Attachment A

RFP 4063

Mississippi Department
of Public Safety

AFIS Technical and Functional Requirements

ITS Project No. 42660

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

Attachment A
RFP No. 4063 – AFIS Technical Requirements

I. General

A. How to Respond

1. Beginning with Section B, Item 9 of this attachment, label and respond to each outline point in this section as it is labeled below.
2. The Vendor must respond with "ACKNOWLEDGED," "WILL COMPLY" or "AGREED" 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.
3. "ACKNOWLEDGED" should be used when no vendor response or vendor compliance is required. "ACKNOWLEDGED" simply means the vendor is confirming to the State that he read the statement. This is commonly used in the RFP sections where the agency's current operating environment is described or where general information is being given about the project.
4. "WILL COMPLY" or "AGREED" are used interchangeably to indicate that the vendor will adhere to the requirement. These terms are used to respond to statements that specify 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 "ACKNOWLEDGED," "WILL COMPLY," or "AGREED," then the Vendor must respond with "EXCEPTION." (See Section V, 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. Procurement Goals and Objectives

9. The proposed solution must meet the minimum goals and objectives of the MDPS/CIC as described below.
10. MDPS is seeking best-of-breed AFIS applications with non-proprietary, open-standards database architecture and software interfaces:
    a. MDPS is seeking the most current, state-of-the-Art AFIS (e.g., Ten Print, palm print, latent) applications and workflows, including integration with the current Livescan fingerprint and mug shot systems;
    b. A primary procurement goal is to ensure that the proposed solution will manage the workflows and transactional integrity of all sub-components of the current in-place AFIS;
    c. MDPS is seeking Commercial Off-The-Shelf (COTS) applications software and non-proprietary hardware;

d. The MDPS desires to migrate the existing NIST formatted database of fingerprints, latent prints, and mug shots from the existing State systems to the proposed solution. State resources will not be available for this effort.

C. Current AFIS Overview and Configuration

11. The *AFIS Current Environment for RFP 4063* is considered necessary for a proper response to this RFP. This document provides an assessment of the current AFIS/MCHS environment. Responding vendors must request a copy of this document by sending an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request.

    a. Vendor agrees to use this document only for the purposes of responding to this RFP and to otherwise treat this document as proprietary and confidential information.

12. The *AFIS MCHS ICD for RFP 4063* is considered necessary for a proper response to this RFP*.* This document describes the interface between MCHS and the current AFIS. The interface is designed so that either AFIS or MCHS can take down or restart its side of the interface without affecting the other side or suffering a loss of requests or responses. Responding vendors must request a copy of this document by sending an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request.

    a. Vendor agrees to use this document only for the purposes of responding to this RFP and to otherwise treat this document as proprietary and confidential information.

13. The *AFIS MCHS Tenprint ICD for RFP 4063* is considered necessary for a proper response to this RFP. This document provides the interface requirements between the MCHS repository and either fingerprint card scans or fingerprint live scan stations. It also provides the guidelines for tenprint certification that is required for prospective tenprint vendors wanting to provide services within the State. Responding vendors may access this document at https://www.dps.state.ms.us/wp-content/uploads/Tenprint-ICD-V502R31_20180330-1.pdf.

D. Vendor Qualifications

14. **Mandatory:** Proposing Vendor must be an established, prime manufacturer of AFIS systems equal to or greater in size and scope to the solution being sought by this RFP No. 4063. Such equivalencies include, but are not limited to AFIS functionality, database size, transaction throughput, and identification accuracies.

15. **Mandatory:** Proposals will not be accepted from third-party manufacturer representatives, system integrators, or from manufacturers whose systems do not meet the equivalency requirements and productive use requirements established in this solicitation.

16. **Mandatory**: Proposing Vendor must name at least three (3) implementations of the proposed AFIS solution for U.S. state level public safety/law enforcement environments (Identification Bureaus). At least two (2) of the named implementations must have been within the past three years and must have been for or on behalf of a State Identification Bureau (SIB) similar in size and complexity to that of the State of Mississippi. At the time of the response to this RFP, the proposing vendor must be the current vendor for the named states/bureaus.

17. **Mandatory**: Proposing Vendor must provide a minimum of three (3) qualified U.S. state references who are using the proposed AFIS solution. Two of the three references must be similar in size and complexity to the State of Mississippi SIB. The third reference can be any current customer using the proposed AFIS solution. The forms for submitting references are in RFP 4063, Section IX.

18. Vendor must provide an introduction and general description of its company's background and the number of years spent providing the products and services sought by this RFP.

19. Vendor must be in the business of providing AFIS solutions that meet the technical specifications and associated services required by this RFP. Vendor must have been in business of providing such solutions for at least three years.

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 any pending actions against them.

E. Vendor Implementation Team and Work Requirements

23. Vendor must demonstrate that all team members have the necessary experience for design, installation, implementation, training and support of the services required by this RFP.

24. Vendor must identify the primary, key staff who will be responsible for the execution of the various aspects of the project, including but not limited to: project manager, development team, business analyst(s) and technical architect(s).

25. Describe team member roles, functional responsibilities, and experience with projects similar in size and scope to the services required by this RFP.

26. For each participating team 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 has the ability to communicate clearly in the English language both verbally and in written form.

28. Vendor must agree that all work performed in response to this procurement will be subject to the following requirements:

    a. No State data will be communicated to anyone who is not a U.S. citizen or lawful permanent resident (LPR) of the United States. State data includes, but is not limited to: biometric data, identity history data, biographic data, property data, and case/incident history data as defined in the CJIS Security Policy.

    b. State data will not be stored, accessed from, or transmitted out of the U.S. without the State's written permission, which must be provided in advance.

        1. The State retains the right to designate certain subsets of State data as being subject to additional storage, access or transmission restrictions at its sole discretion.

F. General Requirements

29. **Mandatory:** The proposed solution must support, comply, and be compatible with the FBI's NGI Rapback to accommodate any future decision by the State to implement Rapback functionality.

30. **Mandatory:** Proposing Vendors must request a copy of the NIST formatted sample records dataset by sending an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request.

31. **Mandatory:** Proposing Vendor must review the sample NIST formatted sample records dataset and attest that the data can be properly converted, stored, searched, and accessed by the proposed solution and that all costs and other considerations for the conversion are detailed in RFP Section VIII, Cost Information Submission.

32. **Mandatory:** Proposed solution must include the capability to process slap-only applicant transactions that do not include tenprint data and are not stored for future search.

33. **Mandatory:** The proposed solution must utilize ANSI/NIST/FBI record constructs and retain archives of records in those standard formats.

34. The proposed solution must provide configurable, role-based, administrative tools and controls and must be capable of interfacing with the MDPS Active Directory implementation for internal MDPS users for the purpose of authentication and privileging.

35. The proposed solution must manage and control biometric data using subject biometric identifiers as keys.

36. The proposed solution must provide efficient and cost-effective storage and retrieval.

37. The proposed solution must detect and provide alerts when systems, applications, equipment, or networks are interrupted or when there is a loss of power.

38. The proposed solution must enable the incremental enhancement/ addition/replacement of applications and workflows for friction ridge (finger, palm, latent), and facial data capture, iris, voice, scar, marks, and tattoos, facial recognition, and DNA biometric toolsets.

39. The proposed solution must store integrated subject biometric data (captured via the various biometric toolsets) that enables online inquiries and reporting based on integrated subject biometric data.

40. The proposed solution must be sized to meet current needs and must accommodate future growth.

41. The proposed solution must conform to national and international biometric standards.

42. The proposed solution must be capable of supporting and performing Livescan/Cardscan transaction certifications if and when DPS needs to move this functionality to AFIS from MCHS. Currently, MCHS performs Livescan certifications.

43. The proposed solution must be capable of interfacing with all external Livescan/Cardscan devices or other interfaces currently deployed in the legacy environment, without any changes by these Livescan/Cardscan devices or other interfaces.

44. The proposed solution must be capable of printing a fingerprint card (demographics and images) for any record in the AFIS database or in the archive.

45. Vendor agrees that any third party software, tools, utilities, or applications will name the State of MS as the licensee.

II. Functional Requirements

G. System Design – Functional Requirements

46. Vendor must agree to design and configure/develop the awarded solution to meet the AFIS functional requirements that are more fully described in this Attachment A, Section II, Functional Requirements.

47. Vendor must indicate when the proposed solution exceeds a cited functional requirement and describe the nature by which the solution exceeds the stated requirement.

H. MDPS Current AFIS Quantitative Information

48. Vendor must acknowledge the following tables that provide the basis for requirements regarding capacity and performance. Vendor should assume an eight percent (8%) per year growth rate for all transaction types.

Table 1 – Record type and Count 2018

MS DPS Record Type	Record Count 2018
Ten-Prints	695,597
Unsolved Latent	19,867

Table 2 – Annual MS DPS Transaction Counts

Type	Transaction Description	2014	2015	2016	2017
ARR	Arrest	88,400	85,100	79,821	72,829
APP	Applicant	135,300	146,700	160,948	154,658
DOC	Corrections	n/a	8,667	8,982	8,509
SOR	Sex Offender	523	2,806	167	139
EXP	Expunction	2,923	3,008	3,319	3,760
CON	Consolidation	n/a	509	316	1,559
Totals		**227,146**	**246,790**	**253,553**	**241,454**

Table 3 – Hardware and Licensing Requirements

Ref.	Workstation Type	Total	Locations
1	Tenprint Workstations	4	CIC
2	Latent Workstations	4	Crime Labs (Four Locations)
3	Administrative Workstations	1	CIC

I. Ten-Print

49. **Input**: The proposed solution must accommodate any and all means of input formats. Vendor must agree to the following for purposes of this procurement. Ten-print identification transaction data is transmitted as Electronic Biometric Transmission Specifications (EBTS) files or paper forms (e.g., inked cards) to AFIS for pre-processing. Inked forms will be converted to appropriate EBTS transactions, and the proposed solution must handle them as specified below:

    a. For paper forms (cards) submitted, the proposed solution must provide the user with the capability to scan the image portions of inked fingerprint and palmprint cards at 1,000 pixels per inch (ppi) using FBI-certified Appendix F scanner systems and assign a unique TCN (Transaction Control Number), pursuant to the EBTS.

    b. For paper forms (cards) submitted, the proposed solution must support the scanning of the entire front and back of the cards at 250 or 300 ppi as Type 20 records and link the image(s) with the friction ridge image entry per ID Input 1.

    c. For paper forms (cards) submitted, the proposed solution must provide the user with the capability of entering card field text, pursuant to the EBTS, and linking the text fields (Types 1 and 2) with the appropriate scanned images per ID Input 1 and 2.

    d. For paper forms (cards) submitted, after scanning and text entry are complete (ID Input 1 through ID Input 3), the proposed solution must automatically create a complete EBTS Transaction with the Record Types 1, 2, 14, 15, and 20, as appropriate, using an appropriate Type of Transaction (TOT).

    e. The proposed solution must be able to ingest EBTS transactions and parse them for compliance with the EBTS, to include checking for duplicate TCNs.

    f. The proposed solution must be able to quality check (i.e., fingerprint quality via NFIQ (NIST Fingerprint Image Quality), sequence, and presence of spurious fingers) the friction ridge images of ingested and created EBTS transactions against adjustable quality thresholds (NFIQ threshold and non-recoverable sequence errors).

    g. The proposed solution must forward the transactions that fail the automated quality checks to appropriate examiner work queues for examiner-assisted QC.

    h. The proposed solution must permit examiners to selectively pick a transaction from the QC queue and present the selected transaction's images within four seconds of the selection.

    i. The proposed solution must provide support to examiners performing QC activities such as adjusting sequence, correcting or establishing patterns, centering images, rejecting a transaction, and responding to the Livescan/Cardscan station when finished.

j. The proposed solution must log the NFIQ score for each rolled finger in a retrievable format to include finger number and all Type 1 field data, independent of the transaction passing or failing the automated QC.

k. The proposed solution must be able to respond to the noncompliant or unacceptable image quality transactions via an EBTS ERRT (Ten-Print Transaction Error).

l. The proposed solution must be able to forward the acceptable transactions to the local criminal records repository to solicit any name-based candidates via an EBTS transaction.

m. The proposed solution must be able to ingest EBTS responses from the criminal records repository.

n. The proposed solution must update the original ingested transaction with information from the criminal records repository response.

o. The proposed solution must update the log entry for each transaction with the results of each EBTS ingested.

p. The proposed solution must store a copy of each EBTS forwarded for processing in a temporary file.

q. The proposed solution must be able to ingest EBTS transactions received from the various Livescan and Cardscan devices and external systems (cross-jurisdictional searches).

r. The proposed solution must parse ingested EBTS transactions from external systems checking for compliance with the EBTS to include checking for duplicate TCNs.

s. The proposed solution must record a copy of each ingested transaction in the ANSI/NIST Archive.

t. The proposed solution must be able to ingest tenprint submission in the format that Livescan and Cardscan devices currently utilize, which is the MCHS tenprint format. See Section I.D. for access to MCHS interface control documents.

u. The proposed solution must be able to ingest and process ANSI/NIST Type-4, high-resolution grayscale fingerprint image, record types.

v. The proposed solution must be able to ingest and process ANSI/NIST Type-14, variable-resolution tenprint image, record types.

w. The proposed solution must be able to ingest and process ANSI/NIST Type-10, facial & SMT (scars, marks, and tattoos) image, record types.

x. The proposed solution must be able to ingest transactions for the registration and creation of a record of a sex offender when there may be no arrest or charges (out of state sex offender for registration). These registrations are stored in the criminal history as a registration.

y. The proposed solution must be able to ingest manual transactions that are exceptions to normal processing, such as the entry of arrests for juveniles only after and upon a conviction. *Normal* submission processing must not allow the saving of juvenile transactions.

z. The proposed solution must be able to ingest both tenprint and slap-only transactions for the purposes of applicant inquiry processing.

50. **Processing:** For purposes of this procurement, Vendor must agree to the following: The AFIS processes identification transactions that are received from the various Livescan/Cardscan devices and external systems. The various biometric modality data (fingerprint and palmprints) will be sent to the appropriate back-end matchers and the proposed solution must handle them as follows:

a. For all transactions, the proposed solution must *feature extract* all friction ridge images and create appropriate internal TP-TP searches of the matchers, and cascade TP-LT, and KP-LT internal searches based on the record types (4, 14, and 15) in the transaction.

b. The proposed solution must automatically execute all searches of the database with the transactions ingested during the input process.

c. If the TP-TP matcher score for a name-based searched candidate is above a settable threshold (#1), then the proposed solution must automatically declare a match.

d. If the TP-TP matcher score for a technical search candidate is above a settable threshold (#2), then the proposed solution must automatically declare a match.

e. If the matcher score for all candidates is below a settable threshold (#3), then the proposed solution must automatically declare a no-match.

f. If there is no automatic decision (match or no-match) and there are candidates with scores between Thresholds 2 and 3, then the proposed solution must create and move a verification package (original images and candidate images and information) to the appropriate examiner work queues for examiner-assisted verification for a settable number of candidates (up to 10), to include any candidate in score order.

g. The proposed solution must permit examiners to selectively pick a transaction from the verification queue and present the selected transaction's images for at least the search prints and the first candidates within 4 seconds of the selection.

h. The proposed solution must provide support for examiners to verify candidates for searches selected from the queue and to selectively manipulate the original image and the candidate image separately or in synchrony (i.e., zoom, magnify, and rotate, and adjust contrast, brightness, and sharpness) as well as use hyperlinked fields in the candidate entries to go to the Master ID cross-reference file or to a specific archived transaction.

i. The proposed solution must permit the examiners to print any search or candidate fingerprint set with Type 1 and Type 2 data.

j. In the case of an automatic or manual no-hit decision where the retention code is set to Y, the proposed solution must establish a new State Identification Number (SID).

k. The proposed solution must be able to ingest EBTS response transactions (SRE [Submission Results-Electronic] and ERRT) from the FBI, and any other external systems where a search was requested in Field 2.098 NDR and store an original copy of the response in the ANSI/NIST Archive.

l. The proposed solution must use the response information from the external systems to update the master identity files and the transaction log.

m. The proposed solution must establish and maintain a master identity for each subject enrolled, including links to all successfully processed transactions' TCNs, and associated SIDs.

n. The proposed solution must automatically log all search transaction results including the original Type 1 fields, time received, time at end of processing, and the results.

51. **Output:** For purposes of this procurement, Vendor must agree to the following: The AFIS prepares responses to all transactions received from Cardscans, Livescans, or other systems, etc. If a transaction fails to pass the various quality checks, it will have already generated an error message in the input stage.

a. The proposed solution must automatically prepare and return an SRE response containing the original TCN, ORI, and Cardscan/Livescan ID for all transactions where the subject was successfully searched – showing the results (for hit and no-hit).

b. The proposed solution must automatically forward any external system SREs and ERRTs to the submitting agency or department.

c. The proposed solution must automatically prepare and return an ERRT response containing the original TCN and Incident ID for all transactions where the transaction was not processable.

d. The proposed solution must automatically add response transactions (SRE and ERRT) to the ANSI/NIST Archive.

e. The proposed solution must automatically send an SRE to the appropriate criminal records repository system.

J. Ten-Print to Latent Inquiry Service Requirements

52. The Proposed solution must ensure that all identification transactions containing fingerprint or palmprint records (and marked as "add to proposed solution") will be automatically reverse-searched against the unsolved latent. This search occurs in the course of the input phase of ten-print identification services.

53. **Input:** The proposed solution must satisfy the ten-print to latent inquiry service requirements as described below.

a. The proposed solution must be able to ingest EBTS transactions as responses from searches made in response to ten-print identification service input.

b. The proposed solution must be able to ingest EBTS transactions from the FBI/NGI.

c. The proposed solution must record in a log the results of each EBTS ingested.

d. The proposed solution must store in a temporary file a copy of each EBTS forwarded to the AFIS.

e. The proposed solution must be able to ingest EBTS transactions received from the various latent stations.

f. The proposed solution must record a copy of each ingested transaction in the ANSI/NIST Archive in the EBTS compliant form in which it was received.

54. **Processing:** The proposed solution must satisfy the ten-print to latent inquiry service requirements as described below.

a. The proposed solution must add all transactions that are received from the FBI to the ANSI/NIST Archive.

b. The proposed solution must forward all transactions that are received from the FBI to the appropriate latent station.

c. The proposed solution must create an LCMS (Latent Case Management System) entry in the appropriate verification work queue for each transaction that is received.

d. The proposed solution must support examiners in selectively picking a transaction from the verification queue.

e. The proposed solution must support the examiners in the verification of candidates for searches selected from the queue by providing the associated friction ridge images (reverse search print and original latent image) within three seconds of the verification transaction selection.

f. The proposed solution must support the examiners in the verification of candidates for searches selected from the queue and to selectively manipulate the original image and the candidate image separately or in synchrony (i.e., zoom, magnify, rotate, contrast adjust, brightness adjust, reverse black and white, apply gamma correction, mirror [horizontal or vertical], sharpen/unsharpen, mark points of similarity, apply false color encoding based on image density, and generate histograms).

g. The proposed solution must permit the examiners to print:

   1. Any search latent at 1:1 or 5:1 size for latent images with case number and image number as well as time and date printed; or

   2. Any candidate fingerprint/palmprint set with Type 1 and Type 2 data for ten-print and palmprint cards.

h. The proposed solution must support the forensic examiner in selectively declaring a match, returning the transaction to the work queue, or forwarding the transaction to another examiner for confirmation or advice.

i. The proposed solution must automatically log all reverse friction ridge search transactions and the steps taken, the examiners involved, and the search results in the LCMS.

j. The proposed solution must support the preparation of court presentations when a match is found in any TLI (Ten-Print to Latent Inquiry) search.

k. The proposed solution must automatically log all TLI search transactions and the examiners' results in the system log and LCMS.

55. **Output**: The proposed solution must satisfy the ten-print to latent inquiry service requirements as described below.

a. The proposed solution must automatically prepare a LCMS report for all TLI searches.

b. The proposed solution must support the examiner in selecting to mark the case as closed or simply saving and closing the LCMS file.

c. The proposed solution must maintain a searchable log of all TLI searches submitted to the proposed solution by external systems and to the latent stations from the proposed solution.

K. Latent Inquiry Service Requirements

56. The following descriptions represent the State's expectations regarding the overall capabilities of the proposed solution for latent inquiry services. The proposed solution must accommodate the latent inquiry service processes as described below.

    a. Proposed solution must accommodate Latent to Latent Inquiry (LI) searches that use latent fingerprint and palmprint samples collected at crime scenes, disaster victim fingerprints, as well as fingerprints from deceased subjects collected by morgues, to determine whether the subject has been previously encountered and enrolled in the AFIS. External agencies, using Universal Latent Workstations (ULW), can also submit LI searches.

    b. For input, the proposed solution must accommodate the following process: In each case, along with an image, other case-related information must be supplied, such as date collected, unique identification number of the image or sample, the point of contact where results should be reported, collection location, crime type or morgue case type, etc. The images and information will be entered though a workstation and transmitted to the proposed solution via an LCMS. The LCMS will provide tracking of the processing of the latent through all searches including maintaining a log of searches, image processing, candidates, etc. The LCMS will provide the ability for examiners to query status and other attributes of latent submittals and cases as well as to return to open cases whenever, and as often as they see fit. Transactions entered through ULWs from external agencies will be entered through the LCMS for tracking and reporting purposes.

    c. For processing, the proposed solution must accommodate the following processes: The examiner will forward the latent transactions with the impression and tracking information to the LCMS for forensic processing as an LFFS (Latent Friction Ridge Feature Search) transaction type. Vendor must respond to each item.

        1. The LCMS will queue the latent transaction for a latent examiner to select and process, or if the transaction originated from a ULW or cross-jurisdictional partner, it will be auto-launched without any examiner action – as a lights-out remote search. Because the proposed solution will not know whether or not the remote submitter made an identification, these submittals will not be automatically forwarded to the FBI and the originating agency must resubmit them for forwarding.

        2. The examiner will perform pre-search steps (rotate, crop, mark and edit minutiae, etc.) before submitting a search. This will be performed using latent editing software integrated into the proposed solution software, including Photoshop.

        3. The examiner will be able to limit the search by crime type, finger or palm position, geographical region where the crime was committed, and other traditional parameters or elect to use no search limitations. The proposed solution will search the record against known records as well as against unsolved latent records. The known record files for latent searches to run against, sometimes referred to as the "latent cognizant files," will contain up to three instances of known fingerprints and one of palmprints enrolled in the system rather than just a single set of best images.

d. For output the proposed solution must prepare responses to all LI transactions received. The examiners will be given the opportunity to forward unsolved latents to the FBI, to add them to the proposed solution unsolved latent file, to edit and resubmit them, or to save them for future work. If there is a match, then the identity of the subject is returned to the submitting agency. If there is no match and the latent sample is selectively added to the unsolved latent file, it will be reverse searched against all subsequent transactions that include fingerprint and palmprint data.

57. **Input**: The proposed solution must satisfy the following latent inquiry service requirements.

a. The proposed solution must support the examiners in creation of a new case in the appropriate LCMS to include entering data in the case information fields as well as the following image fields per image:

1. Latent collection location.
2. "Method of processing" using a pull-down menu.

b. The proposed solution must support the ingesting of digital images with latent fingerprints or palmprints captured at various scales as Type 13 images into a specific case using a pull-down menu of cases associated with the examiner's agency.

c. The proposed solution must support the scanning of latent friction ridge material into Type 13 images at 1:1 scale, 1,000 ppi, 8-bit gray scale, along with a ruler for calculating/verifying scale and resolution into a specific case using a pull-down menu of cases associated with the examiner's agency.

d. The proposed solution must support the imaging with a high resolution digital camera of latent friction ridge material as Type 13 images at 1:1 scale, 1,000 ppi, 8-bit gray scale, along with a ruler for calculating/verifying scale and resolution into a specific case using a pull-down menu of cases associated with the examiner's agency.

e. The proposed solution must support the ingesting of latent case textual information linked to a latent image as Type 2 fields from a text file or the keyboard into a specific case using a pull-down menu of cases associated with the examiner's agency.

f. The proposed solution must support the scanning of inked fingerprints into Type 13 images from deceased persons at 1,000 ppi, 8-bit gray scale into a specific case using a pull-down menu of cases associated.

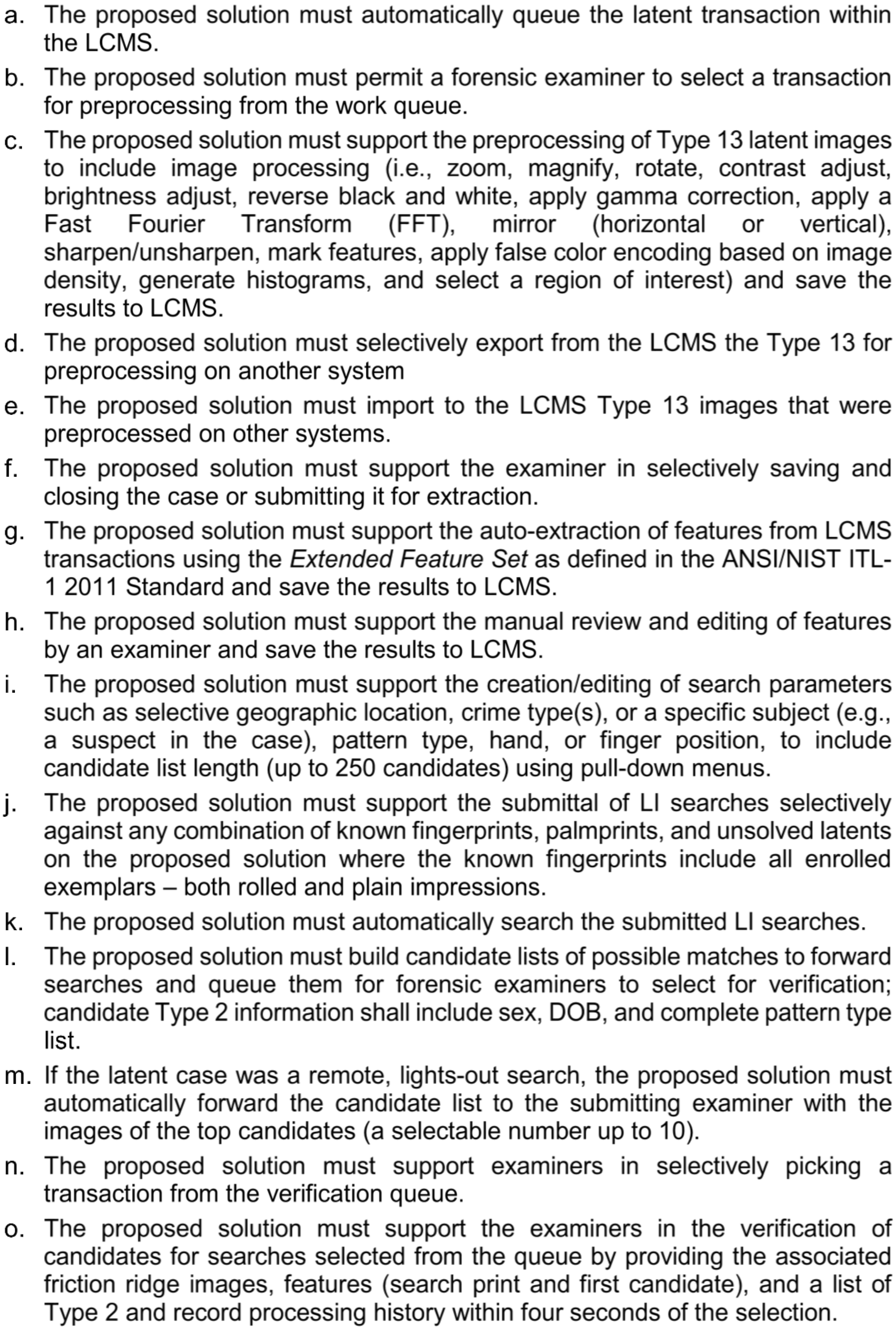
g. The proposed solution must support the ingesting of crime scene and object reference images selectively as Type 20 and Type 21 images for use in the LCMS into a specific case using a pull-down menu of cases associated.

h. The proposed solution must ingest LFFSs submitted from ULWs at outside agencies, after logging them into the LCMS, set them for auto run.

i. The proposed solution must support the examiner in selectively creating an LFFS package for each latent image in a case, with the appropriate Type 1, Type 2, Type 13, and Type 20 records, and store it in the LCMS as an LFFS.

j. The proposed solution must update the LCMS logs with the results of each step in the forensic services input process.

58. **Processing**: The proposed solution must satisfy the following latent inquiry service requirements.



a. The proposed solution must automatically queue the latent transaction within the LCMS.

b. The proposed solution must permit a forensic examiner to select a transaction for preprocessing from the work queue.

c. The proposed solution must support the preprocessing of Type 13 latent images to include image processing (i.e., zoom, magnify, rotate, contrast adjust, brightness adjust, reverse black and white, apply gamma correction, apply a Fast Fourier Transform (FFT), mirror (horizontal or vertical), sharpen/unsharpen, mark features, apply false color encoding based on image density, generate histograms, and select a region of interest) and save the results to LCMS.

d. The proposed solution must selectively export from the LCMS the Type 13 for preprocessing on another system

e. The proposed solution must import to the LCMS Type 13 images that were preprocessed on other systems.

f. The proposed solution must support the examiner in selectively saving and closing the case or submitting it for extraction.

g. The proposed solution must support the auto-extraction of features from LCMS transactions using the *Extended Feature Set* as defined in the ANSI/NIST ITL-1 2011 Standard and save the results to LCMS.

h. The proposed solution must support the manual review and editing of features by an examiner and save the results to LCMS.

i. The proposed solution must support the creation/editing of search parameters such as selective geographic location, crime type(s), or a specific subject (e.g., a suspect in the case), pattern type, hand, or finger position, to include candidate list length (up to 250 candidates) using pull-down menus.

j. The proposed solution must support the submittal of LI searches selectively against any combination of known fingerprints, palmprints, and unsolved latents on the proposed solution where the known fingerprints include all enrolled exemplars – both rolled and plain impressions.

k. The proposed solution must automatically search the submitted LI searches.

l. The proposed solution must build candidate lists of possible matches to forward searches and queue them for forensic examiners to select for verification; candidate Type 2 information shall include sex, DOB, and complete pattern type list.

m. If the latent case was a remote, lights-out search, the proposed solution must automatically forward the candidate list to the submitting examiner with the images of the top candidates (a selectable number up to 10).

n. The proposed solution must support examiners in selectively picking a transaction from the verification queue.

o. The proposed solution must support the examiners in the verification of candidates for searches selected from the queue by providing the associated friction ridge images, features (search print and first candidate), and a list of Type 2 and record processing history within four seconds of the selection.

p. The proposed solution must support the examiners in the verification of candidates for searches selected from the queue and allow them to selectively manipulate the original image and the candidate image separately or in synchrony (i.e., zoom, magnify, rotate, contrast adjust, brightness adjust, reverse black and white, apply gamma correction, apply FFT, mirror [horizontal or vertical], sharpen/unsharpen, mark points of similarity, apply false color encoding based on image density, generate histograms, turn on and turn off all minutiae, and dMS DPSlay matching minutiae).

q. The proposed solution must support the forensic examiner in selectively declaring a tentative match, returning the transaction to the queue, forwarding the transaction to another examiner for confirmation or advice, or editing and resubmitting the search to include manually editing the feature set.

r. The proposed solution must support a second forensic examiner selectively selecting a confirmation-verification package and using the tools declaring a match, non-match, or elimination; or editing and resubmitting the search to include manually editing the feature set.

s. The proposed solution must automatically log all forward friction ridge search transactions and the steps taken, the examiners involved, and the search results in the LCMS.

t. The proposed solution must support the preparation of court presentations when a match is found in any forensic friction ridge search.

u. The proposed solution must automatically log all LI search transactions and the examiners' results in the system log and LCMS.

59. **Output**: The proposed solution must satisfy the following latent inquiry service requirements.

a. The proposed solution must automatically prepare an LCMS report for all forensic searches that lead to an identification.

b. The proposed solution must support the examiner in selecting to:

1. Add new unsolved latents to the unsolved latent file with a link to the appropriate LCMS records;
2. Delete the record, or
3. Simply save and close the LCMS file.

c. The proposed solution must support the selective forwarding of LFFS transactions to the FBI, first using an LPNQ transaction, if appropriate, or to other systems (e.g., cross-jurisdictional partners) using the EFS or ULW to generate a more appropriate Type 9 record.

d. The proposed solution must support the ingesting of any response to a Latent Penetration Query (LPNQ) transaction (a Latent Penetration Query Response (LPQR) TOT) automatically forwarding it to the appropriate LCMS case.

e. The proposed solution must support the ingesting of any response to an LFFS transaction (SRL or ERRL TOTs) automatically forwarding it to the appropriate LCMS case.

f. The proposed solution must maintain a searchable log of all forensic transactions submitted (along with the responses) to the proposed solution and to external systems in the system log and LCMS.

g. The proposed solution must support the selective forwarding of FBI and other external responses (SRL TOTs) to latent transactions to the appropriate verification queue.

h. The proposed solution must automatically log all LI search transactions and the examiners' results in the system log and LCMS.

L. NIST Image Retrieval

60. **Input:** The proposed solution must satisfy the following requirements for NIST image retrieval.

a. The proposed solution must be able to ingest EBTS from the criminal records repository and parse them for compliance with the EBTS to include checking for duplicate TCNs.

b. The proposed solution must be able to respond to the noncompliant transactions via an EBTS ERRT to the criminal records repository.

c. The proposed solution must provide the ability for the user to create transactions using pull-down menus or manually enter the Type 2 fields.

d. The proposed solution must forward the acceptable transactions for processing.

e. The proposed solution must record in a log the results of each EBTS ingested.

f. The proposed solution must store in a temporary file a copy of each EBTS forwarded for processing.

g. The proposed solution must be able to ingest EBTS transactions received from the various Livescan or input devices and external systems, such as mugshots sent from a booking station.

h. The proposed solution must record a copy of each ingested transaction in the ANSI/NIST Archive in the fully EBTS compliant form in which it was received.

61. **Processing:** The proposed solution must satisfy the following requirements for NIST processing.

a. The proposed solution must process EBTS transactions and determine whether the requested image is available.

b. If the image is not available, proposed solution must forward image retrieval transactions to the FBI's NGI.

c. The proposed solution must be able to ingest responses from the NGI.

d. The proposed solution must use the response information from the FBI NGI processing to update the transaction log.

62. **Output:** The proposed solution must satisfy the following requirements for NIST output.

a. The proposed solution must automatically forward any internal or external system response transactions to the submitting criminal records repository or user/ORI (Originating Agency).

b. The proposed solution must automatically add response transactions to the ANSI/NIST Archive.

M. Mobile ID

63. Vendor must agree that mobile ID workflow is for the rapid searching of AFIS and, in turn, the FBI. If no identity is determined at AFIS, the transaction can be submitted

to the FBI as a Ten-Print Fingerprint Image Search (TPIS) (for a 2-minute FBI turnaround) against the entire NGI repository.

64. **Input:** Vendor must agree that mobile data will be transmitted as EBTS files. These will be rapid turnaround transactions set to the highest priority by the AFIS, if not already set as such by the submitting device. At the AFIS all records will be parsed for compliance with the EBTS. Transactions that fail the parsing test will be logged and returned to the submitting device with an ERRT response.

    a. The proposed solution must be able to ingest TPIS transactions and parse them for compliance with the EBTS to include checking for duplicate TCNs.

    b. The proposed solution must be able to forward the acceptable transactions to the local criminal records system to solicit any name-based candidates.

    c. The proposed solution must be able to ingest EBTS responses from the criminal records system.

    d. The proposed solution must process the acceptable TPIS transactions at the priority set to 1 (the highest priority value).

    e. The proposed solution must record in a log the results of each TPIS transaction ingested.

    f. The proposed solution must store in a temporary file a copy of each TPIS forwarded for processing.

    g. The proposed solution must be able to ingest TPIS transactions received.

    h. The proposed solution must record a copy of each ingested TPIS transaction in the ANSI/NIST Archive in the fully EBTS compliant form in which it was received.

65. **Processing:** Vendor must agree that the proposed AFIS will process Mobile ID transactions received at the highest system priority level. The fingerprint images will be feature extracted and searched “without add.” Matcher results will be made available via EBTS responses. Based on the submittal data, the transaction may or may not be forwarded to the FBI for further searching against their Identification system.

    a. The proposed solution must “feature extract” the fingerprint images and create an appropriate internal search of the database (TP-TP).

    b. The proposed solution must automatically prepare and return an ERRT response containing the original TCN and Incident ID for all transactions that were not process-able.

    c. The proposed solution must automatically execute all TP-TP searches using the features extracted.

    d. If the matcher score for a name-based candidate or a technical candidate is above a settable threshold, the proposed solution must automatically add that subject to the candidate list, with any name-based strong candidate in the number one position.

    e. The proposed solution must forward transactions to the FBI’s NGI if a search was requested and no match was made at AFIS.

    f. The proposed solution must ingest the FBI responses (SRT, TPRR, and ERRT).

g. The proposed solution must automatically log all TPIS search transaction results (local and FBI) to include the Type 1 fields, time received, time logged at end of processing, and the results.

66. **Output**: – Vendor must agree that the proposed AFIS will prepare responses to all Mobile ID transactions received. If the transaction failed to pass the various checks above, then it will have already produced an error message, pursuant to the EBTS.

a. If there are any candidates available, then the proposed solution must automatically return a response TOT with the five highest (configurable) scoring candidates and associated mug shots, if available.

b. If there are no candidates available, then the proposed solution must automatically return a response TOT with that information.

c. The proposed solution must automatically forward FBI responses (SRT, TPRR, and ERRT) to the originating device.

d. The proposed solution must automatically add response transactions (SRT, TPRR, and ERRT) to the ANSI/NIST Archive.

III. TECHNICAL REQUIREMENTS

A. System Design – Technical Requirements

67. Vendor must agree to design and develop the awarded solution to meet the AFIS technical requirements that are more fully described in this Attachment A, Section III, Technical Requirements.

a. Vendor must indicate when the proposed solution exceeds a cited technical requirement.

B. Storage Capacity

68. Proposed solution must accommodate storage capacities that are relevant to the following areas of the proposed AFIS system architecture, including:

a. ANSI/NIST Archive

b. The templates/features loaded in the matchers

69. Proposed solution must be designed to accommodate an ANSI/NIST Archive of all MS DPS input and output transactions through the life of the contract

70. The Vendor must perform the appropriate analysis to determine the design requirements in terms of terabytes as a function of transaction type using the quantitative data specified in this document.

a. Refer to Tables 1 and 2 of this document. Vendor must use these tables to calculate storage requirements based on these record counts and transaction counts.

C. Throughput and Response

71. Proposed solution must meet the currently contracted performance and response times as shown in the tables below:

Table 4 – Currently Contracted AFIS Transactional Throughput Capabilities

Ref.	MDPS Record Type	Peak Hour	Per Day	Response Time/Peak Load
1	Tenprint Submissions	150	1,500	2 minutes
2	Tenprint Technical Searches	N/A	N/A	2 minutes
3	Tenprint-to-Latent Inquiries	N/A	1,500	5 minutes
4	Palm Submissions	50	500	10 minutes
5	Latent Inquiries	10	50	5 minutes
6	Latent Palm Inquiries	2	10	20 minutes
7	Mobile Identification Inquiries	N/A	N/A	2 minutes
Admin Functions				
8	Expunctions/Deletions	2	20	N/A
9	Consolidations	2	20	N/A

Table 5 – Currently Contracted Response Times Per Transaction Type – Peak Load

Transaction Class Types	Response Time Requirements Under Peak Load
Criminal TP-TP	2 minutes
TP-LT	5 minutes
LT-TP	5 minutes
Palm LT-KP	20 minutes
Criminal KP-LT	10 minutes
Rapid/Mobile ID TP-TP	2 minutes

D. Accuracy

72. Vendor must agree that for this procurement, accuracy requirements will include three definitions:

a. True Match Rate – the probability that a true match will be found when it is in the background reference file (also known as a repository). This term replaces older terminology such as matcher reliability or true accept rate.

b. Failure to Match Rate – the probability that a search will not return a true match when the true match is in the reference file. The failure to match rate is 100 percent minus the true match rate.

c. Selectivity – the number of candidates that will be examined to determine the true match rate. While the system administrators will be able to selectively change the length of candidate lists by transaction class, and by threshold scores, during testing, system accuracy will be measured using the selectivity numbers shown in Table 6 below.

73. The proposed solution must meet the performance and accuracy requirements during peak load times as presented in Table 6 below:

Table 6 – Response Times - Peak Load and Accuracy Requirements

Transaction Class Type	Response Time Requirements Under Peak Load	Selectivity	True Match Rate
Criminal TP-TP	2 minutes	1	99.9%
Criminal KP-LT	10 minutes	10/25	93%/100%
TP-LT	5 minutes	10/25	93%/100%
LT-TP	5 minutes	10/25	93%/100%
Palm LT-KP	20 minutes	10/25	93%/100%
Mobile ID TP-TP	2 minutes	8	99.9%

E. Safety

74. Vendor must agree that all hardware configuration items delivered as a part of the proposed solution will conform to the appropriate U.S. Underwriters Laboratory (UL LLC) standards for electronic devices and be so certified.

75. Vendor must agree that all required grounding will conform to the manufacturer’s specifications and recommendations.

F. Hardware

76. Vendor must agree to provide all equipment and software necessary to satisfy the proposed system requirements at the DPS primary and remote operational site(s), as well as the Vendor recommended Continuity of Operations Plan (COOP) site.

a. Vendor agrees that *necessary equipment and software* includes, but is not limited to servers, communications gear, workstations, printers, and all other equipment required for full implementation of the proposed solution.

b. Vendor agrees to provide all necessary cabling, connectors, and ancillary devices necessary for full operations of the proposed solution.

77. Vendor must agree that all recommended hardware will be commercially available from providers other than the Vendor.

78. Vendor must agree that MDPS reserves the right to purchase recommended hardware from providers other than the Vendor.

79. Vendor must agree that each ten-print workstation will have:

a. A microprocessor with at least 2.8 GHz clock speed and at least four cores;

b. Built in graphics or a graphics board with at least 512 MB of onboard memory;

c. 16 GB of internal RAM;

d. Two 24-inch or larger flat panel display with at least 1920×1200 resolution and digital visual interface;
e. 1 Gigabit Network Interface Card;
f. At least one 500 GB hard disk drive;
g. Wireless keyboard and mouse;
h. FBI EBTS Appendix F certified printer and certified software;
i. The most recent version of the operating system that was used to certify the scanner;
j. A full suite of the Vendor ten-print software, and the optional ability to use the Vendor latent software;
k. Installed Microsoft Office™ Version 2016 or later using the MDPS Microsoft Enterprise Agreement license;
l. Installed latest version of Microsoft Endpoint security utilizing the MDPS Microsoft Enterprise Agreement license.

80. Vendor must agree that each latent workstation will have:

a. A microprocessor with at least 3.2 GHz clock speed and at least four cores;
b. Built in graphics or a graphics board with at least 1 GB of onboard memory;
c. 16 GB of internal RAM;
d. Two 24-inch or larger flat panel display with at least 1920×1200 resolution and digital visual interface;
e. 1 Gigabit Network Interface Card;
f. At least one 750 GB hard disk drive;
g. Wireless keyboard and mouse;
h. FBI EBTS Appendix F certified flatbed scanner;
i. FBI EBTS Appendix F certified printer and certified software driver;
j. The most recent version of the operating system that was used to certify the scanner
k. Adobe Photoshop Elements™ Version 9 or later;
l. A full suite of the Vendor latent software, and the optional ability to use the Vendor ten-print software;
m. Installed Microsoft Office™ Version 2016 or later using the MDPS Microsoft Enterprise Agreement license;
n. Installed latest version of Microsoft Endpoint security utilizing the MDPS Microsoft Enterprise Agreement license.

81. Vendor must agree that each administrative workstation will have:

a. A microprocessor with at least 2.4 GHz clock speed and at least four cores;
b. Built in graphics or a graphics board with at least 256 MB of onboard memory;
c. 8 GB of internal RAM;
d. One 24-inch or larger flat panel display with at least 1920×1200 resolution and digital visual interface;
e. 1 Gigabit Network Interface Card;
f. At least one 500 GB hard disk drive;

g. Wireless keyboard and mouse;

h. The most recent version of the operating system that was used to certify the scanner;

i. Installed Microsoft Office™ Version 2016 or later using the MDPS Microsoft Enterprise Agreement license;

j. Installed latest version of Microsoft Endpoint security utilizing the MDPS Microsoft Enterprise Agreement license.

82. Vendor must agree that each card printer will have:

a. At least two drawers/trays to support fingerprint and palmprint card stock simultaneously without having to physically change trays;

b. FBI Appendix F Certification;

c. Connectivity to a workstation or server running the most recent version of the operating system that was used to certify the printer

d. Simultaneous two-sided print capability;

e. 1 Gigabit Network Interface Card;

f. At least 256 MB of memory;

g. The ability to print cards at least 1000 ppi resolution using a compatible printer driver for the specific model printer listed in the FBI Appendix F Certification.

G. Environmental

83. Vendor must agree that each workstation will have a UPS that can support the workstation for up to 20 continuous minutes in the event of a loss of building power.

84. Vendor must agree that each workstation UPS will provide the user with a signal in cases where the UPS has been the only source of power to the device for ten continuous minutes.

85. Vendor must agree that each workstation will automatically shut down properly, based upon the receipt of a 10-minute warning, if the operator does not initiate a shutdown within 10 minutes of the signal when the UPS has continuously remained the only source of power to the device for that time.

86. Vendor must agree that the verification stations will be able to operate in an office environment, without any requirement for supplemental air conditioning or noise suppression:

a. 68° to 76° temperature with a relative humidity between 40 and 60 percent.

b. Noise below 70 dBA measured at the workstation suite.

H. Backup and Recovery

87. Vendor must agree that the proposed solution will need to be backed up (data and system configurations) at least daily for continuity of operations considerations. Copies of the backup tapes will be stored off site from the central site (primary and disaster sites) to increase the likelihood of their availability in case of a natural or man-made disaster. Note: MDPS currently uses Veeam for Backup/Recovery and would prefer the Vendor to use this as well for the proposed solution.

88. Vendor must agree that the proposed solution will permit the system administrators to selectively create full and incremental backups of any and all files on the AFIS, to include administrative files, ANSI/NIST Archive files, transaction files, master identity

indexes, transaction results, and the back-end matcher files, to include feature sets and matcher identity indexes, without impacting functionality of the system.

89. Vendor must agree that the proposed solution will permit the system administrators to selectively support the recovery of any and all files from the backups to the appropriate locations.

90. Vendor must agree that the proposed solution will maintain synchrony between the primary AFIS site and the disaster recovery site to ensure that each and every transaction successfully enrolled in the operational site is still available in case of a switchover to the other AFIS site.

91. Vendor must provide a backup solution that will allow MDPS to create archive tapes for offsite storage.

I. Service Availability and Restoration

92. For the initial term and any extended terms of service, the Vendor must agree that, except as the result of a catastrophic event, the proposed solution will provide at least 99.8 percent availability of all AFIS services, to be measured monthly.

93. Vendor agrees to include as unavailable time:

    a. Any scheduled outages for preventive maintenance;

    b. Planned upgrades where the AFIS users do not have access to and the use of AFIS services.

94. For purposes of this requirement, “catastrophic event” is defined as a natural or man-made disaster that destroys both the primary and the disaster recovery AFIS sites or renders both unusable due to fire, water damage, earthquake, radioactive leak, large-scale power outage, declared medical pandemic, or a large-scale communications infrastructure outage (telephones and Internet access). Large-scale means at least affecting the city where the site is located.

J. Interfaces

95. In the implementation of the proposed solution, Vendor must agree to provide, implement, test, and make operational each of the key interfaces and exchanges in the proposed solution, as described below:

    a. FBI NGI: EBTS;

    b. MCHS: To receive a copy of the MCHS Interface Control Document, proposing vendors must send an email request to jeannie.williford@its.ms.gov.;

    c. MCHS Tenprint: To receive a copy of the MCHS Tenprint Interface Control Document, proposing vendors must send an email request to jeannie.williford@its.ms.gov.;

96. If and when Rapback functionality is implemented by the State, the proposed solution must be compatible with and support NGI Rapback functionality through either:

    a. Its interface with MCHS; or

    b. An interface with NGI Rapback program, without requiring a major upgrade or system replacement.

K. Standards

97. Below are the minimum standards that apply to the current State AFIS solution. Proposed solution must comply not only with the standards named below, but must comply with any and all subsequent federal or state issuances and/or updates that may take place during the course of this procurement.

    a. American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, Update 2015.

    b. Electronic Biometric Transmission Specification (EBTS), IAFIS-DOC-01078-10.0.8. September 30, 2017.

    c. IAFIS-IC-0110 (V3.1), October 4, 2010. FBI Wavelet Scalar Quantization Compression Standard for 500 ppi fingerprint images.

    d. IS 10918-1, 1994. Joint Photographic Experts Group (JPEG) – Compression standard for continuous tone (e.g., photograph) images.

    e. IS 15444-1, 2001. Joint Photographic Experts Group (JPEG 2000) – Compression standard approved by the FBI for 1,000 ppi fingerprint images.

    f. NIST Best Practice Recommendation for the Capture of Mugshots. NISTIR 6322. Version 2.0. June 1, 1999.

    g. FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.6, CJIS Security Policy, Version 5.6, dated June 5, 2017.

    h. State of Mississippi Enterprise Security Policy

        1. For access to the State of Mississippi Enterprise Security Policy, send an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request.

    i. For hosted services, the AFIS design must be compliant with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy;

        1. For access to the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, send an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request

    j. MDPS Information Security Plan

        1. For access to the MDPS Information Security Plan, send an email request to greg.nations@dps.ms.gov. Include a reference to this RFP requirement as justification for your request.

98. Proposed solution must comply with the most recent form of any and all regulatory standards that apply to the AFIS technologies sought by this RFP, whether or not they are defined by this RFP.

L. Administrative Functions

99. The proposed solution must accommodate the need for system administrators (Provider and MDPS) to perform the necessary administrative functions, including but not limited to creating and maintaining user accounts, backing up and restoring files, exporting files, generating reports, etc.

100. **Input:** AFIS administrators must be able to use input workflows to test new and modified types of transactions (TOTs). The TOTs can be any of those ingested by or created as output by any other workflow. They may be sent to the AFIS. The

format is the normal TOT name with a T appended to it (***T) to signal all systems that it is a test transaction and thus should not be added to any system.

a. The proposed solution must be able to ingest test EBTS transactions from the criminal record repository and parse them for compliance with the proposed solution to include checking for duplicate TCNs.

b. The proposed solution must be able to respond to the noncompliant Test transactions via an EBTS error transaction (ERRT) to the criminal record repository or other submitter.

c. The proposed solution must be able to forward the acceptable Test transactions to the originator.

d. The proposed solution must log the results of each Test EBTS ingested.

101. **Processing**: The proposed solution must locally process all submitted test transactions.

a. The proposed solution must process the test EBTS transactions received from the devices and process them.

b. The proposed solution must process the test transaction – without adding or changing the archive, the matcher repositories, or any indexes.

c. The proposed solution must update the transaction log with the processing results.

102. **Output**: The proposed solution must prepare responses to all test submitted transactions.

a. The proposed solution must automatically generate and forward the appropriate system response transaction to the submitting criminal record repository.

b. If the Test Transaction is marked to be forwarded to the FBI, the proposed solution must automatically forward it as designated during the system design.

c. The proposed solution must ingest all responses received from the FBI and forward them to the appropriate device.

d. The proposed solution must update the transaction log with the processing results.

103. **System Administrator Input Requirements**: The proposed solution must accommodate all routine and special functions native to the present AFIS, and/or the equivalent upgraded functions native to the proposed solution.

a. The proposed solution must permit the system administrators to selectively set up and manage at least ten (10) classes of users (e.g., latent supervisor) with configurable permissions per class.

   1. Must be based on Active Directory groups linked to MDPS Active Directory accounts for centralized user management and single-sign-on.

b. The proposed solution must support the system administrator in assigning workflows and within workflows specific TOTs to default priority queues – with up to nine priorities to conform to the ANSI/NIST Standard for Field 1.006: “The values shall range from “1” to “9”, with "1" denoting the highest priority. The default value shall be defined by the agency receiving the transaction.”

c. The proposed solution must support the system administrator in maintaining and redefining the configuration parameters for Scoring Thresholds 1, 2, 3, and 4 as appropriate.

d. The proposed solution must support the system administrator in maintaining and changing QC thresholds for ten-prints and separately for palmprints and slap prints.

e. The proposed solution must support the system administrator in maintaining and changing default candidate lengths for verification, separately for ten-prints, LIs, and TLIs.

f. The proposed solution must support the system administrator in maintaining and changing a selectable second-level verification per International Standards Organization (ISO) standards.

g. The proposed solution must support the system administrator in selectively reviewing and printing the AFIS logs. Reviewing and printing may be organized by any or all of the following: time, date, user, transaction type, file-accessed name, device logged into, problem reports, transaction control number, and transaction results.

h. The proposed solution must enable the system administrator to selectively back up IT, biographic, ANSI/NIST archive, and forensic files at all system levels from workstations to the AFIS.

i. The proposed solution must support the system administrator in selectively restoring IT, biographic, ANSI/NIST Archive, and forensic files.

j. The proposed solution must allow the system administrator to selectively ingest any supported transactions, individually or in bulk, and process them as appropriate to the TOT.

k. The proposed solution must permit the system administrator to selectively cancel programs that are not responding and restart any program or computer.

l. The proposed solution must support the forensic system administrator in selectively exporting “known” files in bulk or individually.

m. The proposed solution must support the system administrator in selectively exporting “unknown” (latent) files in bulk or individually.

n. The proposed solution must support the systems administrator in preparing selective reports for, at a minimum:

   1. Selectable time periods and classes of services;
   2. Use patterns of the AFIS; and
   3. For aggregating reports so they can be edited, merged with other reports, and printed.

o. The proposed solution must support automated logging and system administrator selective reporting on the following information:

   1. Use by time, person, functionality, etc.;
   2. Viruses encountered – at the device level; and
   3. All events associated with unsuccessful login attempts, at the device level.

p. The proposed solution must support automated logging and system administrator selective reporting on the following information:

   1. Disk memory used, free, and as-built totals by system and component:

a. ANSI/NIST Archive;

b. Temporary files; and

c. The LCMS.

2. Matcher memory used, free, and totals by system, by component, and by modality (e.g., reverse palm search matchers).

q. The proposed solution must support automated logging and system administrator selective reporting on the following information:

1. A record of abnormal shutdown of any computer, along with any available diagnostics;

2. Number and percentage of transactions by class that failed/passed parser and image quality checks; and

3. Configuration changes to server, database, tools, utilities, and application parameters.

r. The proposed solution must support automated logging and system administrator selective reporting on the following information: NFIQ scores by finger, TOT, ORI, and/or time.

s. The proposed solution must support automated logging and system administrator selective reporting on the following information: Number of transactions, searches by class, hit rate by class, hit rate by TOT, error rate in processing transactions, and current size of each repository to include available space, selectively for one or more system elements, or the entire AFIS.

t. The proposed solution must support the selective production of reports from all workflows and administrative functions:

1. To a specified color or gray-scale printer;

2. To a file using comma-separated format for future use including editing and merging with other such files; and

3. Saving any and all reports as an Adobe Portable Data Format (PDF) file;

u. The proposed solution must offer AFIS management the ability to easily track, monitor, and produce reports on the types of ten-print, latent, and administrative activities listed below in Item M, Reports.

v. The proposed solution must permit administrators to design their own report formats from pull-down menus.

w. The proposed solution must permit administrators to select auto synchronization of system time across all AFIS elements that have or use time clocks (e.g., servers, workstations, and logs) on a selectable frequency (between 6 hours and 24 hours).

M. Reports

104. Vendor must provide access to authorized State staff, the Remote Site administrators, FBI auditors, and other authorized personnel to inspect the repository, the log of transactions and performance/ throughput rates, and user-level access history in order to allow State to generate predefined (canned) reports and create ad hoc reports.

105. At a minimum, the proposed solution must provide the following reports by workflow and type of transaction (TOT) and user must be allowed to select date ranges.

a. Number of transactions received and processed;

b. Number of hit/no hit transactions;

c. Number of transactions sent to the FBI (and other national databases), number of responses received, percentage of responses that were hits;

d. Number of transactions by day/week/month/quarter/year and average hour versus peak hour; and

e. Number of transactions processed by crime type.

106. The proposed solution must support the latent examiners and system administrators in selectively reporting on latent case management status over the life of the system, or any specified period of time and must report at a minimum:

a. Number of open and closed cases;

b. Number of cases closed due to a match;

c. Expiration of associated data due to statute of limitations or other reasons;

d. Average number of latent images per open case;

e. Maximum number of latent images per case;

f. Percentage of capacity used at various levels;

g. Number of cases within 90, 60, and 30 days of eclipsing their associated statute of limitations;

h. Average number of minutiae per latent finger or palm;

i. Maximum and minimum number of minutiae per latent finger or palm;

j. Number of searches executed; and

k. Average number of searches executed per latent image.

107. The proposed solution must allow the system administrator to generate reports on capacities and sizes and specified date ranges and must provide at a minimum:

a. Criminal, ID slaps, and/or tactical submissions by:

1. Number of individuals in databases and/or archives by ten-print, known palms, unknown palms, and unsolved latent records;
2. Number of fingers in databases and/or archives by ten-print, known palms, facial images, and unsolved latent records (fingerprints and palmprints);
3. Sex of individuals in databases and/or archives by ten-print, known palms, and facial images; and
4. Average image quality (using NFIQ and Vendor metrics) for rolled fingerprints and flats for databases or archives by finger and averaged across both hands.

b. For databases, archives, and matchers:

1. Sizes and usage by selectable date;
2. Capacity available by selectable date; and
3. Projected need for additional capacity by date.

c. Administrative reports for each AFIS matcher, to include at a minimum:

1. Matcher number and name – types of data contained in the matcher;
2. Number of Individuals enrolled in each matcher;

3. Number of individuals with one record, two records, or three records in the matcher;
4. Average minutiae per record;
5. Average NFIQ score per finger per image; and
6. Average compression rates per image.

d. Administrative reports for all of AFIS reflecting the following information, at a minimum:

1. Number of persons authorized to access the AFIS;
2. Number of persons who have administrator access;
3. Number of persons who have ten-print access;
4. Number of persons who have latent print access;
5. Number of Live-Scans;
6. Number of ORIs; and
7. Number of workstations (by type).

IV. Implementation Requirements – Statement of Work

A. Vendor Acknowledgement

108. Section IV outlines the MDPS minimum expectations of the awarded Vendor for implementation of the selected solution. Implementation deliverables will reveal the Vendor's expertise in project management, AFIS process improvement, data migration, acceptance testing, etc. MDPS expects the proposed preliminary implementation plans to be refined by the awarded Vendor and MDPS project managers during the implementation process.

Section IV includes requirements for proposing Vendors and requirements for the awarded Vendor. Proposing Vendor requirements require the Vendor to present detailed plans, strategies, and methodologies to prove Vendor capabilities. Post-award requirements require implementation of the proposed plans, strategies, and methodologies as agreed upon by the State and the awarded Vendor. For all such requirements, the term *Vendor* is used interchangeably and the intent is determined by the context of the requirement.

Upon award, MDPS intends for the requirements set forth in this Section IV, and the responding Vendor's proposal, including any subsequent, agreed upon provisions and revisions, to act as the Implementation Statement of Work.

Vendor must acknowledge that he has read and understands the intent of Section IV, Implementation Requirements - Statement of Work.

B. General Scope

109. Vendor must agree to implement the selected solution to achieve the following minimum goals:

a. Replicate the functional, technical, and administrative capabilities of the existing AFIS solution;

b. Enhance the functional, technical, and administrative capabilities of the existing AFIS system.

c. Migrate the existing NIST formatted AFIS database content from the existing solution to the selected solution;

d. Conduct extensive testing of the proposed system to identify and correct deficiencies in base capabilities, customizations, integrations, interfaces, migrations, MDPS processes, and all related hardware and software. Such efforts must include but may not be limited to:

1. Factory Acceptance Testing;
2. On-site Testing;
3. COOP Testing;
4. User Acceptance Testing; and
5. Final Acceptance Testing.

e. Train system users and provide complete system documentation and user documentation.

C. Program Management

110. The Vendor agrees to establish a formal *Program Management Office* (PMO), which will be responsible for executing the total effort required for implementation, testing, acceptance, training, and maintenance of ongoing operations of the proposed AFIS solution.

a. Vendor must define roles, responsibilities, authority structures, and reporting requirements for each organizational element.

111. Vendor agrees to appoint a Project Manager to be responsible for overseeing the execution of all facets of implementing the proposed solution.

a. The Project Manager will have full authority over all program activities and Vendor resources, subject to MDPS oversight and approval.

b. The Project Manager will be responsible for Vendor’s technical, schedule, and cost performance.

c. The Project Manager will be the principal interface between the Vendor and the State for all matters relating to the implementation of the proposed solution and the resulting contract with the State.

d. The Project Manager or his designee will be available to the State on a 24/7/365 basis, as needed.

112. As a part of program management, Vendor agrees to conduct technical reviews and provide technical reports for ongoing operations for the term of the resulting contract.

a. Vendor agrees to log all transaction and system activity necessary to evaluate performance and facilitate trend analysis.

b. Vendor agrees to conduct appropriate quality assurance and audits to ensure that logs are complete and accurate.

113. During the implementation phase, Vendor agrees to meet with State designees to review program objectives, at least on a monthly basis or more often as needed, and on-site as needed:

a. To confirm that technical problems have not caused the program to fail to maintain agreed upon service levels;

b. To provide immediate feedback for the resolution of any issues on a timely basis;

c. To ensure that the parties are proactively identifying and addressing issues that could adversely affect service levels; and

d. To provide a written review of the status of all plans and documents described in RFP No. 4063.

114. Vendor agrees to participate in a program kickoff meeting at a State facility 30 days prior to the date scheduled for declaring the State's *Initial Operating Capability* (IOC). The purpose of the meeting is to introduce key State and Vendor operations support personnel, discuss plans, examine risks, and address any other issues important to successful operations.

115. Vendor agrees to conduct periodic quarterly or semi-annual *Operational Management Reviews* for the purpose of addressing concerns such as:

a. Performance against SLAs;

b. Financial and schedule status;

c. Planned activities;

d. Action items/status;

e. Problem report status;

f. Configuration management and quality assurance reporting;

g. Issues and risks; and

h. Other service level shortfalls and plans for corrective action.

116. Vender understands that the State expects operational management review meetings to be held at MDPS or State sites. For meetings not held at State sites, Vendor agrees to assume vendor related travel expenses.

117. Vendor agrees to participate in required operational management review meetings as requested by the State, or as required by operational conditions.

118. For operational management review meetings, Vendor agrees to provide agendas, presentation materials, minutes, technical reports, and system performance reports.

D. Project Management Plan

119. *Project Management Plan* (PMP): The MDPS desires to implement the proposed solution within 18 to 24 months of an executed contract with the Vendor. So that MDPS can assess Vendor's ability to implement within 18 to 24 months of an awarded contract, Vendor must propose a PMP that includes, but is not limited to all tasks (all phases), estimated hours per task, major project milestones, quality assurance checkpoints, testing, etc.

120. MDPS prefers the Vendor to use Microsoft Project as the tool for preparing and maintaining the PMP.

121. Vendor's PMP must reflect industry best practice standards and must detail Vendor's plans for planning, monitoring, supervising, tracking, and controlling all project activities.

122. Vendor's PMP must describe the implementation team member organizational structure, roles and responsibilities, resources, processes, and all other information necessary for MDPS to assess your ability to manage the AFIS implementation.

123. Vendor’s PMP must include an Integrated Master Schedule (IMS), that the Vendor agrees to maintain and update as necessary in response to implementation requirements. The project timetable must estimate the time necessary for all phases of implementation from the point of contract execution through completion of go-live, final system acceptance, and user training.

124. Upon award, the Vendor must agree to work with MDPS to modify the proposed PMP, as appropriate, to meet agreed upon implementation objectives. MDPS expects the Vendor to work with the MDPS Project Manager to ensure effective project management during all phases. MDPS reserves the right to approve or disapprove material changes to the Vendor’s PMP.

125. Risk Management: In the PMP, Vendor must present a risk management strategy to address known assumptions, risks, roadblocks, challenges, and constraints that may negatively affect the timely and successful completion of the project.

126. The PMP must provide detailed project management strategies for all phases and components common to AFIS implementations including, but not limited to development, customization, interfaces, integrations, migration, testing, production, and training.

127. The PMP must include detailed strategies for Vendor testing of phases and components common to AFIS implementations including, but not limited to development, customization, interfaces, integrations, migration, and production.

128. Vendor will be responsible for any integration, interface, migration, or implementation issues that may arise during implementation.

129. MDPS requires that the current system will remain operational until the cut over from the legacy AFIS to the proposed AFIS. Vendor must describe plans to ensure continued operations, or to at least minimize the down time. Vendor must:

    a. Be specific about the effects that a cutover might have on continued operations;
    b. Highlight the measures you expect to take to minimize downtime; and
    c. Present known risks and risk management strategies. For all project management and implementation deliverables, incorporate any related cutover variables.

E. RFP No. 4063 Compliance Documents

130. Reference documents and standards cited by this RFP will be considered compliance documents.

    a. If federal or state compliance documents or standards are updated during the scope of this implementation, the Vendor must agree with the State to recognize and comply with the updated documents or standards.
    b. If Vendor proposes changes to compliance documents during the scope of this implementation, Vendor agrees to:
        1. Identify existing material needs to be replaced or updated;
        2. Identify the proposed new material and/or associated data items;
        3. Provide a rationale for using the new items including cost, schedule, performance and supportability impact; and
        4. Obtain State approval.

F. System Requirements Review

131. Prior to implementation, Vendor must conduct an in-depth System Requirements Review (SRR). The SRR will educate the Vendor on all technical, functional, and procedural aspects of current MDPS AFIS operations and identify steps that must be taken to prepare for the implementation of the proposed solution. MDPS will expect the Vendor to identify areas of current operations that need improvement and recommend changes where appropriate.

    a. Vendor must document the findings of the SRR to represent to the MDPS a complete understanding of the existing internal and external processes, the interaction among and between the various users, all interfaces and integrations, and the Vendor's ability to migrate legacy NIST formatted AFIS database contents to the proposed solution.

132. Functional and Technical Requirements: Sections II and III of this RFP No. 4063, Attachment A present the minimum functional and technical requirements of the AFIS solution sought by this procurement. Vendor must review each functional and technical requirement with designated MDPS team members. Vendor and MDPS team members must reach a consensus on whether to validate or modify each requirement as appropriate to achieve successful implementation and ongoing operations.

    a. Vendor must present rationale and justification for each agreed upon modification, and each modification must be adequately documented to become a part of the implementation design and development procedures. Include cost benefit analysis, if appropriate

133. Current AFIS Operations: For this requirement, the term *AFIS Operations* generally refers to local MDPS AFIS operations and procedures. AFIS administrative requirements are addressed in Attachment A, Section III, Technical Requirements.

    Vendor must conduct a thorough review of current, integral MDPS AFIS operations. Vendor and MDPS team members must reach consensus on whether to validate or modify each process or procedure. MDPS expects the Vendor to recommend changes to correct operational deficiencies and to position MDPS to maximize the benefits of the proposed solution. Note: Awarded solution will be required to initially interface with all current external systems without any changes being required to those external interfaces.

    a. Vendor must present rationale and justification for each agreed upon modification, and each modification must be adequately documented to become a part of the implementation design and development procedures. Include cost benefit analysis, if appropriate.

134. Other Requirements: In the SRR, MDPS and the Vendor must identify any additional areas that need to be addressed or modified to achieve successful implementation and ongoing operations of the proposed solution.

    a. Vendor must present rationale and justification for each agreed upon modification, and each modification must be adequately documented to become a part of the implementation design and development procedures. Include cost benefit analysis, if appropriate.

b. As a result of the SRR, the Vendor must provide a finalized AFIS System Specifications document which will be the finalized version of the MS AFIS System Specifications (presented in the RFP and responded to in the proposal) after the SRR has been conducted and approved by MDPS.

c. The Vendor must create a Requirements Verification and Traceability Matrix (RVTM) with the AFIS System Specifications for the purpose of tracking, verifying, and tracing the presence of all AFIS requirements during development and testing.

G. System Design and Development

135. Prior to implementation, Vendor must prepare a *System Design Document* (SDD) for review and State approval. The SDD must:

a. Be complete down to the line replaceable unit (LRU) level for all hardware items and through the computer software unit (CSU) level for all developed software;

b. In the case of commercial off-the-shelf (COTS) software, be complete through the level of licensed software products (LSP[s]);

c. Identify the functions performed by, performance required of, and interfaces supported by each CSU (for developed software) and each LSP (for COTS software);

d. Document the number and interconnection of all LRUs and identify the software components loaded on each LRU;

e. Document the bandwidth, memory, and throughput of each LRU;

f. Describe the interfaces supported by each CSU, LSP, and LRU;

g. Specify any standards with which each CSU, LSP, and LRU complies; and

h. Include complete work flows for all operational user and administrative functions.

136. As part of the SDD review, Vendor must present evidence (e.g., results of analyses, computer model and simulation results, benchmark results, and offeror-supplied specifications) to demonstrate that the design satisfies the requirements of the State's System Requirements Specifications and the required standards set forth in:

a. The *AFIS Current Environment for RFP 4063*;

b. AFIS specifications as required by Section VII of RFP No. 4063;

c. American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Biometric and Forensic Information, Update 2015;

d. Mississippi Electronic Fingerprint Submission Specifications;

e. Electronic Biometric Transmission Specification (EBTS), IAFIS-DOC-01078-10.0.8. September 30, 2017;

f. FBI Criminal Justice Information Services (CJIS), CJISD-ITS-DOC-08140-5.6, CJIS Security Policy, Version 5.6, dated June 5, 2017;

g. State of Mississippi Enterprise Security Policy

1. For access to the State of Mississippi Enterprise Security Policy, send an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request.

h. For hosted services, the AFIS design must be compliant with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy;

1. For access to the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, send an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request

i. MDPS Information Security Plan

1. For access to the MDPS Information Security Plan, send an email request to greg.nations@dps.ms.gov. Include a reference to this RFP requirement as justification for your request.

137. When the SDD document has been approved by the State, the Vendor may proceed with procuring system hardware and software.

H. Data and Property Management

138. *Data and Property Management Plan*: Vendor agrees to develop, document, and implement comprehensive procedures for the management of data, documentation, and State property (equipment, hardware, and software that belongs to State).

139. The data management plan must encompass all data and documentation that is:

a. Produced by Vendor under the terms of the resulting contract;

b. Procured by the Vendor under terms of the resulting contract; and

c. Received from the State for use under the terms of the resulting contract.

I. System Migration Plan

140. Vendor must prepare a comprehensive *System Migration Plan* that details the Vendor's approach to migrate MDPS from its current legacy AFIS to a new AFIS environment under the proposed solution. So that MDPS can assess Vendor's ability to conduct such a migration, Vendor must provide a preliminary *Migration Plan* for MDPS with the following details and requirements:

a. Vendor must be specific about the tools, data, facilities, personnel, and other resources required for the migration. Regarding personal and other resources, be specific about whether the resources are supplied by the Vendor, MDPS, or other. Vendor should keep in mind that MDPS has limited available resources.

b. Upon award, the system migration plan will be amended to meet specific migration needs as determined by the Vendor and MDPS.

141. As part of the system migration plan, Vendor must conduct site surveys and analyses to determine facility readiness for the replacement system. Vendor must evaluate site(s) for HVAC, lighting, electrical power, structural loading, and physical access. The scope of this requirement includes primary and remote sites, including COOP site.

a. Vendor must review the network configuration at each remote site to ensure that the proposed is compatible with existing network topologies and security.

b. Vendor must prepare an *Installation Survey Report* to document any incompatibilities between the proposed AFIS equipment and the related facilities or networks and any modifications to be made by MDPS. The installation survey report is subject to approval by the MDPS.

c. Vendor must prepare a *Version Description Document* documenting complete site specific instructions necessary to install and configure all hardware, software and data associated with each site deployment. The version description document is subject to approval by the MDPS.

142. Vendor must prepare an *Installation Plan* to document the necessary installation tasks, responsibilities, schedule, resource requirements, equipment layout, cabling, and testing.

    a. The installation plan is subject to approval by the MDPS.
    b. The installation plan will be used to verify the correct installation of equipment and software at the primary and remote sites, including the COOP Site.
    c. Vendor must prepare *Installation Drawings* to define equipment layout and cabling. The installation drawings are subject to approval by the MDPS.

143. Upon approval of all site prep and system migration plans, Vendor must deliver and install the necessary system hardware, software, and any other necessary components at the primary and remote sites, including the COOP site.

    a. Vendor must prepare system equipment and software to support upcoming system acceptance and user acceptance testing.

J. Data Migration Plan – Legacy Data

144. Legacy data from the current AFIS has been converted from the incumbent's proprietary format to NIST format. Vendor must migrate NIST formatted legacy data from the current AFIS to the awarded AFIS. A file of the legacy data in NIST format will be made available to the Vendor. A sample of the NIST file is available to interested vendors upon request. Proposing vendors must request a copy of this sample records dataset by sending an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request.

145. So that MDPS can assess Vendor's ability to migrate MDPS legacy data to the proposed AFIS, Vendor must submit a preliminary *Data Migration Plan*. Vendor must specific about Vendor's methodology. Highlight any known risk factors and present risk mitigation plans.

146. Vendor must detail data migration testing plans to validate the successful migration from the legacy AFIS to the proposed AFIS.

147. Vendor must work with the MDPS project implementation team to update and modify the preliminary data migration plan as appropriate.

148. Final data migration and data migration testing plans are subject to approval by the MDPS.

K. Factory Acceptance Test

149. Vendor must conduct *Factory Acceptance Testing* (FAT) for the fully assembled and operational system.

150. For purposes of this procurement, Vendor must agree to provide FAT in accordance with the State's presumptions that, at a minimum:

    a. The purpose of the Factory Acceptance Test ("FAT") is to ensure that the basic capabilities are available and work in a factory setting, and that the documentation associated with the system reflects the design and is usable (e.g., start-up and shut-down procedures to verify that they can be used, as written, to perform the intended function). These tests are oriented toward verifying as much functionality, hardware, interface requirements, performance requirements, accuracy requirements, and documentation as possible.

b. FAT is typically conducted with scripts to ensure agreement among the stakeholders on the input and expected results and that the tests are repeatable. After successful passage of the FAT at Vendor's facility, Vendor will be given permission to ship the System to the Operational Site(s).

151. Vendor must agree to conduct FAT for the fully assembled and operational system for both the Primary Site and the COOP Site (disaster recovery site) levels.

152. FAT must include all tests necessary to confirm that all requirements of the AFIS System Specifications described in this RFP No. 4063 have been satisfied and to demonstrate compliance with required standards listed.

153. FAT must include all tests necessary to demonstrate satisfaction of those requirements from any (provider-developed) subordinate specifications.

154. In cooperation with the State, Vendor must agree to prepare a FAT Plan and FAT Procedures to be approved by the State.

155. Vendor must agree that the State will witness the execution of all FAT activities.

156. Vendor must agree to document the results of FAT in a FAT Report(s).

157. Vendor must agree to conduct a Pre-Ship Review to demonstrate the FAT success, to determine the readiness of the system(s) for delivery, first to the State's Primary Site, and then to the COOP Site, and to secure State authorization to ship the System components and configurations.

L. System Acceptance Test

158. Vendor must conduct *System Acceptance Testing* (SAT), also known as system-level integration testing, to demonstrate the following minimum outcomes:

a. To demonstrate that the equipment was installed correctly and operates at the functional and performance levels verified at FAT;

b. To verify connectivity and throughput requirements that could not be tested during FAT (such as operations using remote network sites);

c. To verify that all system interfaces function properly at required accuracy and throughput thresholds as described in Sections II and III of this RFP No. 4063, Attachment A;

d. In accordance with the performance requirements described in Sections II and III of this RFP No. 4063, Attachment A, to verify performance with the full initial data load, multiple workstations, etc. Any remaining performance requirements that were not tested or completed with FAT will be tested at this stage;

e. To verify that the integrated sum, including any remote site testing, is at least as functional as the sum of the individual parts and to verify that end-to-end workflows execute as anticipated (data accuracy to be verified during UAT); and

f. To validate COOP activities, including data backup and restoration, as well as using the COOP site for primary processing, then restoring the entire system, ensuring that the repositories and matchers are current and identical across the two sites.

159. Vendor must agree to regular status meetings with MDPS project management team to review progress on system acceptance testing.

a. Vendor agrees to submit meeting agendas, presentation materials, and subsequent meeting minutes.

160. Vendor must submit a preliminary, comprehensive SAT plan to demonstrate Vendor's ability to conduct AFIS SAT. Vendor's SAT plan must incorporate the following minimum components:

a. Bill of Materials (for documentation purposes);
b. Installation Plan;
c. Training Plan;
d. Installation Drawings;
e. Training Materials;
f. SAT Test Procedures;
g. SAT COOP Plans;
h. Version Description Document (Version of System s/w and application s/w);
i. SAT Test Plan; and
j. SAT Test Report.

161. Upon award, Vendor agrees to finalize the preliminary SAT plan with input from the MDPS project team.

a. Vendor agrees that the final SAT plan requires approval from MDPS.
b. Vendor agrees that MDPS expects to witness the execution of the SAT.
c. Vendor agrees that MDPS retains the right to determine the success or failure of individual SAT tests.

162. Upon satisfactory completion of SAT, Vendor agrees to conduct an *Operational Readiness Review* (ORR) so that MDPS can determine the readiness of the system(s), facilities, and personnel for User Acceptance Testing (UAT).

M. User Acceptance Testing

163. Vendor agrees to conduct User Acceptance Testing (UAT) to prove that the AFIS system fully meets the requirements of RFP No. 4063.

a. Vendor agrees that UAT procedures will include both scripts and normal operations to test end-to-end workflows, including all MDPS interfaces and interfaces with the FBI.
b. Vendor agrees that UAT will include all reasonably expected events, such as full backup and restore, switchover to the COOP site.
c. Vendor agrees that UAT will provide a full suite of reports generated during the UAT period to validate the reporting functions.

164. Vendor must agree to regular status meetings with MDPS project management team to review progress on UAT.

a. Vendor agrees to submit meeting agendas, presentation materials, and subsequent meeting minutes.

165. Vendor must submit a preliminary, comprehensive UAT plan to demonstrate Vendor's ability to conduct AFIS user acceptance testing.

166. Vendor's UAT plan must incorporate the following minimum components:

b. UAT Test Procedures;

c. UAT COOP Plans;

d. UAT Test Report; and

e. Training Materials;

167. Upon award, Vendor agrees to finalize the preliminary UAT plan with input from the MDPS project team.

a. Vendor agrees that the final UAT plan requires approval from MDPS.

b. Vendor agrees that MDPS expects to witness the execution of the UAT.

c. Vendor agrees that MDPS retains the right to determine the success or failure of individual UAT tests.

d. Vendor must provide the facilities, equipment, and personnel to support the services identified in UAT.

168. Vendor must agree to provide the equipment and personnel to identify and resolve discrepancies between the results of the legacy system(s) and results of Vendor delivered system(s).

a. Vendor must agree to take corrective measures at no additional cost to MDPS when such discrepancies result as a failure of the Vendor-delivered system(s).

N. System Configuration Management Plan

169. Because MDPS AFIS devices are geographically dispersed, Vendor must prepare a preliminary *Configuration Management Plan* to address potential problems related to reporting, testing, diagnosis, deployment of patches and revisions, and all other aspects of configuration management.

170. At a minimum, Vendor's preliminary Configuration Management Plan must account for the following:

a. Establish a controlled configuration for each hardware and software component at the Primary Site, the COOP Site and each Remote Site;

b. Maintain current copies of the deliverable documentation and code;

c. Give State access to the documentation and code under configuration control; and

d. Control the preparation and dissemination of changes to the master copies of the deliverable software and documentation placed under configuration control so that they reflect only approved changes.

171. Vendor must generate management records and status reports on all products composing the controlled configuration for each hardware and software component at the Primary Site, the COOP Site and each Remote Site. The status reports must, at a minimum:

a. Make changes to controlled products traceable;

b. Serve as a basis for communicating the status of configuration identification software; and

c. Serve as a vehicle for ensuring that delivered documents describe and represent the associated software.

172. Vendor must agree to participate in MDPS configuration control meetings. State configuration control meetings will establish and control the requirements baseline throughout the performance of the Agreement and will control the operational baseline (deployed hardware, software, databases and documentation) once the AFIS becomes operational.

O. User Training and Documentation

173. Vendor must conduct comprehensive training that will address all user functions for all user types, e.g., ten-print and latent examiners, system administrators, maintenance personnel, etc.

174. Vendor must provide detailed user documentation that will at a minimum:

    a. Describe system components, functions, and operations of each server and workstation type.

    b. Include a list and description of all error conditions, as well as the associated error messages, and the actions required of the operator to address each error condition.

    c. Vendor must provide each AFIS workstation with online user documentation that will be resident on the workstation or accessible via the agency's internal networks. Vendor must also provide a paper copy.

175. Vendor must conduct four types of training courses that meet the following minimum requirements:

    a. Ten-Print Workstation Baseline: This course will cover all ten-print functionality associated with the new AFIS. The course will provide hands-on instruction on the ten-print workstation for manual and automated ten-print processing. "Hands-on" requires that each student have access to a fully functional workstation and training database during the training sessions. The course will cover ten-print manual and automated work flows, displays, data entry, quality assessment, and all functionality. In addition, the course will cover the basic and administrative user functions of the NIST archive. This course will also include the method by which NIST standard fingerprint transactions can be run against non-State agency AFISs. This course will also cover palm-print and slap-print entry and quality assessment functions. This course will need to be conducted enough times initially to accommodate approximately 25 examiners, with no more than five examiners per session.

    b. Latent Workstation Baseline: This course will cover all AFIS latent functionality associated with the new AFIS. The course will provide hands-on instruction on the latent workstation and latent case management system. "Hands-on" requires that each student have access to a fully functional workstation and training database during the training sessions. The course will cover latent manual work flows, displays, data entry, quality assessment, and all functionality. In addition, the course will cover the basic user functions of the NIST archive. This course includes the method by which NIST standard latent transactions can be run against non-State member agency AFISs. The course will include instruction in best practices for ensuring optimum accuracy. This course will also cover latent palm-print and slap entry, quality assessment, and matching functions. This course will need to be conducted enough times initially to accommodate approximately 60 examiners, with no more than five examiners per session.

c. MCIC Staff: This course will provide an overall view of the technical aspects of the AFIS and provide methods to manage and resolve minor incidents quickly and effectively. This course will need to accommodate an agreed upon number of participants initially and must be conducted at least once yearly for the duration of the Agreement for approximately 4 participants. This training must accommodate new personnel and keep existing staff current.

d. CIC Administration, Managers, and Supervisors: This course will cover AFIS Management functions. This course will provide hands-on instruction for accessing and producing management reports, creating user accounts, and performing audits and inquiries using the tools provided by the System.

176. Vendor must agree to provide any additional training needs related to remote sites, including COOP sites, at no additional cost to MDPS.

P. System Documentation

177. Upon implementation, Vendor agrees to provide a comprehensive set of system documentation, system management documentation, and user documentation.

178. Vendor agrees to provide system documentation in both Microsoft compatible file formats and .pdf format.

179. Vendor agrees to provide system documentation in both digital and hard copy formats.

Q. Ongoing Project Administration

180. Vendor must agree to provide ongoing project administration, that shall include, but not be limited to the following activities:

a. Provide monthly written Project Plan update reports;

b. Participate in weekly status update conference;

c. Attend meetings with State Executives and Management as needed; and

d. Update the PMP and the Project Schedule as appropriate.

R. Change Management

181. Vendor must agree that upon award, Vendor will describe, justify, and submit all proposed changes to the agreed upon project deliverables to MDPS for approval. Such proposed changes include, but are not limited to project scope, any and all implementation requirements, technical, functional, and configuration requirements, and/or all other agreed upon project deliverables.

V. SECURITY

A. General

182. For installation, implementation, and ongoing operations, Vendor agrees to observe all contemporary, best practice security measures to provide end-to-end security for all AFIS components and operations. Such measures include but are not limited to:

a. All necessary hardware and software updates;

b. All third party data and software components;

c. Anti-virus updates;

d. Configuration management;

e. Backup, restoration and recovery;

f. System Logging; and

g. Report generation, to include all available metrics involving system security status and/or breaches.

183. Vendor must agree that all processes, transmissions, digitally stored information, and any and all other AFIS related components will conform to the most recent InfoSec standards.

184. At a minimum, Vendor agrees to meet the following information security requirements:

a. The AFIS design must conform to the CJIS Security Policy v5.6 or latest;

b. Antivirus software must be loaded on all processors that run operating systems where there are commercial antivirus packages available. DPS desires the Vendor to utilize the Microsoft Enterprise Security products;

c. Any server components proposed for purchase by DPS for the solution must utilize the Microsoft Enterprise security product via the Microsoft Enterprise Agreement with the MDPS;

d. The antivirus software must automatically virus scan all files on portable data storage devices (i.e., CDs, DVDs, USB devices with memory, and floppy disk media) presented to a system and report alerts and other problems;

e. The antivirus software must automatically log all virus alerts and action taken;

f. The AFIS must support the updating of antivirus software databases of virus information without compromising the security of the system;

g. The AFIS design must be compliant with MS ITS Enterprise Security Policy;

1. For access to the State of Mississippi Enterprise Security Policy, send an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request.

h. For hosted services, the AFIS design must be compliant with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy;

1. For access to the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, send an email request to jeannie.williford@its.ms.gov. Include a reference to this RFP requirement as justification for your request

i. The AFIS design must be compliant with MS DPS Security Policy.

1. For access to the MDPS Information Security Plan, send an email request to greg.nations@dps.ms.gov. Include a reference to this RFP requirement as justification for your request.

185. For any intrusions or other security breaches or events, Vendor agrees to immediately notify the State. The immediate contact must be verbal and the Vendor must follow up in writing within four hours of the event. The follow-up report must include detailed documentation describing the event as well as any steps taken/plans for remediation.

186. The AFIS must support encryption of data both at rest and in transit on any hard drive or other storage device used in the AFIS system environment.

187. Vendor agrees to take reasonable precautions, as approved by the State, to ensure the physical security of the state’s Primary site and COOP site.

188. For security monitoring, Vendor agrees to provide access to State designees for system security reviews, penetration testing, and system security logs.

189. For any candidate proposed by the Vendor to have access to State systems and sites, Vendor agrees that the State requires a fingerprint background check and the State reserves the right to reject those have failed to pass a background check or to maintain a clean criminal record.

B. In-Plant Security Plan

190. Upon award and implementation, Vendor agrees to thoroughly document all security processes, procedures, personnel duties, and all other components necessary to administer agreed upon security measures. This document will be considered the *In-Plant Security Plan*.

    a. In-Plant Security Plan: Vendor must agree to develop and implement a detailed, in-plant security plan in accordance with CJIS Security Policy v5.6 or latest.

    b. The in-plant security plan will incorporate input from State personnel as appropriate and will be subject to approval by the State.

    c. The in-plant security plan must include contact information and protocol for alerting the State of security events and this information must be kept updated at all times.

    d. Vendor agrees to keep the in-plant security plan updated and distributed to the appropriate Vendor and State personnel.

    e. When operational or procedural changes result from updates to the in-plant security plan, Vendor agrees to provide immediate training to all appropriate Vendor and State Personnel.

VI. CONTINUITY OF OPERATIONS PLAN

191. Many of the requirements of this RFP No. 4063 refer to the need for continued operations if a local or regional event adversely affects access to the primary site or interrupts normal operations. To address these needs, Vendor must prepare a *Continuity of Operations Plan* (COOP).

    a. COOP services include, but are not limited to the provision of facilities, equipment, system data, and documentation to ensure essential services in the event of a disaster declaration. The COOP must include plans for periodic training drills involving all pertinent personnel, equipment, and systems to maintain readiness to respond to disaster declarations. MDPS and Vendor will agree on the timing of disaster training drills.

    b. The COOP must document procedures to ensure the performance of essential functions during abnormal conditions, including system maintenance and system upgrades. Essential functions are defined as those functions that enable Vendor to provide vital services under any and all circumstances.

192. Vendor agrees that COOP services will be considered a part of system maintenance and will be covered by the system maintenance fees.

193. At a minimum, the COOP must:

    a. Ensure continuous performance of essential AFIS functions and operations during an emergency or planned outage;

    b. Protect essential facilities, equipment, records, and other assets;

c. Reduce or mitigate disruptions to operations; and

d. Achieve a timely and orderly recovery from an emergency and resume of full service to users.

194. At a minimum, the capabilities provided by the Vendor in the COOP must:

a. Be maintained as an active-active site;

b. Be capable of providing 100 percent of the AFIS services (in the event of the loss of the Primary Site) both with and without warning/scheduling; and

c. Be continuously operational in a load-balanced environment during normal operations.

195. At a minimum, the COOP must contain:

a. Plans and procedures;

b. Identification of essential functions;

c. Alternate facilities;

d. Interoperable communications;

e. Vital records and databases; and

f. Tests, training, and monthly exercises and drills;

196. Upon implementation, the COOP must:

a. Outline a decision process for determining appropriate actions in implementing COOP plans and procedures.

b. Establish a roster of fully equipped and trained emergency provider and State personnel with the authority to perform essential functions and activities.

c. Include procedures for employee advisories, alerts, and COOP Plan activation, with instructions for relocation to predesignated facilities, with and without warning, during duty and non-duty hours. This includes providing for personnel accountability throughout the duration of the emergency and providing for continuous operational status in an active-active environment.

d. Establish reliable processes and procedures to acquire resources necessary to continue essential functions and sustain operations similar to that of the primary site for up to 30 days.

197. Declaration of Disaster

a. A declaration of disaster may be called by the State or by the Vendor.

b. In the event of a declared disaster, MDPS expects the Vendor to be completely responsible for the restoration of AFIS operations.

c. Vendor will be expected to invoke the appropriate disaster recovery plan within four (4) hours from the disaster declaration and the disruption of normal AFIS operations.

d. MDPS must be able to log on to the secondary system at the disaster recovery site immediately upon the disaster declaration.

e. Vendor shall have 100% capacity of the operational system regardless of the declaration of the disaster by the State or the Vendor.

f. Vendor's failure to make a declaration of a Disaster within four (4) hours shall result in any system downtime, as a result of this incident, being deemed as *Unscheduled Downtime*.

g. In the event of a disaster declaration, Vendor must remain in regular and consistent communications with MDPS, keeping all relevant managers and responders informed and updated on efforts to restore normal operations.

VII. Final Acceptance Review

198. Vendor agrees that upon the successful completion of all implementation phases, MDPS will conduct a *Final Acceptance Review* (FAR) to determine whether or not Vendor has satisfied the terms and conditions of the awarded contract, which includes the requirements of this RFP No. 4063, Attachment A.

VIII. Warranty, Support, and Maintenance

A. Warranty

199. The warranty period is a one-year period during which the Vendor must warrant, at no cost to MDPS, all vendor provided system components and vendor provided services performed as stated in the RFP, Vendor's proposal, and any subsequent Statement(s) of Work. The warranty period must include the necessary Vendor support to correct any deficiencies found and to provide any other consultation as needed.

200. For any phased implementations or processes, the warranty period for each phase or process will begin only when Vendor has fully implemented the phase or process and MDPS has accepted the phase or process as functioning properly and in coordination with any previously implemented phase(s) or process(es).

201. The Vendor must agree to warrant all proposed application software to be free of errors for a minimum period of one year after acceptance. During this period, the Vendor must agree to correct, at his own expense, any discovered errors. If the system fails during warranty period due to a defect, the Vendor will offer a workaround solution within 24 hours and a full fix within five business days.

202. The Vendor must state and discuss the full warranty offered during the warranty period on all proposed system components, software, and services and state if it is longer than the required one-year minimum.

203. This warranty must cover all components for which services were provided, including all equipment, programs, forms, screens, reports, subroutines, utilities, file structures, documentation, interfaces, conversions, configurations, or other items provided by the Vendor.

204. The Vendor must agree that all corrections made during the warranty period are integral to the work associated with this project and will, therefore, be made at no additional charge to the State.

B. General

205. The State expects the proposed solution to operate within the functional, technical, and performance requirements set forth in this RFP No. 4063. When trouble issues occur, the State desires simple, streamlined processes for reporting and tracking trouble tickets.

a. Vendor agrees to provide web-based and toll-free telephone based trouble ticket access. The State expects to designate certain individuals to report and receive updates on reported trouble conditions, but does not expect to limit trouble reporting access to designees.

b. Vendor agrees to train users to submit trouble tickets and support requests and to provide always updated documentation.

206. Vendor agrees to provide 99.8 percent availability for all services required by this RFP No. 4063, Attachment A. Services available will be measured monthly and will be subject to the remedies as required and outlined in Section VIII, Item N (Remedies) below.

C. System Support

207. Vendor must provide primary and remote site support services as needed for continued, optimal AFIS operations. Such services include, but are not limited to responding to and tracking reported problems, resolving deficiencies, controlling software configurations, and ensuring hardware performance baselines and lifecycle expectations.

208. Vendor must provide daily backup of data and system configurations. Copies of backup tapes must be stored off-site from the primary site and the disaster recovery site to ensure their availability in the event of a disaster declaration.

209. Vendor must provide all upgrades, once generally available, to the installed operating system(s), database management systems, tools, utilities, and application software(s). All such upgrades will ensure that provided services conform to future FBI EBTS interface specifications and that no service is running on software that is no longer supported by the Vendor.

210. Vendor must provide status reports on the system, the services provided, and the repository and transaction volumes.

D. Customer Support

211. Vendor must provide 24 x 7 x 365 operational support for system users.

212. Vendor must provide a toll-free telephone number for MDPS staff to call 24 x 7 x 365 and an always-accessible website for trouble reporting.

213. 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.

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

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

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

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

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

219. Vendor agrees to provide adequate user training as requested by the State.

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

E. Software Updates

221. Once available, Vendor must provide all software updates necessary to keep current with the proposed solutions technology standards, industry standards, third party software upgrades, enhancements, updates, patches, and bug fixes, etc.

    a. Such Software updates shall include, but not be limited to enhancements, version releases, and other improvements and modifications to the core solution software, including application software.

222. Vendor agrees that maintenance services will also include maintaining compatibility of the solution software with any and all applicable contractor provided interfaces.

223. Vendor agrees that prior to installation of any third party software or any update thereto, Vendor must ensure compatibility, promptly upon release, with the then-current version of the software.

    a. Vendor agrees to ensure compatibility with all required or critical updates to third party software, including without limitation, service and compatibility packs, and security patches.

    b. Vendor agrees that third party application software incorporated by the Vendor is subject to the same maintenance and service obligations and requirements as the application software components that are owned or are proprietary to the Vendor.

F. Server Software

224. Vendor agrees to provide maintenance of the server software for the proposed solution, including but not limited to operating software, database software, and any other non-application software installed in the server environment.

225. Vendor agrees to update, upgrade, replace, and/or maintain server software components in accordance with the warranties specified in the resulting agreement and to maintain compatibility with the application software, including any modifications provided by the Vendor.

226. Vendor agrees to provide server software updates necessary to keep current with technology standards, industry standards, software updates to the application software, and other application modifications.

227. Vendor agrees to coordinate all server software updates with the MDPS project manager.

G. Server Hardware

228. Vendor agrees to repair, upgrade, replace, and/or maintain the server hardware components during the term of the resulting agreement so as to remain in compliance with all system requirements, including compatibility with the application software and any subsequent modifications.

229. Vendor agrees to maintain compatibility with the State’s client environment by providing software updates to the software and hardware upgrades to the application software.

230. Vendor agrees to maintain all network connectivity from the State of Mississippi point of presence (CIC) to the primary service site as well as the COOP site.

231. Vendor agrees to provide all maintenance of the server hardware components, including but not limited to all equipment and networking components and all other hardware upgrades and all other services as described above at no additional cost beyond the agreed upon maintenance and service fees.

H. Scheduled Downtime and Preventive Maintenance

232. Vendor agrees to conduct all scheduled maintenance services, including installation of software updates, during *Scheduled Downtime*. Scheduled downtime should be during late evening or early morning hours.

    a. Vendor agrees that scheduled downtime for performing preventive maintenance or other maintenance services at any site shall not exceed two hours per month, per site, unless agreed to in advance by the State.

    b. Vendor agrees to coordinate scheduled downtimes with the designated State management and technical support staff and to keep them informed of progress and status.

233. Vendor agrees that any downtime outside the agreed upon windows of time will be considered *Unscheduled Downtime* and will entitle the State to remedies as described in this RFP No. 4063, Attachment A.

234. Vendor may request scheduled downtime for the purpose of providing emergency corrective measures to the AFIS solution. Such requests must be approved by the State's project manager.

235. Vendor agrees to reflect scheduled downtime in the project Integrated Master Schedule.

236. Vendor agrees to provide preventive maintenance for all Vendor provided equipment and software.

    a. Vendor must dispatch maintenance personnel to clean, inspect, adjust the equipment, and replace defective or worn parts at the manufacturer's recommended intervals to keep the equipment in good working condition.

    b. Vendor must perform period maintenance tasks on all electronic components to ensure they are operating at maximum capabilities. Such maintenance will be scheduled at a minimum of once per month during hours agreed to by the State.

237. Vendor agrees to provide documented preventive maintenance procedures for all Vendor provided equipment and software.

I. System Interfaces

238. Vendor agrees to maintain all State and National interfaces through the wide area network (WAN) using FBI EBTS conformant transactions and international transactions via the CJIS gateway.

239. Vendor agrees that outside criminal agencies, such as local law enforcement, will be able to connect through the AFIS to run searches directly to NGI using ULW.

240. Vendor agrees to maintain all requisite data repositories and systems with networks that connect to booking stations and other criminal justice systems using the FBI EBTS.

J. Repository Maintenance

241. Proposed solution must provide a well-maintained repository of all enrolled transactions, which must be stored and must be retrievable in FBI EBTS formats.

242. Proposed solution must provide access that will include but not be limited to the ability to update, delete, retrieve, link enrolled transactions, and print appropriate card formats.

K. Technology Refresh and Enhancements

243. Vendor agrees to conduct joint technology reviews with the State to guarantee that the hardware, software, and system security are adequate for State purposes and are consistent with then-current technology used in similar systems.

    a. Vendor agrees that such evaluations will occur no less frequently than every six months.

    b. Vendor agrees that such evaluations will include a review and evaluation of AFIS technology enhancements available from the Vendor and third parties.

    c. Vendor agrees that such evaluations will review pending and implemented changes in NIST, EBTS, and other standards applicable to the State's primary and remote sites, including COOP sites.

        1. Vendor agrees to evaluate with the State, any software changes necessary to respond to any such developments and to provide migration paths for functional or technological updates.

        2. Vendor agrees that such changes will be provided at no cost to the State, beyond the service fees payable by the State to the Vendor.

244. After system acceptance, Vendor agrees to provide one hardware refresh every five years. Vendor must propose related costs or fees in Section VIII, Cost Information Submission of the RFP.

    a. Vendor understands and agrees that the purpose of the hardware refresh is to maintain AFIS performance at the requisite service levels, to improve performance with additional functionality, to take advantage of changes in technology, and to respond to regulations and standards promulgated by the federal law enforcement agencies such as the FBI or Homeland Security.

    b. Prior to commencing hardware refresh, Vendor agrees to submit hardware specifications to the State for approval.

245. For refresh and enhancement efforts, Vendor agrees to provide meeting agendas, presentation materials, technical reports, and meeting minutes.

L. Response Time Monitoring

246. For all performance related requirements related to the proposed solution, Vendor agrees to monitor the related system response times to verify compliance.

247. Vendor agrees to provide monitoring tools, such as dashboard functionality, to enable the State to view and comprehend real-time system status indicators upon demand.

248. Vendor agrees to perform response time monitoring at regular intervals and in sufficient detail to detect problems.

249. Vendor agrees to provide direct access to the State at any time to the data collected from response time monitoring.

250. Upon request by the State, Vendor agrees to provide reports and/or download data and related documentation that may be necessary for the State to independently monitor the response time of the system.

251. The State reserves the right to periodically revisit the response time baselines and to reset them to ensure that State operations are not restricted.

M. Correction of Deficiencies

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

253. 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.

254. Vendor agrees to inform the State within one hour of any service interruptions and to notify the State within eight hours of any hardware or software problems that the Vendor has identified and resolved.

255. Vendor agrees that Priority Level 1 deficiencies (See Table 7) require an immediate response. Examples are deficiencies that prevent subjects from being enrolled, images from being searched, or responses from being delivered. This includes all failures of Vendor supplied equipment, including remote site printers, scanners, and other required peripherals that would prevent users from accomplishing their work.

256. Vendor agrees to provide corrective maintenance for any deficiency in Vendor provided equipment or software that fails to perform in accordance with the finalized System Specifications document as an outcome of the SRR above pertaining to the functional, technical, or operational requirements contained in this RFP No. 4063, Attachment A. The scope of corrective maintenance coverage is 24 x 7 x 365.

257. Vendor agrees to keep the State designated management and technical support staff informed and updated about progress of correcting reported deficiencies.

258. Vendor agrees to maintain an electronic report log that indicates the problem report number, problem description, time the problem call was received, the priority assigned, all actions taken, and the time the problem was corrected. The problem log must be maintained in a database that is remotely accessible by State personnel.

259. Vendor agrees to designate one central point of contact for support of hardware and software deficiency issues.

260. Vendor agrees to replace failed equipment, especially for remote sites (tenprint and latent devices), within eight consecutive hours. If a device is out of service for eight (8) consecutive hours from the time of trouble intake, by the end of the eighth hour, Vendor agrees to be actively repairing or replacing the defective equipment with an operable device until the defective item has been fully repaired or replaced.

261. If a deficiency can't be repaired by phone or remote access, Vendor agrees to begin on-site repair within four (4) hours of notification, depending on the availability of the site where the equipment resides. All conditions that prevent the initiation of on-site repair within four (4) hours must be documented in Vendor's electronic log and reported to the State's help desk or other State-designated point of contact.

262. Vendor agrees to deficiency priority definitions and resolution times prescribed by Table 7 – Deficiency Priority Levels. See Table 7 below.

Table 7 - Deficiency Priority Levels

Priority Level	Description of Deficiency	Response Timeframe	Resolution Time
1 Critical	System is down (unscheduled downtime) or is practically down (e.g., extremely slow response time) or does not function at all, as determined by State. There is no way to circumvent the problem; a significant number of State users are affected. A production business system is inoperable.	1 hour from intake	8 consecutive hours from intake
2 Severe	A component of the solution is not performing in accordance with the specifications (e.g., slow response time), creating significant State business impact, its core functionality is not available, or one of system requirements is not met, as determined by State.	4 hours from intake	24 hours from intake
3 Moderate	A component of the solution is not performing in accordance with the specifications; there are unexpected results, moderate or minor operational impact, as determined by State.	24 hours from intake	14 days from intake
4 Low	This is a low impact problem and is not significant to operations or is related to education (e.g., general "how to" and informational solution software questions, documentation requests, understanding of reports or general "how to" create reports), as determined by State.	2 days from intake	Next version release or six (6) months unless otherwise agreed to by State and Vendor.

N. Remedies for Failure to Meet Service Levels

263. Vendor agrees that service credits will accrue for unscheduled downtime, including Vendor's failure to meet system availability requirements or response time requirements for curing deficiencies.

264. For purposes of assessing service credits, response timeframes will be measured from the time the Vendor is properly notified until the State determines that the deficiency has been resolved.

265. For purposes of assessing service credits, Vendor agrees that credits will be measured in monthly cumulative minutes for unresolved deficiencies and unscheduled downtime.

266. Vendor agrees that Priority Levels 1 and 2 response time deficiencies will be considered unscheduled downtime and will entitle the State to service credits in accordance with Table 8, Service Credit Assessments.

267. Without limiting any other rights and remedies available to State, Vendor agrees to issue service credits in accordance with the measures prescribed by Table 8, Service Credit Assessments.

268. Vendor agrees that service credits will be calculated separately for each applicable deficiency and will be assessed at the end of each month of system maintenance.

269. Vendor agrees that after 30 days of continued, deficient response time, according to the SLA, the State will consider the conditions to be equal to unscheduled downtime and the service credits in the Table 8 will go into full force and effect.

270. Vendor agrees that service credits are not penalties and, when assessed, will be deducted from the State's payment due to the Vendor.

Table 8 – Service Credit Assessments

Length of Continuous Unscheduled Downtime	Service Credits
1 to 4 hours	1 day of Service Credits equal to 1/30th of Monthly Fees
4 to 48 hours	2 days of Service Credits equal to 1/15th of Monthly Fees
48 to 96 hours	5 days of Service Credits equal to 1/6th of Monthly Fees
Each additional block of 96 hours thereafter	Additional 5 days of Service Credits equal to 1/6th of Monthly Fees

IX. Deliverables

A. General

271. Vendor must agree to provide the deliverables described in Table 9 below:

Table 9 - Deliverables

Deliverable/Plan Title	Delivery Dates
1. Project Management Plan	With proposal and with update – within 30 days after the Effective Date of the Agreement.
2. AFIS System Specifications	At System Requirements Review.
3. Integrated Master Schedule	With proposal and with update at Project Management Reviews.
4. Test and Evaluation Master Plan	With proposal and with update – within 30 days after the Effective Date of the Agreement.

Table 9 - Deliverables

Deliverable/Plan Title	Delivery Dates
5. Migration Plan	At System Design Review.
6. Test Reports	Several sets, each corresponding to the outcomes of Factory Acceptance Test, System Acceptance Test and User Acceptance Test. For each increment, at Pre-Ship Review and Operational Readiness Review.
7. Agenda	Five (5) Business Days prior to a meeting.
8. Presentation Materials	Draft – five (5) Business Days prior to a meeting, with updates – at the meeting and final – as part of Minutes.
9. Minutes	Draft – two (2) Business Days after the meeting, with final – five (5) Business days after receipt of State comments.
10. In-Plant Security Plan	With proposal and with update – within 30 days after the Effective Date of the Agreement.
11. User Manuals	At each training session and for online reference.
12. Database Design Document	Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and Final as part of System Acceptance.
13. Interface Design Document	Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and final – as part of System Acceptance.
14. System Design Document	Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and final – as part of System Acceptance.
15. Bill of Materials	At System Design Review with updates – at Pre-Ship Review.
16. Installation Plan	For each delivery, at Product Test and Readiness Review or 12 weeks prior to installation, whichever is earlier, with updates – at Pre-Ship Review.
17. Training Plan	At System Design Review with updates – at Pre-Ship Review.
18. Installation Drawings	At System Design Review with updates – at Pre-Ship Review.
19. Training Materials	For each delivery, at Product Test and Readiness Review or 12 weeks prior to installation, whichever is earlier, with updates – at Pre-Ship Review.
20. Technical Report	As specified, or required, or requested by State.

Table 9 - Deliverables

Deliverable/Plan Title	Delivery Dates
21. Test Procedures	Draft – 30 working days prior to Product Test and Readiness Review and System Test and Readiness Review, with updates – at the review, and final – as part of User Acceptance Testing.
22. COOP Plan	At System Design Review with revision – at Pre-Ship Review.
23. System Hardware	Prior to Operational Readiness Review.
24. Software Licenses	Prior to Operational Readiness Review.
25. System Data	Prior to Operational Readiness Review.
26. Version Description Document	At Pre-Ship Review with updates – at Operational Readiness Review and Final Acceptance Review.
27. Installation Survey Report	At completion of each site survey.
28. Test Plan	At System Design Review with revision – at Test Readiness Review.
29. Configuration Management Plan	Within 30 days after the Effective Date of the Agreement.
30. Requirements Verification and Traceability Matrix	Draft – five (5) Business Days prior to System Design Review, with updates – at the review, and final – as part of User Acceptance Testing.
31. System Performance Report	Periodic logs of all transaction and System activity necessary to evaluate Agreement performance and to facilitate trend analysis, support system and other transactional analysis as specified in this RFP 4063.
32. Data and Property Management Plan	Vendor must develop, document and implement comprehensive procedures for the management of data, documentation and State property (equipment, hardware or software that belongs to State).
33. Service Level Plan	In accordance with the functional, technical, maintenance, and support requirements of this RFP No. 4063, Vendor must develop a Service Level Plan (SLP) to govern Vendor's performance after system acceptance. The SLP must meet the performance reporting requirements outlined in Table 9, Item 31.

X. GLOSSARY

Table 10 - Glossary

Acronym	Definition
AFIS	Automated Fingerprint Identification System
ANSI	American National Standards Institute
CAR	Criminal Ten-Print Submission
CCH	Computerized Criminal History
CJIS	Criminal Justice Information Services
CNA	Criminal Ten-Print Submission (No Answer Necessary)
COOP	Continuity of Operations
DEK	Known Deceased
DEU	Unknown Deceased
DHS	Department of Homeland Security
DOB	Date of Birth
EBTS	Electronic Biometric Transmission Specification
EFS	Extended Feature Set
ERRA	Administrative Transaction Error
ERRI	Image Transaction Error
ERRL	Latent Transaction Error
ERRT	Ten-Print Transaction Error
FBI	Federal Bureau of Investigation
FFT	Fast Fourier Transform
FISR	Fingerprint Image Submission Response
IAFIS	Integrated Automated Fingerprint Identification System
IOC	Initial Operating Capability
ISO	International Standards Organization
IT	Information Technology
JPEG	Joint Photographic Experts Group
KP-LT	Known Palm to Latent
LCMS	Latent Case Management System
LFFS	Latent Friction Ridge Feature Search
LI	Latent to Latent Inquiry

Table 10 - Glossary

Acronym	Definition
LPNQ	Latent Penetration Query
LPNR	Latent Penetration Query Response
MAP	Miscellaneous Applicant Civil
MID	Mobile Identification
MPR	Missing Persons
NFF	National Fingerprint File
NFIQ	NIST Fingerprint Image Quality
NFUF	Non-Federal Applicant User Fee
NGI	Next Generation Identification
NIST	National Institute of Standards and Technology
ORI	Originating Agency
PDF	Portable Data Format
QC	Quality Check
RFP	Request for Proposals
RISC	Repository for Individuals of Special Concern
RPIS	Rapid Fingerprint Identification Search
RPISR	Rapid Fingerprint Identification Search Response
SIB	State Identification Bureau
SID	State Identification Number
SRE	Submission Results-Electronic
SRL	Search Results-Latent
TLI	Ten-Print to Latent Inquiry
TCN	Transaction Control Number
TOT	Type of Transaction
TPIS	Ten-Print Fingerprint Image Search
TP-LT	Ten-Print to Latent
TPRR	Ten-Print Rap Sheet Response
TP-TP	Ten-Print to Ten-Print
TU	Ten-print Update.
UAF	User Authentication File

Table 10 - Glossary

Acronym	Definition
UPS	Uninterruptable Power Supply
ULM	Unsolved Latent Match
ULW	Universal Latent Workstation