Attachment A

to

RFP No. 4581

Mississippi Department of Corrections
(MDOC)

Technical Specifications

Cellphone Interdiction System

ITS Project No. 47925

TABLE OF CONTENTS

TABLE OF CONTENTS

ATTACHMENT A

I. GENERAL

A. How to Respond

1. Beginning with Item 22, label and respond to each outline point in 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. 4581, 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.

B. Overview and Background

8. Introduction – The Mississippi State Department of Corrections (MDOC) is seeking proposals from qualified vendors to provide comprehensive Contraband Interdiction System (CIS) for correctional facilities across the state to combat prohibited/illegal activities associated with illicit cell phone use. This RFP outlines the background, requirements, and evaluation criteria for interested vendors.
9. Background – The use of contraband wireless devices poses significant security risks within correctional facilities. To mitigate this threat, MDOC seeks to procure and implement robust CIS capable of detecting and disabling contraband devices while ensuring compliance with all regulatory requirements. The facilities for which a CIS is requested are listed below in priority order based on time and available funding:

Table 1: List of Facilities

Facility	Abbr.	Address
Mississippi State Penitentiary	MSP	MS Hwy. 49 West, Parchman, MS 38738
South Mississippi Corrections Institution	SMCI	22689 MS Hwy. 463 North, Leakesville, MS 39451
Central Mississippi Correctional Facility	CMCF	3794 Hwy. 468, Pearl, MS 39208
Marshall County Corrections Facility	MCCF	833 West Street, Holy Springs, MS 38634

Facility	Abbr.	Address
Walnut Grove Correctional Facility	MGYCF	1650 MMS Hwy. 492, Walnut Grove, MS 39489
Delta Correctional Facility	DCF	3800 Baldwin Road, CR540, Greenwood, MS 38930

10. The desired cellular service-management system is a specialized variant known as a Contraband (Cell Phone) Interdiction System (CIS), specifically labeled within the industry as a Managed Access System (MAS). Unlike systems that simply deny cell phone use, MAS actively manages a cell phone's access to a nearby Mobile Network Operator (MNO), ideally blocking all unauthorized cell phones while permitting authorized ones unfettered access. The system must also facilitate identification of usage and device identification. The rationale for implementing such a system is rooted in the unique challenges faced by correctional institutions, particularly concerning the smuggling and illicit use of contraband materials, including cell phones. Such unauthorized devices not only contravene institutional rules but also serve as tools for criminal activities within and beyond prison walls.

11. The impetus for this solicitation stems from the urgent need to significantly mitigate the occurrence of such criminal acts by curbing the illicit use of contraband cell phones within correctional facilities. This initiative is critical to MDOC's broader strategy to combat contraband cell phones effectively.

12. **MANDATORY:** Vendors responding to this solicitation must have required certifications from the Mississippi State Board of Contractor and must have written approval to deploy CIS solutions in accordance with Federal Communications Commission (FCC) order adopted July 13, 2021, FCC-21-82. Proof of these certifications must be provided in Vendor's response to this RFP.

C. Procurement Goals and Objectives

13. According to the need to block wireless communications from contraband cell phones and the technology challenges surrounding this problem, the MDOC expects that solutions proposed for this solicitation will satisfy the high-level objectives described here.

D. Statements of Understanding

14. Throughout this document, references to this RFP will mean RFP No. 4581, including Attachment A to RFP 4581, and all accompanying exhibits and appendices.

15. Unless otherwise specified, throughout this document, references to Customer will mean Mississippi Department of Corrections.

16. 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 Mississippi Department of Information Technology Services.

17. 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.

18. Vendors should expect to find Section VIII, *Cost Information Submission* form in RFP No. 4581 unless otherwise specified, rather than in this Attachment A document.

19. Vendors should expect to find Section IX *References* forms in RFP No. 4581 unless otherwise specified, rather than in this Attachment A document.

20. Vendors must agree to provide best practices, industry-standard tools, and methodologies. The Vendor acknowledges that the State will not accept proprietary formats.

21. The Vendor will be responsible for implementing the proposed solution. The comprehensive solution proposed by the Vendor must address the general and functional requirements outlined in this RFP, including all applicable State and Federal requirements.

E. Glossary of Terms

Acronym	Description
3GPP	Third-Generation Partnership Project
ACL	Antenna Centerline
AGL	Above Ground Level
ASCA	Association of State Correctional Administrators
CN	Core Network
CIS	Contraband Interdiction System
CPNI	Customer Proprietary Network Information
CTIA	(formerly) Cellular Telecommunications and Internet Association
dB	Decibel
dBm	Decibel (relative to milliwatt)
DoS	Denial of Service
EDGE	Enhanced Data rates for GMS Evolution
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HSDPA	High-Speed Downlink Packet Access
HSUPA	High-Speed Uplink Packet Access
HSPA	High-Speed Packet Access
km	Kilometer
LBS	Location-Based Services
LCS	Location Services
LTE	Long Term Evolution

Acronym	Description
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
m	Meter
MAPL	Maximum Allowable Path Loss
MAS	Managed Access System
MAS-E	Managed Access System – Evolved
MASL	Minimum Acceptable Service Level
MNO	Mobile Network Operator
MVNO	Virtual Mobile Network Operator
NR	New Radio
NTIA	National Telecommunications and Information Administration
PA	RF Power Amplifier
PC	Personal Computer
PLMN	Public Land Mobile Network
PSAP	Public Safety Access Point
RAN	Radio Access Network
RAT	Radio Access Technology
RFE	Radio Frequency Emissions
RRC	Radio Resource Control
RSRP	Reference Signal Receive Power
RSSI	Received Signal Strength Indicator
SIM	Subscriber Identity Module
SMS/MMS	Short Message Service / Multimedia Message Service
TDD	Time Division Duplex
UMTS	Universal Mobile Telecommunications System
VoLTE	Voice over LTE
VoNR	Voice over New Radio
Wi-Fi	IEEE 802.11 wLAN
wLAN	Wireless Local Area Network

F. Cloud or Offsite Hosting Requirements

22. Data Ownership – The State shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Vendor 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 the State's written request.

23. 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:

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

    b. 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 by copied, disclosed, or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include the State.

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

25. Encryption

    a. The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.

    b. For engagements where the Vendor stores non-public data, the data shall be encrypted at rest. Both parties will discuss and negotiate the key location and other key management details. Where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection. Additionally, when the Vendor cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements:

        i. The policy shall be issued by an insurance company acceptable to the State and valid for the entire term of the contract, inclusive of any term extension(s).

        ii. The Vendor and the State shall reach agreement on the level of liability insurance coverage required.

        iii. The policy shall include but not be limited to coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.

        iv. At a minimum, the policy shall include third-party coverage for credit monitoring, notification costs to data breach victims, and regulatory penalties and fines.

        v. The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Vendor's limit of liability.

        vi. The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.

vii. The Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.

viii. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.

ix. In the event the Vendor fails to keep in effect at all times the insurance coverage required by this provision, the State may, in addition to any other remedies it may have, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.

26. Breach Notification and Recovery – Unauthorized access or disclosure of non-public data is considered to be a security breach. The Vendor will provide immediate notification and all communication shall be coordinated with the State. When the Vendor or their sub-contractors are liable for the loss, the Vendor shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least three (3) years, mailing costs, website, and toll-free telephone call center services. The State shall not agree to any limitation on liability that relieves a Vendor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Vendor harmless.

27. Notification of Legal Requests – The Vendor 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 Vendor shall not respond to subpoenas, service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

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

a. Suspension of Service – During any period of suspension of any Agreement resulting from RFP 4581, for whatever reason, the Vendor shall not take any action to intentionally erase any State data.

b. Termination of any services or agreement in entirety: In the event of termination of any services or of the agreement in its entirety, the Vendor 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 Vendor 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 Item 28(d) below. Within this 90-day timeframe, Vendor will continue to secure and back up State data covered under the contract.

c. 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.

d. Secure Data Disposal: When requested by the State, the provider shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape,

and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods. Certificates of destruction shall be provided to the State.

29. Background Checks – The Vendor warrants that it will not utilize any staff members, including subcontractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty. The Vendor shall promote and maintain an awareness of the importance of securing the State's information among the Vendor's employees and agents.

30. Security Logs and Reports – The Vendor 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 as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency. These mechanisms should be defined up front and be available for the entire length of the agreement with the Vendor.

31. Contract Audit – The Vendor 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.

32. Sub-contractor Disclosure – The Vendor 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 Vendor, who will be involved in any application development and/or operations.

33. Sub-contractor Compliance – The 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.

34. Processes and Procedures – The Vendor 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.

35. Operational Metrics – The Vendor and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement (SLA). At a minimum, the SLA shall include:

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

G. Vendor Qualifications

36. The Vendor must be capable of and have previous experience in developing and implementing Cellphone Interdiction System solutions of similar size and scope. The references required as noted in Section IX of RFP No. 4581 must substantiate this experience.

37. The Vendor must have been in the business of providing such solutions for at least the last two years.

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

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

40. The 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).

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

42. The Vendor headquarters must be in the United States and provide U.S.-based customer support.

H. Vendor Implementation Team

43. The Vendor must demonstrate that all team members have the necessary experience for developing, configuring, implementing, testing, user training, maintenance, and supporting the services required by this RFP. At a minimum, the 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.

44. Identify the key staff members responsible for executing the various aspects of the project, including, but not limited to, the Project Manager, Development Team, Business Analyst(s), and Technical Architect(s).

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

46. The Vendor must ensure that each team member assigned to this project can communicate clearly in English, both verbally and in written form.

II. FUNCTIONAL/TECHNICAL REQUIREMENTS

A. Managed Access System – Evolved (MAS-E) Functions

47. The Mississippi Department of Corrections (MDOC) issues this RFP No. 4581 to obtain proposals from qualified vendors capable of providing a Cellphone Interdiction System (CIS) in the form of a MAS-E to be installed at the State facilities listed in Item 9 above. The nominal MAS-E proactively manages cellphone access to cellular services through interworking agreements with proximate Mobile Network Operators (MNOs). The MAS-E functions like a traditional MNO partner network that serves roaming subscribers. This is achieved by initially “capturing” cellphones attempting access and subsequently either facilitating the requested access for legitimate cellphones or denying service to illicit cellphones.

48. Devices connecting to the MAS-E are authenticated such that the MAS-E may continue with any other signaling that may require a security context. The authenticated device should not have any knowledge that it is being served by a

network other than its home network. This capability nominally requires the execution of interworking agreements (IAs) with proximate MNOs and establishing network interconnections supporting necessary logical signaling associated with roaming or related protocols. Indirectly, this also requires not only conformance to specifications, but adherence to the MNO internal specific configurations and parameters. The capabilities exhibited by the MAS-E include the following:

49. Emulation of the broadcast transmissions from MNO cell sites normally used by cell phones to identify them and transmission of connection messages with sufficient fidelity to attract and “capture” the cell phone. This requires careful attention to the deployed RATs, frequencies, and RF power levels to ensure that the cell phone attempts to connect to the MAS-E and not to an MNO network. As these frequencies are licensed by the FCC to proximate MNOs, this also implies that appropriate arrangements are in place for the use of those frequencies.

50. Transmission of messaging and use of protocols normally associated with device registration with the MNO's network which must be emulated with sufficient fidelity (e.g. strict conformance to specifications) to solicit cell phone equipment and subscriber identities, to ascertain whether the cell phone is legitimate or illegitimate. This includes processes within the MAS that support automated decision-making based on databases of legitimate identities.

B. System Deployment

51. The system must be designed and deployed such that there is a high probability that cell phones within the Facilities will be “captured by the MAS-E” whenever they attempt to register with a proximate MNO or request service, regardless of its location within the indoor and outdoor spaces of the Facilities that are accessible to its residents. This should be balanced in turn against an expectation of a very low probability that cell phones located beyond the Facility would have their service affected.

52. The Facilities are represented as a fenced polygonal compound(s) with areas ranging from 0.028 to 5.0 square miles that encompass both open areas and multiple multi-story concrete buildings. There are no explicit deployment constraints; in theory, components of the System can be placed within/atop buildings, atop peripheral structures (e.g. fencing, light poles, guard towers), or within/atop custom-built structures. It is also anticipated that it will be desirous that some MAS-E components (e.g. RF antennae) be placed immediately outside the fence to serve both indoor and outdoor spaces. It is however assumed that the MDOC will be provided an opportunity to vet the proposed deployment for practicality and provide feedback to allow modified deployments to be developed and proposed.

C. Coordination with Mobile Network Operators (MNOs)

53. A MAS-E system must detect subtle details of the transmissions of proximate MNOs to function effectively. It is therefore expected that the awarded Vendor will be aware of the addition of the MNO’s tower sites, frequency bands, and technology changes within proximity of the Facility which can affect the performance of the MAS-E.

D. Cellphone Activity and Circumvention Monitoring

54. The operational effectiveness of the System must be continuously verified using any reliable mechanism that provides a method for monitoring the cell phone channel transmissions directed to either the System or proximate MNOs. Monitoring nominally consists of accurately detecting uplink transmissions by time/frequency/power, identifying relevant transmissions, and geographically localizing the transmission.

E. Wi-Fi Service Denial

55. Within the facility, the System must include a capability to identify unauthorized Wi-Fi transmissions over the IEEE 802.11 RAT which may or may not terminate at an MNO core network. These include both Access point-controlled access and Peer-to-Peer access.

F. Future Scalability

56. The system's architecture must be designed with future scalability in mind, capable of accommodating advancements in wireless communication technologies. This includes support for emerging Radio Access Technologies (RATs) such as 6G and beyond. By future-proofing the system, MDOC can ensure its long-term viability and effectiveness in combating contraband cell phone usage within its facilities.

III. System/Solution Design

57. MDOC will evaluate proposed solutions for their ability to meet the requirements and provide additional credit for meeting and/or exceeding the requirements. Further, proposed solutions may contain capabilities or solutions that are not explicitly required here or that go above and beyond the stated requirements. Such proposals will be evaluated and may be rewarded to the extent that they more effectively execute the stated objectives listed in the evaluation criteria.

A. System Requirements – Cellular Channel Operation, RF Coverage, and Access Capture

58. The Vendor shall install and operate a System at the Facilities that meet the system requirements listed below and must respond to the requested items:

59. The system shall be capable of operating cells that can facilitate a radio-layer connection (e.g. RRC-layer for 4G, 5G) with cellular communication devices. These cells shall be deployed such that devices within the facility are unable to connect to MNO-operated cells at a center frequency below 39 GHz with at least one commercial deployment within the distance of the Facility indicated by Table 1. Cell phone access shall be prevented to access nearby MNO cells of any RAT, downlink channel center frequency (ChFreq), or duplex mode.

60. Exceptions for MNO cellular channels within the distance from the facility indicated in Table 2 would be allowed in MDOC has expressly allowed for connection to a particular cell or network (such as an authorized on-premises network intended for inmate access).

Table 2 – Distance of MNO Cell Requirements Based on Frequency Range

Frequency Range (GHz)	Distance (km)
0-3	12
3-6	8
24+	1

61. Describe the overall architecture of the system, including radio access network (RAN) equipment, core network components, network interfaces, physical connections, and RF equipment.

62. Describe the System's ability to operate cellular channels, including:

    a. The radio access technologies the System will support and the ability to facilitate radio-level connections with any cellular device that attempts to connect.

    b. The ability to prevent devices from accessing MNO networks.

    c. The ability to operate many different cells at different frequencies, as determined by MNO-operated cells in the area around the facility.

    d. The ability to operate both FDD and TDD channels for 4G and 5G (depending on the MNO network).

63. Describe the System's ability to retain connected devices.

64. System cells shall broadcast over-the-air Public Land Mobile Network (PLMN) codes that are present on nearby MNO-operated cells such that a user whose subscription is offered by any PLMN will be captured by the System.

65. Describe the System's ability to ensure that subscribers of any Proximate PLMN broadcasting its specific PLMN will be captured by the System.

66. If an MNO uses dynamic spectrum sharing to allow access from two RATs at the same ChFreq, the Vendor shall provide a solution for preventing access through either RAT.

67. Describe the System's ability to allow subscriber access from multiple RATS at the same Channel Frequency when the Proximate MNO's have deployed dynamic spectrum sharing.

68. Throughout the interior of the Facility perimeter, each 4G and 5G System cell shall have at least 7 dB RSRP advantage, and each 2G and 3G cell a 10 dB RSSI advantage, over the strongest corresponding MNO cell of the same RAT and frequency band for which the System cell is intended to prevent access. The signal strength advantage will be assessed at the time of acceptance testing. The tests shall include drive/walk surveys with a selection of test phones registering, accessing, and attempting authorized/contraband calls to assess the effectiveness of the System while continuously recording phone state, messaging, and received signal strengths.

69. Describe the RF planning and deployment process and how you ensure that the desired RSRP and RSSI advantages are met throughout the interior of the facility perimeter.

70. Describe the System's targeted signal strength advantage for each radio access technology.

71. Describe typical characteristics of the signal strength near the facility boundary.

72. Along with all other device connection data capable of characterizing the performance of the System, provide the System's Link-budgets examples for Low/Mid/High bands voice and data services with inputs and assumptions yielding the MAPL (Maximum Allowable Path Loss).

73. Vendor must provide estimates on the number of radio units and the number of antennas locations.

74. Vendor must provide Aerial view layout maps with their RFP response showing nodes and RF distribution with antennae locations for each facility.

75. Describe the implementation strategy, including configuration, pilot testing, and acceptance.

76. Provide the Coverage Maps specified below, in Items 109 & 111, along with the raw data files of all maps exported in ArcGIS or MapInfo format on a secured storage device.

77. The System shall be able to interact with a connecting device to capture both the subscriber identity (IMSI) and the device identity depending on the RAT (IMEI, MEID), regardless of the RAT used for the initial connection to the System.

78. Describe how the System functions to capture a UE's (IMEI, MEID) or other unique mobile device identifier for each RAT during the initial connection attempt irrespective of the CIS connection decision on access or denial to mobile services.

79. The System shall be able to make "allow" or "block" decisions for each connection originating from within the facility based on a pre-determined identity Whitelist. This decision shall be made before a device is granted access to calling, SMS/MMS, or data services.

80. Describe how the System functions in making allow or block decisions for each connection attempt originating from within the Facility based upon a pre-assembled device identity Whitelist.

81. The System shall have a mechanism by which the Vendor can modify the System's Whitelist to add or remove authorized users, based upon requests from MDOC.

82. Describe the process for receiving and implementing MDOC requests for adding and removing authorized users to the System's Whitelist. Specify where the Whitelist is maintained and if the MDOC can be granted remote access to modify the Whitelist. Specify the timeframe for Whitelist changes to be actualized on the System.

83. The System shall allow and facilitate calling, SMS/MMS, and data access for authorized users.

84. Describe the System's ability to operate cellular channels providing voice calls (VoNR, VoLTE, and Circuit Switched), SMS/MMS Messaging, and Data Access from authorized users originating and receiving calls within the Facility. Indicate how the System handles mobility within the Facility and if calls can be handed over

to/from the appropriate MNO if a user enters or exits the facility while engaged in a voice call.

85. The System shall prevent voice calling, SMS/MMS, and data access (except for emergency calls) for unauthorized users, while still retaining the device on the MAS network or otherwise preventing the device from connecting to an MNO-operated cell.

86. Describe the System's ability to capture and block voice calls (VoNR, VoLTE, and Circuit Switched), SMS/MMS Messaging, and Data Access from unauthorized user devices originating and receiving calls within the Facility. Explain how the System retains and terminates these unauthorized connection attempts and acquires the device identities and location information to provide to the MDOC.

87. When the System operates in a mode that uses an IA with an MNO, it shall be capable of authenticating both authorized and unauthorized connections whose subscriptions belong to said MNO while still being able to block calling/SMS/MMS/data access from unauthorized users.

88. Describe the System's ability, when IAs are in place, to authenticate users and retain cellular devices on the MAS in a manner that a device expects on a typical MNO network.

89. Describe the System's ability to obtain subscriber and hardware identities of connected devices, regardless of the initial access technology on which the device connects, both with IA-enabled authentication and without authentication.

90. The System shall not block emergency (911) calls from either authorized or unauthorized devices connected to the System. Emergency calls from unauthorized devices must be routed to the MDOC's preferred master communications station, while emergency calls from authorized devices must be routed to the local public safety answering point (PSAP). The System shall comply with all relevant FCC regulations on emergency calls.

91. Describe the system's ability to connect emergency calls to 911 from authorized devices to the appropriate local PSAP while routing unauthorized emergency (911) calls to the MDOC's preferred master communications station and if not answered, then establish a connection with the local PSAP.

B. System Requirements – Coordination with MNOs

92. By the Acceptance testing date, the awarded Vendor shall have entered into IAs with every MNO that operates cellular channels in the area around the facility and the System shall have the technical interfaces and capabilities installed and available for use. These IAs and the associated technical capabilities shall enable the System to authenticate devices connecting to the System's network on a cell.

    a. Describe the process used to ensure all System operations are legal, including the ability to transmit in licensed frequencies.

    b. Describe any relevant technical details of the IA that ensure effective System operation.

93. The subscriber authentication shall be conducted in a way that the device is not aware it is connecting to a network other than its own.

a. Describe whether the System has 4G or 5G IAs currently in place with MNOs that operate in the area around the facility, along with any MVNO that would require a separate IA to authenticate a user successfully.

b. If IAs are not in place, describe the Vendor's progress towards this goal and the estimated timeline for completing the agreements and being able to implement the interfaces in a deployment at the facilities.

94. The Vendor shall enter into IAs, or similar arrangements that allow for seamless imperceptible user authentication, with MVNOs and other MNOs who would have access to cellular services in the area.

a. Describe the Vendor's progress towards pursuing 5G IAs with MNOs that operate or are planning to operate 5G SA cells in the area around the facilities.

b. Describe any other coordination the Vendor would pursue with MNOs, including but not limited to:

i. Regular meetings with MNOs.

ii. Further technical coordination such as active handover from the MNO network.

iii. Any ongoing technical research areas with MNOs that may lead to new System features in the future.

C. System Requirements – RF Monitoring and Circumvention Detection

95. The Vendor shall have installed and begun operating at the Facility an RF monitoring subsystem (RFMS). The RFMS shall periodically scan the entirety of all eligible cellular frequency ranges in a manner that would allow it to identify new cellular channels of which it was not previously aware.

a. Describe the System's ability to monitor the signal strength of MNO-operated cells and maintain awareness of relative signal power levels.

b. Describe the metrics used to determine when changes to the system need to be made.

c. Describe the System's ability to monitor any other unauthorized wireless communication methods that may be used within the facility, including two-way radio, satellite phone, etc.

96. The Vendor shall have installed and begun operating at the Facility a circumvention detection subsystem (CDS). The Vendor is encouraged to install and operate any or all of the required components/capabilities by the date the System is operationally ready.

97. Describe the System's ability and the methods used to detect and identify circumvention activity.

98. The CDS shall be capable of detecting in an automated manner instances of circumvention activity that occur using 2G, 3G, 4G or 5G communications.

a. Describe the System's ability and the methods used to automatically detect instances of circumvention activities over 2G, 3G, 4G and 5G RATs and how they can be accurately identified.

b. Describe the level of confidence the System can achieve for identifying circumvention activity.

99. The Vendor shall document observed circumvention activity and provide reports to MDOC as requested. The Vendor shall also have a mechanism or process for responding to observed circumvention events and making adjustments to the System as necessary.

100. Describe the process by which circumvention activity incidents will be addressed.

D. System Requirements – Device Location

101. When an unauthorized device connects to the System, the System shall localize the device over time with a moderate location accuracy of fifty (50) feet.

102. Describe the System's ability and the methods used to localize unauthorized devices that attempted connections to the System within fifty (50) feet of its actual location. If not met, define the System's expected location precision.

E. System Requirements – Wi-Fi

103. The System shall include a solution that combats unauthorized Wi-Fi access points (APs). This solution shall be able to rapidly identify unauthorized APs and deny access to identified unauthorized APs. The solution shall be deployed such that it can combat unauthorized APs within every building in which inmates live or are allowed access. MDOC requires that the Wi-Fi solution must operate at the facilities listed in *Table 1* above.

a. Describe the System's ability and the methods used to automatically detect unauthorized or "rogue" Wi-Fi Access Points (AP) and other transmission over the IEEE 802.11 RAT.

b. Provide details on the software and hardware tools to be employed to detect illegal Wi-Fi activity and identify whether "Ad Hoc" or Peer-to-Peer Wi-Fi networks can be detected.

F. System Requirements – Cyber Security

104. The sharp growth in the dependency of many network functions such as virtual Cores and C-RAN on cyberspace and cloud computing has increased exponentially the risks of cyber-attacks. Cyber threats are in general unpredictable in occurrences and scope. The MAS-E is required to employ robust procedures and protocols for requiring credentialing, authentication, and verification of user's identities and their level of access.

105. Network Domain Security shall be implemented in accordance with 3GPP TS 33.210 or later applicable security specifications, which stipulate the use of IPSec to protect IP communication between administrative domains (including all network connections used to interconnect the domains).

106. All software and systems used in the MAS-E CIS shall be maintained at the most current versions including all software and firmware updates as the environment is in a state of constant change.

107. There are external and internal "Bad Actors" targeting all classes of Information and Telecommunications Systems. From Baby Monitors and Wi-Fi routers to the National Power Grid and the Pentagon, vigilance and adherence to security procedures are of paramount importance.

a. Describe the Vendor's processes, procedures, and measures planned for ensuring that the four (4) cybersecurity threats and measures listed herein are considered, planned for, and mitigated.

b. Describe any additional security threats or measures considered and the technical details concerning these considerations in the Vendor's design and operations plans.

G. System Requirements – RF Coverage Maps

108. MNOs Existing Coverage:

109. For the complete area of the facility to a radius of two (2.0) miles from the outer boundary of said facility the Vendor shall provide two (2) RF propagation Coverage Maps showing RSRP/RSSI levels in 10dB steps from -75/-70 dBm to -125/-120 dBm and the Best Server plot to -125/-120 dBm for each Proximate MNO for each frequency bands they intend to deploy that provides coverage to the facility for each corresponding RAT. All plots shall include the MDOC facility's property boundary polygon.

a. The RF propagation coverage maps shall utilize an appropriate number of tiers of the MNO's Wireless sites according to the area's morphology and shall be of 10m resolution.

b. The RF propagation coverage maps shall be generated with industry-accepted tools such as Atoll, Planet, Asset, EDX, Celplan, or Celwave, and include the MNO's Tower site locations.

c. The Vendor shall provide a table of the MNO's Tower sites used in the generation of the RF coverage maps, their Geo Coordinates, ACL, Antennae models, Tilts, azimuths, and PA power.

d. The Vendor shall provide a table containing the settings and parameters used in the RF Propagation Tool in the generation of the coverage maps. The Vendor can refer to the NTIA.GOV website for information on RF propagation tools and models used by Federal agencies.

https://its.ntia.gov/research-topics/propagation-modeling-website-pmw

110. MNOs and Proposed MAS-E Composite Coverage Maps:

111. For the complete area of the facility to a radius of one (1.0) mile from the outer boundary of said facility, the Vendor shall provide three (3) composite RF propagation coverage Maps showing indoor and outdoor levels of coverage from the proposed MAS-E and from each Proximate MNO combined for RSRP/RSSI levels in 10dB steps from -75/-70 dBm to -125/-120 dBm, a combined Best Server plot to -125/-120 dBm and a combined C/I or SINR plots at 50% loading in 5dB steps for each Proximate MNO for each frequency bands they have deployed or intend to deploy that covers the facility for each corresponding RAT. All plots shall include an MDOC facility's property boundary polygon.

a. The RF propagation coverage maps shall utilize an appropriate number of tiers of the MNO's Wireless sites according to the area's morphology and shall be of 5m resolution with the facilities and 10m resolution outside the facilities.

b. The RF propagation coverage maps shall be generated with industry-accepted tools such as Forsk's Atoll, InfoVista's Planet, Asset, and Celwave and show the MNO's Tower locations.

c. The Vendor shall provide in their RFP response a table of the MNO's Tower sites used in the generation of the RF coverage maps and their Coordinates, ACL, Antenna models, Azimuths, Tilts, and PA power.

d. The Vendor shall provide a table of the MAS-E Nodes used in the generation of the RF coverage maps and their Geo Coordinates, ACL, Antennae models, Azimuths, Tilts, azimuths, PA powers, PA power split ratios, and transmission losses.

e. The Vendor shall provide a table containing the settings and parameters used in the RF Propagation Tool in the generation of the coverage maps. Where applicable in showing the MDOC facility Indoor coverage the Vendor shall consider and utilize the appropriate "in-building" RF penetration losses corresponding to the structures in the analysis.

f. The preferred proposal will have incorporated detailed Indoor Propagation plots using an "In-Building" specific RF Propagation tool or module such as Atoll, Planet, IBwave, Forsk, InfoVista or Remcom.

H. System Reliability and Resiliency

112. The MAS-E solution shall be designed to be resistant to both natural and man-made events that could disrupt or interfere with normal operations. Resiliency and reliability considerations should yield a System that is near Public Safety Grade (PSG). The design and construction of PSG systems are such that they "hold up" during natural disasters and intentionally disruptive events. These include but are not limited to the following:

a. Weather – Rain, Snow and Ice storms, high winds, and Flooding. Considerations must be made at all stages as to how to deploy the System to be resistant to outages caused by natural causes using industry best practices.

b. Lightning Strikes – Lighting poses a significant risk to outdoor Telecommunications appurtenance, therefore sub-systems such as lighting arrestors and ubiquitous grounding are required for reliability.

c. Power Outages – It is a known fact in highly populated areas and facilities that illegal activities increase significantly during power outage events. The deployment of a four-to-eight (4-8) hour battery backup for the System and all critical sub-systems is the minimum acceptable reserved power solution for this RFP.

d. Direct Physical Attack – Events of vandalism of MAS-E infrastructure at the MDOC facilities are to be expected, and the risk is mitigated as much as practical. The Vendor shall document measures in the proposal that provide for the hardening of the exposed parts of the System against vandalism of its components such as its cables, antennas, electronics cabinets, power sources, etc.

e. Fiber Interconnection Loss – The Inter-connection topology should be designed to eliminate single points of failure that could disrupt the entire CIS function at a facility.

f. Intentional Disruptive Radiators (Jammers) – The MAS-E solution should be designed to monitor the System's Noise Floor across the frequency bands to immediately detect the presence and approximate location of White Noise generators which create wideband noise that can jam the CIS and disrupt normal operation.

i. Describe the System's ability, design features, and implementation methods utilized to ensure that the proposed system addresses the six disruptive events listed herein in this section (III. System/Solution Design, H. System Reliability and Resiliency).

ii. Describe any additional measures the Vendor proposes to harden the System against disruption of operation or key functionality.

I. System Redundancy

113. The System shall demonstrate some level of redundancy in its design to the extent possible that the reliability of the System is near the Public Safety Grade. Single points of failure that can disrupt or shut down the entire system shall be considered and mitigated.

114. Nodes should have a significant level of overlap. The right balance between coverage, capacity, and cost has to be struck. This "right balance" between competing network requirements is the hallmark of the quality of the proposal sought by the MDOC.

115. Design choices such as fully addressable MAS-E DAS nodes with power splits no greater than 1:2, would significantly reduce the occurrences of local area outages without it being immediately known to the Vendor

116. Excessive VSWR or PIM on an antenna can be detected to trigger a redistribution of the PA power to other neighboring antennae until the impaired device is replaced or repaired.

117. Describe the proposed design consideration addressing requirements of system redundancy and include the Vendor's methods for reducing or eliminating single points of failure in the System.

J. Radio Frequency NEPA (RF Emissions)

118. The FCC regulates human exposure to Radio Frequency emissions and has established certain exposure limits for different groups of the population based on their level of awareness of the presence of and exposure to Radio Frequency emissions from transmitters mounted on structures. Several publications from the FCC such as the OET Bulletin 65 and its supplements outline the requirements for compliance with these regulations and the governing laws.

119. The Vendor shall conduct and provide Maximum Permissible Emissions (MPE) analyses for each MDOC Facility's structure in and to which it has installed antennae or other device capable of radiating Radio frequency energy in the environment using the formulas and procedures outlined in the FCC OET Bulletin -65 for both Non-Occupational (RFE unaware persons) and Occupational (RFE aware) limit levels.

120. The RF emissions MUST include all radio frequency emitters (transmitters) located in or near the structure so that the true total emissions can be assessed. The emitters must include those pertaining to the MAS-E System and those not.

121. The Vendor shall provide and retain RF emission studies for each structure demonstrating compliance and shall yearly certify in writing that the facility remains compliant.

122. The result of the RF Emissions study shall be utilized to facilitate safety measures such as signage or restriction but may include System design changes or power reductions so that the RF Exposure to residents, employees, and contractors is within full compliance.

123. Describe the processes and procedures the Vendor pursues to review the RF Emissions studies and mitigate areas that exceed the Non-Occupational and Occupational MPE.

    a. Describe any relevant technical details relating to RF Emissions exposure mitigation upon which the Vendor relies to ensure the System is safe for the facility residents.

K. Reporting Requirements

124. For any unauthorized device, the System shall log every attempted phone call or text (SMS) message and retain the information for at least six (6) months. Call logs from authorized devices passed through to the MNO shall likewise be maintained and handled in accordance with the MNO's internal and FCC Regulations concerning Customer Proprietary Network Information (CPNI).

    a. Describe the System's ability to log every attempted unauthorized call attempt, with six (6) months of retention.

    b. Describe the System's ability to handle authorized device call logs in accordance with FCC regulations governing CPNI.

125. Describe the System's security features for guarding CPNI, and the training required by the Vendor's personnel with access to CPNI.

126. The System shall be capable of producing reports of unauthorized activity that can be shared with the MDOC.

127. Describe the System's ability to generate reports of unauthorized connection activities and the formats in which they can be shared with the MDOC. Specify if the MDOC can be provided with remote access to the report-generating software.

128. The System shall not record or store the contents of any communications by authorized users (calls, text messages, etc.).

129. Describe the System's ability to safeguard against recording and storage of the contents of authorized user's communications (including but not limited to calls, SMS/MMS, data access such as Internet browsing history).

130. The System shall provide the logs of unauthorized connection attempts that shall include the following information:

    a. Time of access.

    b. Subscriber Identity (IMEI, MEID) of the unauthorized user.

c. Hardware Identity (IMEI, MEID) of the unauthorized device.

d. Destination phone number (if applicable).

e. Contents of the message (if the activity is SMS or MMS).

131. Describe the System's ability to record and retain logs of the five (5) attributes listed herein as Reporting Requirements item 130 above.

132. For attempted data connections, the System shall log web addresses and IP addresses contacted.

133. Describe the System's ability to record and retain logs of web addresses and IP addresses contacted for every unauthorized data connection attempt.

134. The System shall log location information for unauthorized activity and make this information available to MDOC in the requested reports.

135. Describe the System's ability to record and retain logs of the activity origination location as determined for every unauthorized connection activity.

136. The System's reports shall be made available to MDOC upon request in the format that includes the contents described in Item 130. The report contents shall be also made available as a spreadsheet or delimited text file.

137. Describe the System's ability to produce the required report and content file as outlined.

138. The System shall also be capable of producing summary reports which include the following information:

a. Call attempts.

b. Calls allowed.

c. Calls blocked.

d. Text message attempts.

e. Text messages blocked, with text message contents.

139. Describe the System's ability to produce reports that include logs of the five (5) attributes listed in the item above (138).

140. The System shall log any new connection by a device to the System and retain this information for at least six (6) months. A "new connection" is defined as a connection made by a device that has either been idle or wholly disconnected for at least thirty (30) minutes. The System shall include the following in the log entry:

a. Time of access.

b. Subscriber Identity (IMSI) of the unauthorized user.

c. Hardware Identity (IMEI, MEID) of the unauthorized device.

141. Describe the System's ability to log, record, and retain logs of "new connections" and the three (3) attributes listed in the item above (140).

142. The System shall log the exchange of any 4G or 5G messages, such as "Attach Request" and "Attach Accept." Refer to 4G NAS protocol TS 24.301, and 5G NAS protocol TS 24.501.

143. Describe the System's ability to log, record, and retain logs of 4G and 5G NAS message occurrences as per the reporting requirement listed in the item above (142).

144. The System shall log any 3G, 4G, or 5G RRC message events, except System Information Block broadcasts. This does not need to include the contents of the message, but only that the message was sent/received by an entity (for example, 4G eNB receives an "RRC Connection Request" message and responds with an "RRC Connection Setup" message). Refer to 4G RRC protocol: TS 36.331, and 5G RRC protocol: TS 38.331.

145. Describe the System's ability to log, record, and retain logs of 4G and 5G RRC message occurrences as per the reporting requirements listed in the item above (142).

L. Liquidated Damages and Services Level Agreement

146. A Service Level Agreement shall be entered into pursuant to the Vendor Requirements on Minimum Acceptable Service Levels ("MASLs") and is incorporated into and made a part of this RFP. Vendor agrees to meet or exceed the ("MASLs") set forth in this Service Level Agreement. Failure to meet the MASLs and not correct performance within stated timeframes will result in stated liquidated damages being due MDOC. Vendor offers Operational Availability, Managed Area, Device and Technology Currency, and Support Response Time MASLs.

147. Operational Availability (OA) MASL

Vendor agrees to exercise commercially reasonable efforts to achieve MASLs for Operational Availability no less than 99.9% each week (the optimal target is 100%). If Vendor fails to meet OA MASL of 99.9% in any week, and Vendor fails to meet OA MASL in the immediately following week, then Vendor may be assessed liquidated damages in the amount of $500.00 per week fee for each deficient week.

148. Effectiveness MASLS

Vendor agrees to meet the following System effectiveness metrics: 99% of all instances of attempted cellular access within the areas of the Facility designated by MDOC to be covered by the System are captured by the System (the optimal target is 100%).

a. If Vendor fails to meet the Effectiveness MASLs over any two-week period, Vendor may be assessed liquidated damages in the amount of $500.00 per week fee for each deficient week.

149. Device & Technology Currency MASL

Vendor shall upgrade the System to detect and legally eliminate Illegal Cell Phone Use for the Managed Area for all new wireless communication protocols and frequencies and new carriers/technologies before carrier/technology availability at the facility, with the exception of an instance where an MNO fails to notify Vendor of such a change, in which case Vendor shall make any necessary upgrades to the System within 90 days of carrier/technology availability at the facility. When the System detects a change in power levels or other status of known nearby cells operated by MNOs that can impact the System's effectiveness, Vendor shall make any necessary upgrades to the System within 7 business days. If Vendor fails to

meet the Device & Technology Currency MASL, Vendor may be assessed liquidated damages in the amount of $500.00 per week fee for each deficient week.

M. Performance Requirements

150. As each component has a user interface (GUI), each component must support the below processes:

   a. The user login

   b. Single query and return results

   c. Building and delivering a data file to the user

   d. Standard report generation (the data sets and size that are typically included and the estimated performance for generating these reports)

N. Acceptance Testing

151. The Vendor-declared “operationally ready” MAS-E system shall be subjected to contractual Acceptance Testing. A comprehensive series of functionality tests will be conducted to verify that all the required functions of the CIS have been adequately implemented and to determine if the MAS-E performance with respect to MDOC goals detailed in this RFP and Attachment A have been met.

152. The testing will cover all indoor and outdoor areas of the MDOC facilities, including locations normally occupied by residents during their daily activities.

153. A comprehensive Quality Inspection of the installations will be undertaken to determine that the construction was completed in a manner consistent with industry best practices for reliability and resiliency.

154. The functionality tests will consist of a battery of devices with subscriptions with the proximate MNOs along with an auto-call system, data collection hardware and software that enable the devices to hundreds of both authorized and unauthorized connection attempts and sessions while the mobile tester covers a geographic area.

155. Emergency test 911 calls terminating at the local PSAP will be included in the functionality testing, subject to proper prior notice. However, this testing will be performed manually and not by the auto-call system.

156. The data collected from the devices will be “post-processed” and be displayable on maps and on the facility’s layout views. The MNO and MAS-E signals and states measured by the devices will be analyzed, mapped, and displayed for comprehensive functionality verifications.

157. The following multi-day tests shall be included in the Acceptance Testing process:

   a. Walk functionality test targeting all the indoor areas normally occupied by the Facility residents, including but not limited to Dormitories, Dining Hall, Recreation Spaces, Work and Learning center Bathrooms, Closets, Storage Rooms, Kitchens, Gymnasiums, Infirmaries and Garages.

   b. Drive functionality test targeting all the outdoor areas accessible to the Facility’s residents and employees, including but not limited to Roads, Parking lots Walkways, Outdoor Recreational and Work Areas.

c. Drive functionality test targeting the public outdoor boundary of the of the Facilities including but not limited to public Highways, State, County and Neighbor Roads, Parking lots, cul-de-sacs, parks or other public Recreational Work areas adjacent to the Facility to a distance of a quarter (0.25) mile. The results of this test shall enable the MDOC and Vendor to determine the existence of unintentional CIS disruption of service to the Public which is strictly prohibited by the FCC.

IV. SUPPORT, MAINTENANCE, AND TRAINING

A. Annual Re-Certification

The Vendor proposing the system and services under this RFP and Attachment A shall have its operations subjected to an annual re-certification to achieve the following:

158. Ensure that the MAS-E system continues to meet or exceed all the test initially administered under the Acceptance Test Procedure that the Vendor was contracted and permitted to proceed with the CIS operations at the MDOC facilities.

159. Verify that the Vendor continues to operate a System that remains compliant with all applicable FCC regulations, with special attention to regulations concerning Occupational and Non-Occupational exposure to Radio Frequency Emissions.

B. Maintenance During Warranty

160. The Vendor must provide telephone support for warranty and software Monday through Friday 8:00 a.m. to 5:00 p.m. Central Standard Time (CST).

161. The Vendor must respond to telephone requests within four (4) hours for critical components and eight (8) hours from call to service. For every hour the Vendor fails to respond, there will be a fine of $50 dollars per hour up to $500 dollars per day.

162. The Vendor must provide eight (8) hour turnaround on repairs not requiring parts and two (2) days turnaround on all other repairs. For every hour delay on repairs, there will be a fine of $50 dollars per hour up to $500 dollars per day.

C. Post Warranty System Maintenance

163. The Vendor must provide post warranty and software telephone support Monday through Friday 8:00 a.m.to 5:00 p.m. Central Standard Time (CST).

164. The Vendor must respond to telephone requests within four (4) hours for critical components and eight (8) hours from call to service. For every hour the Vendor fails to respond, there will be a fine of $50 dollars per hour up to $500 dollars per day.

165. The Vendor must provide eight (8) hour turnaround on repairs not requiring parts and two (2) days turnaround on all other repairs. For every hour delay on repairs, there will be a fine of $50 dollars per hour up to $500 dollars per day.

D. Training

166. The Vendor must provide a combination of virtual and onsite training for MDOC personnel.

167. The hardware, equipment, and RF antennae will be physically on-site at each prison. The Vendor must provide this training onsite as MDOC personnel will need hands on training.

168. The general system usage training must include twelve (12) seats for MDOC personnel.

169. The in-depth system administration training must include two (2) seats for MDOC personnel.

170. The Vendor may be required to add an additional training for data conversion.