Attachment A

to

RFP No. 4541

Alcorn State University (ASU)

VIDEO SURVEILLANCE SYSTEM
AND EQUIPMENT

ITS Project No. 47396

TABLE OF CONTENTS

I. GENERAL

A. How to Respond

1. Beginning with Item 17, label and respond to each outline point in this Attachment A as it is labeled.
2. The State is under the impression that Vendors have read and agree to all items in this RFP. Vendors should take exception to items to which they disagree.
3. The Vendor must respond with "WILL COMPLY" or "EXCEPTION" to each point in this section. In addition, many items in this RFP require detailed and specific responses to provide the requested information. Failure to provide the information requested will result in the Vendor receiving a lower score for that item, or, at the State's sole discretion, being subject to disqualification.
4. "WILL COMPLY" indicates that the Vendor can and will adhere to the requirement. This response specifies that a Vendor or vendor's proposed solution must comply with a specific item or must perform a certain task.
5. If the Vendor cannot respond with "WILL COMPLY", then the Vendor must respond with "EXCEPTION". (See Section V of RFP No. 4541, for additional instructions regarding Vendor exceptions.)
6. Where an outline point asks a question or requests information, the Vendor must respond with the specific answer or information requested.
7. In addition to the above, Vendor must provide explicit details as to the manner and degree to which the proposal meets or exceeds each specification.
8. Certain items in the technical specifications of this RFP are MANDATORY. Vendors are specifically disallowed from taking exception to these mandatory requirements, and proposals that do not meet all mandatory requirements are subject to immediate disqualification.

B. Overview and Background

9. Alcorn State University (ASU) is a historically black public land-grant university, founded in 1971, with its main campus at Lorman and two additional campuses at Natchez and Vicksburg, Mississippi. The University's current security architecture and video surveillance system includes the operation of multiple video surveillance systems using a combination of analog and IP based cameras that utilize a combination of coaxial and Cat5E network connections. The current video management system is generic and is accomplished through accessing individual DVRs for each independent system.

C. Procurement Goals and Objectives

10. ASU desires to upgrade this component of the University's security architecture by upgrading and replacing its existing camera system and enhancing location coverage on the University's three campuses. It is anticipated that the project will entail installation of a new video/surveillance management system, as well as replacement of existing cameras, installation of cameras at new locations not presently covered on all three campuses, management software and turnkey installation services for all associated hardware and software necessary for this type of project. 'Attachment B' to this RFP provides a detailed list of locations where cameras are to be replaced and

where new cameras are required, while ‘Attachment C’ contains the floor plans for the areas where cameras and equipment are required.

a. **MANDATORY** - Vendors must attend the Onsite Vendor Conference and Walk Through (ASU and Natchez campuses) on January 24, 2024, at 8:30 a.m. Central Time. The walking tour will start at ASU campus (address 1000 ASU Drive, 6th Floor Conference Room, Administration Building, Lorman, MS 39096). The tour will continue to the Natchez campus after lunchtime.

b. To attend the mandatory onsite vendor conference and walk through, Vendors must contact the Solicitations Team via email no later than Tuesday, January 23, 2024 at 12:00 p.m. Central Time to receive instructions.

D. Statement of Understanding

11. Throughout this document, references to *this RFP* will mean RFP No. 4541, including Attachment A to RFP 4541, and all accompanying exhibits and appendices.

12. Unless otherwise specified, throughout this document, references to *Customer* will mean Alcorn State University (ASU).

13. Unless otherwise specified, throughout this document, references to the *State* can be used interchangeably to represent the State of Mississippi, the *Customer*, and/or the State of Mississippi Department of Information Technology.

14. Unless otherwise specified, throughout this document, references to *the proposed solution* will represent the collective services, system, or solution(s) being sought by the State.

15. Unless otherwise specified, Vendors should expect to find the Section VIII, Cost Information Submission form in RFP No. 4541, rather than in this Attachment A document.

16. Unless otherwise specified, Vendors should expect to find Section IX reference forms in RFP No. 4541, rather than in this Attachment A document.

E. Vendor Qualifications

17. Vendor must be capable of and have previous experience in developing and implementing projects of similar size and scope. At least two of the vendor references submitted under Section IX of RFP No. 4541 must validate/substantiate this experience.

18. Vendor must have been in the business of providing such solutions for at least the last three years.

19. Vendor must provide an introduction and general description of its company's background and years in business providing such services.

20. Vendor must specify the location of the organization's principal office and the number of executive and professional personnel employed at this office.

21. Vendor must specify the organization's size in terms of the number of full-time employees, the number of contract personnel used at any one time, the number of offices and their locations, and structure (for example, state, national, or international organization).

22. Vendor must disclose any company restructurings, mergers, and acquisitions over the past three (3) years and/or any planned, future restructures or mergers.

23. Vendor headquarters must be located in the United States and must provide U.S. based customer support.

F. Vendor Implementation Team

24. Vendor must demonstrate that all team members have the necessary experience for development, configuration, implementation, testing, user training, maintenance and support of the services required by this RFP. At a minimum, Vendor response should include team member roles, functional responsibilities, and experience with projects similar in size and scope to the services required by this RFP.

25. Identify the participating key staff members who will be responsible for the execution of the various aspects of the project, including but not limited to: Project Manager, and Technical Architect(s).

26. For each participating key staff member, provide a summary of qualifications, years of experience, and length of employment with your company.

27. Vendor must ensure that each team member assigned to this project is able to communicate clearly in the English language both verbally and in written form.

II. FUNCTIONAL/TECHNICAL REQUIREMENTS

B. General Requirements for the System and Equipment Upgrade Project

28. Provision of a video management system, including applications, video processing, and storage servers, required to fully support HD image resolution, video retention requirements and policy-based administrative oversight for all cameras.

29. Replacement of approximately 23 existing cameras and the addition of 164 cameras.

30. Expansion of system monitoring capability to include 120 Wisenet SNV-L6014RM cameras deployed by ASU in 2019, and if not feasible, replacement of the said cameras with others that meet system requirements.

31. Implementation of connectivity to provide transport of camera data from each camera location, back to the IDF, MDF and assigned POE capable switches for transmission to central video processing, storage array and management stations.

32. De-installation and mining of existing cameras, and camera cabling, coax, and other wiring supporting old devices.

33. Provision of CISCO POE+ (Power-over-Ethernet) switches to serve all camera locations.

34. Architectural design and provision of furniture and all technology required to build out a video surveillance control room within the ASU Police Department building.

35. Re-cabling and configuration of all offices within the Police department to support improved network connectivity to enable access, viewing, and monitoring of video surveillance and performance of daily duties.

36. Three (3) years Extended Support and Maintenance Plan.

37. Vendor must provide a listing of all services and materials to be provided by the Vendor and any services or materials that must be provided by the University.

38. Vendor shall provide the requirements and specifications for the type of server(s) required and how many cameras each server can be expected to support if the number of cameras per server system is limited.

39. Surveillance System Security - Considering recent events where the Internet of Things (IOT) type devices were used to create a Distributed Denial of Service attack, the network must have a design with functionality that attempts to prevent this type of cyber threat. Please respond and provide your approach to Network Security for the surveillance camera network. Highlight proposed equipment capability and features that minimize vulnerability to hacking.

C. Video Management System Capabilities and Specifications

40. The system shall operate in a Microsoft Windows environment. It shall be an IT server-based solution either purpose-built or VM, for the capture, processing, storage and retrieval of digital video and supporting audio, alarm, associated systems (access control, etc.), and other surveillance data.

41. The (VMS) can be premise or cloud based or a combination of the two.

42. The VMS shall provide direct support of IP-based video sources and operate on stand-alone or integrated host and storage platforms from standard IT industry suppliers. This hardware independence shall allow the host and storage platforms to be sourced from the VMS manufacturer, an integrator certified by the VMS manufacturer or supplied by the customer for optional loading and certification by the VMS manufacturer at the manufacturer’s facility.

43. The VMS shall capture video, audio, alarm, associated systems and other data from a single or multiple servers.

44. The VMS shall support all leading industry-standard compression formats including Motion JPEG, MPEG-4, H.264 and H.265.

45. The VMS shall simultaneously handle recording, archiving, retrieving, playback and live distribution of video and audio. The software shall operate in a continuous recording mode or according to a programmed time/date schedule. Recording functions may also be triggered by events and motion detection. Video shall be captured in such a way as to provide seamless support of multiple, disparate video source technologies transparent to the user and allowing for the integration of new capture technologies as they become available.

46. The VMS shall be capable of exporting video clips or images to CD/DVDs without third party software. All images and video file export shall include an executable player that verifies no tampering has occurred and can be played on standard PC’s.

47. The VMS shall be capable of integrated operation with other security related systems such as Access Control Systems (ACS) and Video Analytics Systems (VAS) or applications.

48. Video servers specified shall be capable of supporting up to 8 mega-pixel resolution per camera and up to 30 Frames per Second (FPS).

49. VMS Server shall be capable of interfacing with MJPEG, Microsoft MPEG-4, ISO MPEG-4, H.264 and H.265 compressions.

50. Separate, programmable event and motion detection settings shall be provided per video input.

51. The VMS shall be compatible with IT backup software and not require a proprietary “archiving” function for management of stored video files. Compatible IT backup software shall include these features: a. Locked file support b. Ability to duplicate files and folders c. Backup without encryption and compression d. Deletion of original files after backup.

52. The VMS shall include a built-in archiving feature for the purpose of moving recordings from their original storage volume to a different local or network- attached storage volume on an administrator-defined schedule.

53. Edge storage integration shall allow the VMS to synchronize any recordings missing on the VMS server as a result of network outage or other event preventing communication between the camera and VMS. The synchronization of missing recordings shall occur automatically when the connection to the VMS server or camera is restored.

54. The VMS shall provide a stable recording environment via a modular video storage and data management architecture to minimize common database corruption situations. The VMS system shall be expandable by adding additional video servers and storage.

55. The VMS shall provide the system administrator with the tools to monitor the overall system health, individual camera status, video archive usage and status plus other elements of every server in the Enterprise system.

D. Video Analytics

56. The VMS shall support video analytics. Vendor shall provide a summary of how the proposed system/solution addresses the below items. The list may not be all inclusive please elaborate on any items that should be considered.

57. *Directional Motion* – when motion is detected in a specific direction, an alarm is triggered. Users have wide flexibility in defining areas of interest and activity thresholds to minimize false alarms.

58. *Adaptive Motion* – advanced motion detection behavior calibrates to scene conditions, allowing the system to distinguish targets from other movement in a scene, such as headlight glare, leaves blowing, a flag flying or snow falling. It is ideal for identifying people and vehicles in parking lots and perimeter detection with such outdoor conditions.

59. *Vibration Removal* – reduces video shake in applications where cameras are subject to vibration, providing a clear picture despite camera shake. Ideal for external cameras with long focal lengths, pole-mounted cameras and an array of other applications.

60. *Object Removal* – alarm triggers when a stationary object, such as a piece of art, is removed from a selected scene. This analytic behavior allows the user to define an object or area of interest in a scene. Motion is allowed in the protected zone, but if an object is removed, an alarm is triggered.

61. *Object Counting* – this behavior counts objects when motion is detected in a specific direction. Users have a wide flexibility in defining areas of interest and activity thresholds. An alarm is generated when the threshold is exceeded. Ideal for counting cars in a parking garage or counting visitors entering/exiting a high-risk department or other similar situation.

62. *Camera Sabotage* – advanced video loss detection recognizes when video has been compromised. For example, if a vandal paints or covers a lens, or reaches to move a fixed camera away from an intended scene, an alarm is triggered.

63. *Abandoned Object* – an alarm triggers when a stationary object appears and remains in a scene, such as a person setting down a backpack in the main lobby. This behavior allows the user to define an object or area of interest in a scene. Motion is allowed in the protected zone.

64. *Loitering Detection* – when people or vehicles remain in a defined zone longer than the user-defined time allows, an alarm is activated. This behavior is effective in real-time notification of suspicious behavior around pharmacy departments, ATMs, narcotic dispensaries and other locations.

65. *Stopped Vehicle* – vehicles stopped near a sensitive area longer than the user-defined time allows are detected. This behavior is ideal in loading and receiving docks, parking enforcement, and vehicles waiting at parking gates.

66. *Auto Tracking* – Pan/tilt/zoom capability to track vehicles or humans entering or stopping in user-defined zones. Once identified, the camera locks on and follows the subject's path. This analytic is best for building perimeters.

E. Surveillance System Servers

67. Vendors are requested to provide the specifications for server and hardware required to support cameras and the storage requirements for the surveillance system and shall propose provisioning the server and network hardware as part of the pricing proposal.

68. Storage policy to estimate hardware requirements for video storage capacity should be based on a single copy of a minimum of 31 days, 24 hours per day, per camera provisioned.

III. CAMERA REQUIREMENTS AND SPECIFICATIONS

A. Indoor Camera Specifications

69. General: The camera shall:

    a. Be designed to provide streams up to 2560x1920 pixels resolution at up to 30 frames per second using H.265 encoding and provide video streams in HDTV 1080p (1920x1080) at up to 30 frames per second using H.265 encoding.

    b. Be equipped with Day/Night functionality.

    c. Be manufactured with a vandal-resistant casing or dome and support operation between -20 to +55C (-40 to +131F).

70. Hardware: The camera shall:

    a. Use a high-quality IR-sensitive progressive scan megapixel sensor.

    b. Be equipped with a removable IR-cut filter, providing so-called day/night (color/B&W) functionality.

    c. Be equipped with high-quality lens that provides automated iris functionality.

    d. Provide pictures down to 0.2 lux while in day mode/color (with IR-filter in use) and down to 0.04 lux while in night mode/B&W F1.2 (with IR-filter removed).

e. As an option, the camera may support memory expansion by providing an available SD/SDHC card slot.

71. Video

a. Resolution: The camera shall:

i. Be able to deliver full resolution video (2560x1920 pixels) at 15 frames per second.

ii. Be able to deliver full frame rate HDTV 1080p video over IP networks. Supported video resolutions shall include:

1. 1920x1080 (HDTV 1080p).

2. 2560x1920.

3. The camera shall be able to provide both landscape format (4:3 and 16:9 aspect ratio) as well as corridor format (3:4 and 9:16 aspect ratio).

b. Encoding: The camera shall:

i. Support Baseline Profile H.265 encoding with motion estimation in a selectable range from 1 up to 30 frames per second in all resolutions up to 2560x1920 pixels.

ii. Support Baseline Profile H.265 encoding with motion estimation in up to 30 frames per second in HDTV 1080p (1920x1080 resolution).

iii. Support Main Profile H.265 encoding with motion estimation and context adaptive binary arithmetic coding (CABAC) in a selectable range from 1 up to 30 frames per second in all resolutions up to 2560x1920 pixels.

iv. Support Main Profile H.265 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 30 frames per second in HDTV 1080p (1920x1080 resolution).

v. Be capable of providing independently configured simultaneous H.265 and Motion JPEG streams.

vi. Support both Constant Bit Rate (CBR) and Variable Bit Rate (VBR) in H.265.

vii. Camera must be Embedded with self-learning video analytics, be ONVIF Profile S and Profile T Compliant.

c. Image control: The camera shall:

i. Be equipped with an electronic shutter operating in the range 1/6 to 1/28 second, and manually defined exposure zones.

ii. Be equipped with Wide Dynamic Range functionality.

72. Functionality

a. The camera shall be equipped with an integrated event functionality, which can be triggered by:

i. External input.

ii. Audio Detection.

b. Response to triggers shall include:

i. Activating external output.

ii. Recording to local storage if provisioned.

c. The camera shall provide memory for pre & post alarm recordings.

d. Event functionality shall be configurable via a web interface.

e. Multi-view streaming: The camera shall allow for at least 8 individual and selectable areas of the image to be cropped out and made available as individual video streams.

73. Interfaces

a. Inputs/Outputs

i. The camera shall be equipped with one (alarm) input and one output, accessible via terminal block. This input shall be configurable to respond to normally open (NO) or normally closed (NC) dry contacts.

ii. Audio -The camera shall be equipped with one 3.5 mm jack for line/mic input and one 3.5 mm jack for line output.

iii. Optional: Local recording capabilities and/or slots for local storage capacity can be included as an option.

74. Enclosure: The camera shall:

a. Include Level 1 Vandal-resistant casing with clear transparent cover/dome.

b. Have IP66-rating.

c. Have NEMA 4X-rating.

B. Outdoor Camera Specifications

75. General: The camera shall:

a. Be a Fixed Day and Night Full HD Color IP Camera.

b. Be designed to provide streams up to 2560x1920 pixels resolution at up to 15 frames per second, using H.265 or Motion JPEG and provide video streams in HDTV 1080p (1920x1080) at up to 30 frames per second using H.265 or Motion JPEG.

c. Be equipped with Day/Night functionality.

d. Be manufactured with an all-metal body and a vandal-resistant casing and support operation between -40 to +55C (-40 to +131F).

e. Be IP66 and NEMA 4X-rated.

76. Hardware: The camera shall:

a. Be provided with a sun shield.

b. Use a high-quality IR-sensitive progressive scan megapixel sensor.

c. Be equipped with a removable IR-cut filter, providing day/night (color/B&W) functionality.

77. Video

a. Resolution: The camera shall:

i. Be able to deliver full resolution video (2560x1920 pixels) at 15 frames per second.

ii. Be able to deliver full frame rate HDTV 1080p video over IP networks.

iii. Supported video resolutions shall include:

1. 1920x1080 (HDTV 1080p).
2. 2560x1920.
3. The camera shall be able to provide landscape format (16:9 aspect ratio).

b. Image control: The camera shall:

i. Be equipped with an electronic shutter operating in the range 1/6 to 1/28 second, and manually defined exposure zones.

ii. Be equipped with Wide Dynamic Range functionality.

c. Encoding: The camera shall:

i. Support Baseline Profile H.265 encoding with motion estimation in a selectable range from 1 up to 30 frames per second in all resolutions up to 2560x1920 pixels.

ii. Support Baseline Profile H.265 encoding with motion estimation in up to 30 frames per second in HDTV 1080p (1920x1080 resolution).

iii. Support Main Profile H.265 encoding with motion estimation and context adaptive binary arithmetic coding (CABAC) in a selectable range from 1 up to 30 frames per second in all resolutions up to 2560x1920 pixels.

iv. Support Main Profile H.265 encoding with motion estimation and context-adaptive binary arithmetic coding (CABAC) in up to 30 frames per second in HDTV 1080p (1920x1080 resolution).

v. Be capable of providing independently configured simultaneous H.265 and Motion JPEG streams.

vi. Support both Constant Bit Rate (CBR) and Variable Bit Rate (VBR) in H.265.

vii. Be Embedded with self-learning video analytics, be ONVIF Profile S and Profile T Compliant.

viii. Provide memory for pre & post alarm recordings.

ix. Event functionality shall be configurable via a web interface.

x. Multi-view streaming: The camera shall allow for at least 8 individual and selectable areas of the image to be cropped out and made available as individual video streams.

78. Interfaces

a. Inputs/Outputs

i. The camera shall be equipped with one (alarm) input and one output, accessible via a removable terminal block. This input shall be configurable to respond to normally open (NO) or normally closed (NC) dry contacts.

79. Enclosure: The camera shall:

a. Be all-metal body providing encapsulated electronics.

b. Have Hardened or vandal-resistant casing.

c. Be IP66 standard rated.

d. Be NEMA 4X rated.

e. Have impact resistance according to IK10 standard.

f. Include thermostat, heater and fan inside the enclosure.

g. Have dehumidifying membrane/methodology.

h. Have a removable weather shield.

C. Camera Horizontal Cabling

80. The horizontal cabling required to support the project shall be based on Cat 6 (Type 2) network cabling supporting POE+ capable Ethernet switches and devices. Each run will be terminated at the device cable termination end in an RJ45 modular jack and at the Wiring Closet IDF/MDF end in an RJ45 Modular Patch Panel port. Vendor shall provide RJ-45 termination patch panel meeting Cat 6 or greater standard. The University will provide rack space for each IDF. Bidder is responsible for providing evidence that all materials and installation practices will meet or exceed BICSI specifications for CAT6 (minimum) or greater compliance for materials and installation.

81. The locations detailed for camera placement, with some exceptions, do not have existing UTP cabling or cable path. Cameras to be replaced are moving from coaxial analog connectivity to IP based connectivity. The existing IP based cameras to be replaced do have installed UTP cabling but in some cases may not meet current standards and should be upgraded to support a uniformed installation if required to be replaced. ASU is requesting that vendors provide a proposal with pricing to establish wire pathways and implement a UTP based connection from camera to IDF patch panel for each camera install.

D. Building Cabling Environment

82. Each of the ASU building facilities represents a unique cable installation environment.

83. Replacement camera locations must be field verified to ensure the new camera is stable and vandal resistant.

84. Some of the buildings’ walls are hard surfaces and the ceiling is a metal grid. There is no ability to route cabling in walls.

85. Ceiling grid may be removed to route camera cabling. New camera locations must either be attached to ceiling grid or have anchors set into the concrete for backbox and/or mounting plate. Wall mounted devices must be served with surface mount wireway, wire mold, or closed or covered wire path providing support for new cabling. No exposed cabling in the wire path will be permitted.

86. For each existing camera location to be replaced as a part of this upgrade project, the vendor is required to mine and remove existing cabling and coax to that location.

E. POE + Network Switch Infrastructure

87. Hardware

a. CISCO® based hardware, rack-mounted 10/100/1000 POE Ethernet switch maximizing POE+ concurrent port utilization (100% concurrent port utilization at 30W per port desired); 300 series, 550x MPP series or 3650 series typical.

b. Capability to provide 802.3at type 2 (30W) per port capable across all ports.

c. Voltage range per port, 50 to 57 V.

d. Per port power management – auto-negotiated.

e. Camera ports, RJ-45 supporting Cat 6 infrastructure.

f. SFP/uplink ports, 10GigE/1GigE capable, supporting fiber optic connectivity for backhaul consolidation or fiber links to cameras beyond Ethernet UTP limitations.

g. 19” Rack mountable.

88. Supported Standards

a. IEEE 802.3 10-BASE-T, Ethernet.

b. IEEE 802.3u 100-BASE-TX, Fast Ethernet.

c. IEEE 802.3ab 1000BASE-T, Gigabit Ethernet.

d. IEEE 802.3ae-2002 10000Base, 10 Gigabit Ethernet.

e. IEEE 802.3x Flow Control (full-duplex flow control).

f. IEEE 802.3af Power over Ethernet (PoE).

g. IEEE 802.3at Power over Ethernet Plus (PoE+).

h. Optional: IEEE 802.3az Energy-Efficient Ethernet.

89. Security

a. Access IEEE 802.1x Port-Based network access control protocol.

b. RADIUS users access authentication.

c. L3 / L4 Access Control List (ACL).

d. Source IP-MAC / Port-Binding.

e. Port Security for Source MAC address entries filtering.

90. Management

a. Full Web-based configuration and management capability.

b. SNMP support (Public and Private MIBs).

IV. POLICE DEPARTMENT BUILDING UPGRADE REQUIREMENTS AND SPECIFICATIONS

A. Control Room

91. Build out of a video surveillance monitoring room within the Police Department building. The current room has a two-tier work desk with a single desktop computer. Contractor shall design and provide furniture and all technology required to build out a video surveillance control room within the ASU Police Department building room.

B. Cabling Upgrade

92. Re-cabling of all offices within the Police Department to support improved network connectivity and enable access, viewing, and monitoring of video surveillance and

performance of daily duties. The horizontal cabling required to support the project shall be based on UTP Cat6 network cabling supporting POE+ capable Ethernet switches and devices. Each run will be terminated at the device cable termination end in an RJ45 modular jack and at the Wiring Closet IDF/MDF end in an RJ45 Modular Patch Panel port. Vendor shall provide RJ-45 termination patch panel meeting Cat 6 or greater standard. The University will provide rack space for each IDF. Vendor is responsible for providing evidence that all materials and installation practices will meet or exceed BICSI specifications for CAT6 (minimum) or greater compliance for materials and installation. Each data location will at a minimum require two connections to support a computer and phone line. Wireless access point locations will require a single data connection terminated on a RJ45 modular jack.

V. WARRANTY AND MAINTENANCE

93. Warranty

    a. The Surveillance Camera Upgrade Project must include a minimum of 1 year warranty period for all components of the VMS, camera and cabling.

    b. Where manufacturer warranties extend beyond 1 year, warranty periods for those components must be identified and the extended warranty period supported by the proposed maintenance plan.

94. Maintenance

    a. ASU requires 3-years support and onsite maintenance with the option to continue annual support after the 3-year period has ended. The vendor should provide a detailed description of standard and extended support, maintenance, and the estimated response time for support requests.

    b. Proposed maintenance plans should be accompanied by proposed costs for hardware replacement following the initial warranty period.

95. Software Updates and Releases

    a. Software updates and releases must be included and supported as a component of the maintenance plan. Maintenance plans may differentiate software release criticality but must indicate planned upgrade schedule from release to implementation.

96. Help Desk

    a. Vendors must identify the help desk, technical support and software support capabilities available.

    b. Manufacturer support services and levels of service available to ASU must be identified and detailed as part of the vendor proposal.

    c. Vendor provided services, on-site support, configuration, or fault isolation capabilities augmenting manufacturer service offered should be defined and detailed in the proposal.

VI. IMPLEMENTATION REQUIREMENTS

A. Vendor Acknowledgement

97. Upon award, Customer intends for the requirements set forth in this section, and the responding Vendor’s proposal, including any subsequent, agreed upon provisions and revisions, to act as the Implementation Statement of Work.

98. The Vendor shall provide all engineering and design documents necessary for any permitting process.

99. The Vendor shall identify all agencies with permitting responsibility and present the engineering documentation.

100. ASU will be available to provide assistance with the permitting process should a meeting with a board or council require their presence.

B. Project Management

101. Contractor must maintain a single point of contact/jobsite supervisor at all times. This person must be designated, and their contact information should be listed in the proposal response.

102. A daily work log must be maintained at the job site and be available for review by ASU at any time. Contractor must coordinate with ASU so that residents can be notified/moved appropriately.

103. Vendor must submit, as a part of its proposal, a high-level Project Work Plan that outlines the overall strategy and approach to providing the requested system and services. The Plan must contain all significant work steps required for provision of the requested services. Timeframes must be specified in terms of workdays or weeks after contract signing. The Plan must include the elements listed below:

a. The Plan must incorporate all tasks to be accomplished;

b. The Plan must address all project deliverables, including implementation, acceptance testing, schedule for actual testing and go-live date;

c. The Plan must include resource estimates for both the Agency and Vendor timelines; and

d. The Plan must address assumptions that the Vendor has made based on the information rendered in these specifications.

104. Upon contract award, the Vendor's Project Manager must work with ASU to develop a more detailed Project Work Plan to guide the project's implementation.

105. The State anticipates that there may be a need for additional modifications after system implementation. In addition to an off-site hourly rate, Vendor must include a fully loaded on-site change order rate as a separate line in the Vendor's Cost Information Submission, Section VIII of RFP No. 4541. The Vendor must describe its change order and staffing strategy under the circumstances in 103 and 104 below.

106. The Vendor must describe its change order and staffing strategy when a customer requires additional functionality that may be within the capability of the proposed system's existing programming, after the initial system acceptance.

107. The Vendor must describe its change order and staffing strategy when a customer requires additional functionality that may require modification of the proposed system's programmed code and/or the addition of new programming, after initial system acceptance.

C. Installation

108. The Vendor must follow all manufacturer documentation for System Installation.

109. Vendor's staff must present their corporate ID or other acceptable credentials to ASU security to enable access to the project sites and work area locations.

D. User Training and Documentation

110. The Contractor shall provide a minimum of sixteen (16) hours of instruction and training. The training shall be provided onsite and shall include the operation of the system and its maintenance. The instruction shall be broken down into four (4) hour blocks of time.

111. The Contractor shall work with ASU to develop an outline of training topics. This outline shall be approved by ASU prior to the start of any training sessions.

112. All onsite training will be coordinated with a University Representative. Training shall take place at an ASU facility.

113. The Contractor shall provide documents certifying that all training has been provided. Documents shall include, but not be limited to, meeting agendas and topics covered, sign-in sheets, letters signed by an authorized University representative that training did occur.

114. The University intends to eventually be a self-maintainer of the VSS with direct access to manufacturer support. Descriptions and costs for additional required training, training material, and/or certifications shall be included in the proposal to achieve this goal. Elements of the proposed solution that do not provide for self-maintenance and/or direct access by the University to manufacturer support and maintenance should be clearly identified.

VII. FINAL ACCEPTANCE REVIEW – TESTING AND ACCEPTANCE

115. Vendor agrees that upon the successful completion of all implementation phases, including end user training, Customer will conduct a Final Acceptance Review (FAR) to determine whether Vendor has satisfied the terms and conditions of the awarded contract, which includes the requirements of this RFP No. 4541, Attachment A.

116. All equipment and software must be tested according to Manufacturer's instructions.

117. ASU must conduct testing of the System once the System is made available for use to ASU and all training is completed.

118. The Vendor must participate in the acceptance testing of the System by providing technical staff on-site for assistance in demonstrating the functions of the installed System. ASU must be in a position to demonstrate that the System is operational to ensure that proper training has been received and sufficient knowledge transfer has been accomplished.

119. As part of the System testing, the Vendor must assist ASU in a performance test to confirm that the system configuration possesses adequate capacity and speed to drive the CCTV Security System and user base without degradation.

120. ASU will communicate to the Vendor regarding any deficiencies identified during either system or performance testing. The Vendor must correct deficiencies within five (5) days of written notice given by ASU. The Vendor must bear the cost to remedy reported deficiencies. These deficiencies must be corrected and tested by the Vendor before submitting the remedy to the Agency for final system acceptance.

121. The Vendor must agree to and allow for a final testing/acceptance period of up to thirty (30) business days from the initiation of system testing and correction of any deficiencies reported by the State.

122. System testing is finished when ASU has successfully completed all acceptance testing as defined by the Agency; and all critical defects have been corrected by the Vendor and successfully re-tested by the Agency and operated without error or defect for the acceptance period.

123. The as-built documents must include a scale map indicating the location of the camera, configuration and test results for camera operation. The Contractor will provide final "as built" drawing in AutoCAD format in both hardcopy and on a CD-ROM for each School.

124. ASU reserves the right to reject the System after the third unsuccessful test of any module of the System.

VIII. SYSTEM ADMINISTRATION AND SECURITY

A. General

125. Solution must allow the system administrator to set rights for access to data by individual or group.

126. Solution must prevent unauthorized access to the system.

127. Solution must accommodate two-factor authentication.

128. Solution must accommodate administrator user rights to any and all workflows and tasks as determined by Customer.

129. Authorized Customer staff must be able to restrict specific user groups from being able to view or print certain types of documentation.

130. Roles, security, and access rights must be easily configurable without Contractor assistance.

131. The proposed solution must adhere to all current, relevant security, and privacy standards.

132. The proposed solution must offer up-to-date, best practice identity management tools to govern user access, such as forced password changes, historical password checks, and the setting of temporary passwords, etc. User management activity must be logged and be available for reporting. Logging must, at a minimum, provide details such as timestamp, user, IP, and action performed.

B. State of Mississippi Enterprise Cloud and Offsite Security Hosting Policy

133. Solution must allow the system administrator to set rights for access to data by individual or group.

134. Solution must prevent unauthorized access to the system.

135. Vendor understands and agrees that all proposed hosting services will comply with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy specified below in this section of this RFP.

136. Per rule 1.4 of the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, each agency must ensure that new contracts and amendments include the terms and conditions approved by ITS. The terms and conditions provided

below are applicable for State of Mississippi data that the agency has categorized as public data.

137. Data Ownership: The State of Mississippi (State) shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Service Provider shall not access State User accounts, or State Data, except (i) in the course of data center operation related to this solution, (ii) response to service or technical issues, (iii) as required by the express terms of this service, or (iv) at State 's written request.

138. Data Protection: Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Vendor to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, the Vendor shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions:

139. All information obtained by the Vendor under this contract shall become and remain property of the State.

140. At no time shall any data or processes which either belong to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction that does not include the State.

141. Data Location: The Service Provider shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State data remotely only as required to provide technical support.

142. Notification of Legal Requests: The Service Provider shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Service Provider shall not respond to subpoenas, service of process, or other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

143. Termination and Suspension of Service: In the event of termination of the contract, the Service Provider shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Service Provider shall guarantee the subsequent secure disposal of State data.

144. Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Service Provider shall not take any action to intentionally erase any State data.

145. Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the Service Provider shall maintain the existing level of security as stipulated in the agreement and shall not take any action to intentionally erase any State data for a period of 90 days after the effective date of the termination. After such 90 day period, the Service Provider shall have no obligation to maintain or provide any State data and shall thereafter, unless legally prohibited, dispose of all State data in its systems or otherwise in its possession or under its control as specified in 48.c below. Within this 90-day timeframe, vendor will continue to secure and back up State data covered under the contract.

146. Post-Termination Assistance: The State shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement.

147. Background Checks: The Service Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration of a minimum of one (1) year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.

148. Security Logs and Reports: The Service Provider shall allow the State access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency.

149. These mechanisms should be defined up front and be available for the entire length of the agreement with the Vendor.

150. Contract Audit: The Service Provider shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State’s expense.

151. Sub-contractor Disclosure: The Service Provider shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Service Provider, who will be involved in any application development and/or operations.

152. Sub-contractor Compliance: Vendor must ensure that any agent, including a vendor or subcontractor, to whom the Vendor provides access agrees to the same restrictions and conditions that apply through this Agreement.

153. Processes and Procedures: The Service Provider shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the vendor. For example: virus checking and port sniffing — the State and the vendor shall understand each other’s roles and responsibilities.

154. Operational Metrics: The Service Provider and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. Examples include but are not limited to:

    a. Advance notice and change control for major upgrades and system changes.
    b. System availability/uptime guarantee/agreed-upon maintenance down time.
    c. Recovery Time Objective/Recovery Point Objective.
    d. Security Vulnerability Scanning.

IX. SUPPORT AND MAINTENANCE

A. Customer Support

155. Describe Maintenance and repair responsibilities and services.

156. Vendor must provide a toll-free telephone number for Customer staff to call 24/7/365 and an always-accessible website for trouble reporting. All telephone customer support must originate in the Continental United States and all support staff must be able to communicate clearly in the English Language.

157. Vendor must disclose instances where a third party or sub-contractor is being used for any portion of customer support services, including the intake of reported problems.

158. Vendor must keep the appropriate Customer management and technical support staff updated on the status of trouble resolution.

159. Vendor agrees to provide adequate training for the effective access and use of support services as requested by the State.

160. Vendor agrees to provide always-updated documentation of all support processes.

161. Vendor agrees that ongoing maintenance and support includes the correction of deficiencies.

162. Vendor agrees that deficiencies may be identified as a result of Vendor's own monitoring or by the State. State discovered deficiencies will be reported to Vendor's customer support for trouble resolution.

B. Issue Tracking

163. The Vendor must use an industry standard tracking system to thoroughly document issues and requests for Customer.

164. Describe how operational trouble issues are submitted, prioritized, tracked, and resolved.

165. Describe how software performance issues are submitted, prioritized, tracked, and resolved.

166. Describe how user support issues are requested, prioritized, tracked and resolved.

167. Detail your escalation procedures for responding to trouble tickets, software performance, and user support issues.

168. The Vendor must provide a customer portal for Customer to track help desk ticketing and incident resolution.

169. For issue tracking, solution must be capable of on demand as well as auto-run reporting.

170. The Vendor must provide a monthly issue tracking report as defined by Customer. For example, the report must detail and comment on any open tickets at month's end, all issues opened and closed within the past month, and other details as required by Customer.