Partial ☐ No ☐ N/A
07	Encryption	Encrypt non-public Citadel Data in transit and at rest, including endpoints, servers, databases, object storage, removable media, backups, snapshots, and replicas. Protect encryption keys and recovery material.	☐ Yes ☐ Partial ☐ No ☐ N/A
08	Logging and monitoring	Maintain protected, time-synchronized logging for authentication, privileged activity, administration, security events, and sensitive-data access. Monitor material events and preserve logs for investigations.	☐ Yes ☐ Partial ☐ No ☐ N/A
09	Vulnerability and patch management	Maintain supported software; scan for vulnerabilities; apply risk-based remediation; expedite remediation for critical or known-exploited vulnerabilities; document exceptions and compensating controls.	☐ Yes ☐ Partial ☐ No ☐ N/A
10	Endpoint and workload protection	Use centrally managed anti-malware/EDR or workload protection, tamper protection, monitored alerts, health reporting, and isolation capability where supported.	☐ Yes ☐ Partial ☐ No ☐ N/A
11	Secure development and supply chain	Use documented secure development, code review, dependency monitoring, secrets management, security testing, release approval, rollback, component inventory, and SBOM practices when applicable.	☐ Yes ☐ Partial ☐ No ☐ N/A
12	Continuity and recovery	Protect backups against unauthorized alteration or deletion; define recovery objectives; maintain continuity procedures; and test restoration and service recovery.	☐ Yes ☐ Partial ☐ No ☐ N/A
13	Incident notice	Notify The Citadel immediately and no later than 24 hours after discovery of a suspected Security Incident affecting Citadel Data or services. Send the initial notice to itssecurity@citadel.edu. Do not delay initial notice pending investigation. Preserve evidence, contain and investigate, provide updates, and coordinate external notices.	☐ Yes ☐ Partial ☐ No ☐ N/A
14	Monitoring tools and remote work	Disable screenshot, keystroke, webcam, or session recording involving Citadel systems or data unless IT and the data owner approve it in writing. Use approved encrypted remote access and managed or compliant devices.	☐ Yes ☐ Partial ☐ No ☐ N/A

15	Return, deletion, and separation	Immediately report personnel separation or reassignment and revoke access. At termination, expiration, or request, return Citadel Data and certify deletion or approved retention within 30 days, subject to legal holds and required retention.	☐ Yes ☐ Partial ☐ No ☐ N/A

Data Portability and Transition. Upon request and at termination or expiration, the Offeror shall provide Citadel Data and associated records required for transition in a documented, commonly usable, and nonproprietary format unless the resulting agreement specifies another format. The Offeror shall reasonably cooperate with transition activities, preserve the integrity and completeness of transferred data, and prevent service termination from impairing The Citadel's authorized access to its data during the agreed transition period. These obligations do not authorize retention beyond the period approved by The Citadel or required by law.

3. NIST SP 800-53 Control-Family Alignment

The Offeror shall maintain a documented security and privacy program aligned, as applicable and proportionate to risk, with the following NIST SP 800-53 control families: Access Control (AC); Awareness and Training (AT); Audit and Accountability (AU); Assessment, Authorization, and Monitoring (CA); Configuration Management (CM); Contingency Planning (CP); Identification and Authentication (IA); Incident Response (IR); Maintenance (MA); Media Protection (MP); Physical and Environmental Protection (PE); Planning (PL); Program Management (PM); Personnel Security (PS); PII Processing and Transparency (PT); Risk Assessment (RA); System and Services Acquisition (SA); System and Communications Protection (SC); System and Information Integrity (SI); and Supply Chain Risk Management (SR). The Offeror shall determine and document applicability based on the proposed service, architecture, data sensitivity, connectivity, threat exposure, and potential impact. For higher-risk procurements, The Citadel may require a tailored control matrix, implementation descriptions, control ownership, and assessment evidence. Alignment is risk-based and does not mean that every catalog control applies to every procurement.

4. Endpoint and Privileged-Workstation Hardening Baseline

The Offeror shall identify and implement the current applicable CIS Benchmark for each endpoint operating system and supporting technology within scope. CIS Level 1 is the minimum baseline for standard desktops and laptops. CIS Level 2 is required, when operationally compatible, for privileged workstations and high-risk use, such as PCI-DSS, GLBA, financial data processing, and FERPA data handling. The Offeror shall document the benchmark title, version, profile, assessment date, and implementation status. Any deviation requires written justification, documented compensating controls, an accountable owner, and a remediation or expiration date.

ID	Control Area	Minimum Requirement	Response
H-01	Supported platforms	Use vendor-supported operating systems and applications; remove or isolate end-of-support technology.	☐ Yes ☐ Partial ☐ No ☐ N/A
H-02	Secure configuration	Document the CIS Benchmark version and profile; assess at least annually and after major upgrades; monitor configuration drift.	☐ Yes ☐ Partial ☐ No ☐ N/A
H-03	Device security	Enable enterprise-managed full-disk encryption, Secure Boot and TPM or equivalent hardware trust where supported, automatic locking, host firewall, and centrally managed device compliance.	☐ Yes ☐ Partial ☐ No ☐ N/A
H-04	Least functionality	Remove or disable default credentials, unnecessary accounts, software, services, ports, protocols, management interfaces, legacy plugins, and insecure discovery.	☐ Yes ☐ Partial ☐ No ☐ N/A
H-05	Privilege and credentials	Prohibit routine local administrator access; use controlled elevation; protect cached credentials, tokens, password stores, certificates, and secrets; rotate or revoke after exposure.	☐ Yes ☐ Partial ☐ No ☐ N/A
H-06	Application and browser controls	Permit authorized software; restrict risky macros, scripts, interpreters, browser extensions, downloads, and unsigned or untrusted executables based on risk.	☐ Yes ☐ Partial ☐ No ☐ N/A
H-07	Network and remote access	Use encrypted remote access, MFA, device-compliance checks, session logging, secure Wi-Fi, segmentation, and restricted management interfaces. Prohibit unmanaged remote-control tools.	☐ Yes ☐ Partial ☐ No ☐ N/A
H-08	Data handling	Restrict local storage, printing, clipboard, screenshots, synchronization, removable media, and transfer based on classification and approved business need. Encrypt, scan, authorize, and track approved removable media.	☐ Yes ☐ Partial ☐ No ☐ N/A

H-09	Administrative environments	Use dedicated hardened workstations or equivalent isolated administrative environments for high-risk administration and separate administration from routine browsing and email when practicable.	☐ Yes ☐ Partial ☐ No ☐ N/A
H-10	Decommissioning	Revoke identities, certificates, tokens, VPN access, and management enrollment; sanitize media by an approved method; document disposition.	☐ Yes ☐ Partial ☐ No ☐ N/A

5. Server, Cloud, Application, and Service Baseline

ID	Minimum Requirement	NIST Alignment	Response
SC-01	Apply the current applicable CIS Benchmark; use Level 2 when applicable for servers, Restricted Data, administrative planes, and Internet-facing workloads.	CM-2, CM-6, CA-7	☐ Yes ☐ Partial ☐ No ☐ N/A
SC-02	Remove default credentials and unnecessary software, services, accounts, ports, protocols, and management interfaces; monitor configuration drift.	CM-6, CM-7, CM-8	☐ Yes ☐ Partial ☐ No ☐ N/A
SC-03	Encrypt non-public Citadel Data at rest and in transit, including databases, object storage, snapshots, replicas, backups, and administrative sessions using AES256.	SC-8, SC-12, SC-13, SC-28	☐ Yes ☐ Partial ☐ No ☐ N/A
SC-04	Use MFA and separate administrative identities; restrict management interfaces by source, network, and role; segment production, development, test, backup, and management functions according to risk.	AC-6, IA-2, SC-7	☐ Yes ☐ Partial ☐ No ☐ N/A
SC-05	Centralize and protect audit, security, administrative, authentication, and data-access logs; monitor material events and preserve evidence.	AU-2, AU-6, AU-9	☐ Yes ☐ Partial ☐ No ☐ N/A
SC-06	Perform authenticated vulnerability scanning where practicable, apply risk-based remediation, and use workload protection or EDR where supported.	RA-5, SI-2, SI-3, SI-4	☐ Yes ☐ Partial ☐ No ☐ N/A
SC-07	Use documented secure development, code review, dependency monitoring, secrets management, testing, release approval, rollback, component inventory, and SBOM practices when applicable.	SA-11, SA-15, SR-4, SI-7	☐ Yes ☐ Partial ☐ No ☐ N/A
SC-08	Protect backups against unauthorized alteration or deletion and test restoration, resilience, and service recovery after material changes.	CP-9, CP-10, SI-13	☐ Yes ☐ Partial ☐ No ☐ N/A

6. Required Evidence

Security Review and Cooperation. The Citadel may evaluate the Offeror's compliance before award and during contract performance by reviewing relevant documentation, requesting clarifications, conducting meetings or demonstrations, requiring remediation plans, or obtaining other evidence proportionate to the risk and scope of the service. The Offeror shall cooperate with reasonable security, privacy, records, legal, audit, and regulatory inquiries relating to Citadel Data or the contracted service. Any review by The Citadel does not relieve the Offeror of responsibility for compliance or transfer responsibility for the Offeror's controls to The Citadel.

The Citadel may require evidence proportionate to the risk, data sensitivity, architecture, and scope of the proposed product or service. Evidence may include: (1) governance and assurance materials, including security and privacy program documentation, independent assurance reports, and a tailored NIST SP 800-53 control crosswalk; (2) architecture and data-governance materials, including data-flow diagrams, data locations, subprocessors, and artificial-intelligence use disclosures; (3) technical-control evidence, including CIS Benchmark assessment results and documentation of encryption, endpoint or workload protection, patching, logging, and device management; (4) testing and resilience evidence, including vulnerability or penetration-test summaries, incident-response procedures, continuity plans, and restoration-test results; and (5) software supply-chain evidence, including an SBOM when applicable. Evidence shall be current, relevant to the proposed solution, sufficient to validate the Offeror's response, and provided within the time specified by The Citadel. The Offeror may identify legitimately confidential material and propose reasonable handling protections, but confidentiality designations do not excuse the Offeror from providing evidence required for evaluation, award, or contract oversight.

ID	Evidence Category	Status / Reference
E-01	Security, privacy, assurance, and tailored NIST control-alignment materials	☐ Included ☐ Upon request ☐ N/A
E-02	Architecture, data flow, processing locations, subprocessors, and AI-use disclosure	☐ Included ☐ Upon request ☐ N/A
E-03	CIS assessment, encryption, EDR or workload protection, patching, logging, and device-management evidence	☐ Included ☐ Upon request ☐ N/A
E-04	Vulnerability or penetration testing, incident response, continuity, and restoration testing	☐ Included ☐ Upon request ☐ N/A
E-05	Software supply-chain evidence, component inventory, and SBOM when applicable	☐ Included ☐ Upon request ☐ N/A

7. Exceptions and Compensating Controls

Exception Field	Offeror Response
Requirement ID(s)	
Affected service/ system	

Reason full compliance is not feasible	
Risk and compensating controls	
Evidence, owner, and remediation date	
Requested expiration	

Exception Review. Submission of an exception does not constitute acceptance by The Citadel. The Citadel may reject the exception, request clarification or additional evidence, require compensating controls, establish remediation milestones, condition an award on resolution, or determine that the exception makes the proposal unacceptable. An exception is effective only when expressly accepted in writing by an authorized Citadel representative and incorporated into the applicable solicitation, award, contract, or purchase order.

Continuing Compliance and Material Changes. The Offeror shall maintain compliance throughout proposal evaluation and, if awarded, throughout contract performance. The Offeror shall promptly notify The Citadel of any material change affecting the security, privacy, architecture, ownership, hosting location, subprocessors, artificial-intelligence functionality, certifications, or control environment of the proposed or contracted product or service. The notice shall describe the change, its effective date, the resulting risk, and any planned mitigation. The Citadel may require additional evidence, compensating controls, remediation, or an updated security review.

8. Offeror Certification, Continuing Obligations, and Order of Precedence

By signing below, the authorized representative certifies that the Offeror has reviewed this Addendum; that the responses and supporting materials are accurate, complete, and current to the best of the representative's knowledge; that all requested exceptions have been disclosed; and that the Offeror will promptly disclose any material change occurring before award or during contract performance. If the Offeror receives an award, the Offeror agrees to comply with the applicable requirements except to the extent that The Citadel expressly accepts a written exception and incorporates it into the resulting contract or purchase order.

Order of Precedence. If this Addendum conflicts with another technology, cybersecurity, privacy, data-use, or secure-configuration requirement in the solicitation or resulting agreement, the more protective requirement applies unless The Citadel expressly states otherwise in writing. An accepted exception applies only to the requirement and scope identified in the written acceptance.

Certification Field	Offeror Entry
Legal name	
Authorized representative / title	
Signature / date	
Security contact / title	
Security contact email / phone	

VENDOR RESPONSE CHECKLIST

Submit with the Offeror response when this Addendum applies.

Solicitation / Offeror Information	Entry
RFP / Solicitation No.	
Offeror legal name	
Proposed product or service	
Completed by / title	
Date	

Instructions: Complete every checklist item and identify the corresponding requirement ID or supporting attachment. Mark each item Yes, Partial, No, or N/A. Every Partial, No, or N/A response must include an explanation and supporting reference, and each requested deviation must be documented in the Exceptions and Compensating Controls section. Attach additional pages when necessary and label each attachment with the applicable requirement ID.

#	Checklist Item	Offeror Confirmation	Response	Reference / Explanation
1	Applicability	We identified whether the service accesses Citadel systems or creates, receives, stores, processes, transmits, or disposes of Citadel Data.	☐ Yes ☐ Partial ☐ No ☐ N/A	
2	Data use	We accept the authorized-use, confidentiality, ownership, minimum-necessary, FERPA, regulated-data, and prohibited-use requirements.	☐ Yes ☐ Partial ☐ No ☐ N/A	
3	Artificial intelligence	We disclosed all AI use and accept the restrictions on unapproved AI services and model training involving Citadel Data.	☐ Yes ☐ Partial ☐ No ☐ N/A	
4	Locations and subprocessors	We disclosed processing, storage, backup, support, remote-access countries, and all applicable subprocessors.	☐ Yes ☐ Partial ☐ No ☐ N/A	
5	Access security	We use unique identities, least privilege, prompt termination, separate administrative accounts, and MFA where required.	☐ Yes ☐ Partial ☐ No ☐ N/A	
6	Encryption	We encrypt non-public Citadel Data in transit and at rest, including endpoints, servers, databases, removable media, backups, snapshots, and replicas.	☐ Yes ☐ Partial ☐ No ☐ N/A	
7	Hardening baseline	We apply the current applicable CIS Benchmark: Level 1 minimum for standard endpoints and Level 2 where required by the Addendum.	☐ Yes ☐ Partial ☐ No ☐ N/A	
8	Endpoint/server controls	We maintain supported platforms, managed EDR or workload protection, host firewalls, secure configuration, patching, logging, and configuration monitoring.	☐ Yes ☐ Partial ☐ No ☐ N/A	
9	Secure development	Where applicable, we use secure development, dependency monitoring, secrets management, testing, release approval, rollback, component inventory, and SBOM practices.	☐ Yes ☐ Partial ☐ No ☐ N/A	
10	Continuity	We protect backups, define recovery objectives, maintain continuity procedures, and test restoration and service recovery.	☐ Yes ☐ Partial ☐ No ☐ N/A	
11	Incident notification	We accept immediate notification and the 24-hour contractual reporting requirement for suspected Security Incidents affecting Citadel Data or services.	☐ Yes ☐ Partial ☐ No ☐ N/A	
12	Monitoring and remote work	We disclosed monitoring tools and accept restrictions on screenshots, keystrokes, webcam, and session recording involving Citadel systems or data.	☐ Yes ☐ Partial ☐ No ☐ N/A	
13	Return and deletion	We accept access revocation, data return, and deletion or approved-retention certification within 30 days, subject to legal holds and required retention.	☐ Yes ☐ Partial ☐ No ☐ N/A	

14	Evidence	We can provide requested security evidence, including applicable assurance, architecture, CIS assessment, encryption, EDR, patching, incident-response, recovery, AI, and SBOM materials.	☐ Yes ☐ Partial ☐ No ☐ N/A	
15	Exceptions	We listed every requested exception and documented affected scope, risk, compensating controls, evidence, owner, remediation date, and requested expiration.	☐ Yes ☐ Partial ☐ No ☐ N/A	
16	Certification	An authorized representative completed and signed the certification below.	☐ Yes ☐ Partial ☐ No ☐ N/A	

Certification

Authorized Representative	Title	Signature	Date