(Revised-Bulletin #12)

REQUEST FOR PROPOSALS

FOR

CRIMINAL BOOKING SYSTEM

(CBS) SOLUTION

APPENDIX B

MINIMUM SOLUTION REQUIREMENTS

JUNE 2018

NOTICE TO RFP PROPOSERS

THIS DOCUMENT DOES NOT STAND ALONE AND MUST BE READ AND REVIEWED IN CONNECTION WITH ALL OTHER PARTS OF THE RFP.

THIS APPENDIX B MAY BE UPDATED TO REFLECT THE SELECTED PROPOSAL PRIOR TO THE NEGOTIATION OF THE RESULTANT CONTRACT.

Req #	Requirement
	1.0 – General Criminal Booking Solution Functions
1.1	The Solution **SHALL** generate, issue and maintain unique transaction numbers, preferably sequential, for each booking or type of transaction (TOT) as defined by County.
1.2	The Solution **SHALL** be capable of reserving a large block of sequential booking numbers obtained from and governed by the County's Automated Justice Information System (AJIS), and issue these unique/sequential booking numbers when requested by User.
1.3	The Solution **SHALL** be capable of deleting a booking number and its associated data if the booking transaction associated with that booking number is not completed within 30 days and **SHALL** retain the audit log of the deleted transaction.
1.4	The Solution **SHALL**, throughout all its functionality, recognize and emphasize the AJIS numbering scheme as County's official booking number.
1.5	The Solution **SHALL** be capable of ingesting, storing and displaying unique booking transaction numbers generated from County's current Automated Booking System (ABS).
1.6	The Solution **SHALL** provide an XML web service (i.e. GJXDM/NIEM) which allows external systems (i.e., Records Management System (RMS) from a local agency) to request booking numbers from CBS, as illustrated in 'Booking Number Request Sample Flow Chart' (Attachment G.2) to the Statement of Work (SOW).
1.7	The Solution **SHALL** be capable of sending data and communicating directly with all interfaces listed in 'System Interfaces' (Exhibit C) to the SOW.
1.8	The Solution **SHALL** provide a method of receiving requests for booking numbers with or without a fingerprint.
1.9	The Solution **SHALL** monitor all booking transactions that do not have an accompanying fingerprint, and provide detailed audit reports.
1.10	The Solution **SHALL** be capable of capturing the Subject's signature at time of booking by utilizing a digital signature pad on the livescan and submitting that signature in the National Institute of Standards and Technology (NIST) file as a Type-8 record.
1.11	The Solution **SHALL** verify the fingerprint captured during the booking number request, is from the same Subject, when the booking record is completed, edited or continued on any Livescan device within the County.
1.12	The Solution's Livescan device, excluding Quick-ID devices, **SHALL** be housed in a ruggedized standup system with adjustable height. Ruggedized means a cabinet-type system that protects monitors, scanners, keyboards, uninterrupted power supply (UPS) and any other component of the system Solution. (Note: Excludes Printers and cameras)
1.13	The Solution **SHALL** allow for fingerprints to be taken at the Livescan device and printed locally, with no booking number issued and no submission made to County, when appropriate, for non-reportable charges at the discretion of the County or reporting agency.

Req #	Requirement
1.14	The Solution **SHALL** include a complete and valid standards-based record in conformance with the most current FBI Electronic Biometrics Transmission Specification (EBTS) https://www.fbibiospecs.cjis.gov/EBTS/Approved, as well as the more stringent Cal-DOJ specifications (i.e., State charge tables) and County specifications (e.g., 1,000 ppi print capture from scanner, mugshot required for every booking).
1.15	The Solution **SHALL** have edit functionality which allows Users to correct errors and resubmit records. It **SHALL** permit the opening and editing of erroneous records. Once a record has been edited, it **SHALL** pass the same validations as would a new record.
1.16	The uninterrupted power supply (UPS) software **SHALL** be capable of sending status emails to the LACRIS Help Desk when power issues arise.
1.17	The UPS software **SHALL** be capable of notifying the User of power issues informing them to save their work and shut down the Livescan device.
1.18	The Solution **SHALL** validate defined data entry fields for compliance, as delineated by County, Cal-DOJ, FBI/Criminal Justice Information Services (CJIS) Division, or other agency specifications.
1.19	The Solution **SHALL** ensure each mandatory field is present before submitting the transaction. Mandatory fields are governed by specifications.
1.20	The Solution **SHALL** adhere to tabled data entry fields for all data where a tabled dataset is available and provided. Depending on the tabled data entry field, the Solution **SHALL**: • Default the field value, based on the User's configuration, with the option for User to override. • Provide a look-up table, such as a drop-down field, for the User to select the correct value from, but also allow the User to enter the field manually with predictive table values suggested.
1.21	The Solution **SHALL** be configurable to include additional tables and fields, with or without drop down menus, when required by County to conform to changing business practices.
1.22	The Solution **SHALL** authenticate each booking record when: • Passing all the Cal-DOJ NIST and Los Angeles County specific NIST validations; • Bundling the booking record as an EBTS-compliant package consisting of all of the required records and types, then; • Submitting the package via interface to the Multimodal Biometric Identification System (MBIS).
1.23	The Solution **SHALL** provide the capability to convert an existing record, with prints, into any other transaction type submission (e.g., converting an IDN TOT to a CRM/REG/APP/DNS or a CRM to a REG/APP/DNS), as required by the County.
1.24	The Solution **SHALL** have passive communication capability (i.e. chat window) for the LACRIS Help Desk to communicate with the User.

Req #	Requirement
1.25	The Solution **SHALL** have the ability to import a NIST file and print a copy of the booking slip and finger/palm print cards.
1.26	The Solution **SHALL** store all transaction files for each local Livescan device, of only the transaction files currently retained on that device. Transaction files stored on the local livescan can be printed even if network connectivity to the central server is not available.
1.27	The Solution **SHALL** store transaction files from every Livescan device within the central server (including a backup), for a County-designated duration.
1.28	The Solution **SHALL** be capable of utilizing permission-based context menus for administrative tasks to include, but not be limited to, opening the data directory folder of a highlighted transaction record selected on the inventory screen, deletion of highlighted transaction records, and export of highlighted transaction records to a NIST-compliant file.
1.29	The Solution's Livescan PCs **SHALL** support Microsoft Windows 10 Enterprise Edition, and Windows Server 2010 and above.
1.30	The Solution **SHALL** support Microsoft Windows 10 on all Participating Agency-owned PC workstations.
1.31	The Solution **SHALL** support Microsoft Server Manager Windows 10.
1.32	The Solution **SHALL** adhere to all Federal and State criminal reporting requirements (i.e., FBI's National Incident-Based Reporting System (NIBRS)).
	2.0 – Specifications – User Security and Functionality
2.1	The Solution **SHALL** include a single User log-in for all CBS application modules, including instances when a User performs business functions for one or more Participating Agencies (i.e., LACRIS Help Desk staff).
2.2	All components of the Solution **SHALL** utilize this centralized User security group roles. Explain how your Solution will function in an offline mode where there is no connectivity to the central User database.
2.3	The User security group roles **SHALL** be maintained in the centralized database, with a local copy pushed out to each Livescan device.
2.4	The proposed Solution **SHALL** support Domain OS logon using a County-designated Active Directory Federation Services (ADFS) Authentication protocol.
2.5	User account information **SHALL** be stored on the central User database as well as locally on each device that the User has been granted permission to.
2.6	The Solution **SHALL** allow the CBS System Administrator to select which logon protocol each User shall follow.
2.7	The Solution **SHALL** allow Users to be assigned to multiple security groups.
2.8	The Solution **SHALL** apply the highest permission levels of any group that a User belongs to, should that User belong to multiple groups.

Req #	Requirement
2.9	The Solution's security groups and rules **SHALL** have the capability of decentralized administration. Examples: a lower level Administrator at a local agency cannot create an account equal in security rights to their own. A local Administrator can only affect those Users within their agency.
2.10	The Solution **SHALL** lockdown the Livescan device's OS for general Users but allow full access for Administrators.
2.11	The Solution **SHALL** support automatic User account: • Lock-out, after a configurable number of days of inactivity • Unlock after a two-factor authentication, or by a system Administrator
2.12	The Solution **SHALL** control excessive image quality error overrides at the User level, with configurable warning and audit report capabilities.
2.13	The Solution **SHALL** contain the below functionality and provide administrative notifications (local and/or LACRIS Help Desk) by e-mail. Thresholds to be set by Administrators. Notifications to include but not be limited to: • User errors • Too many failed login attempts • Too many image quality overrides • Too many match error (from flats or rolls) overrides • User locked out notification • User advised of eminent lockout if errors persist
	3.0 – Specifications – Solution Database
3.1	The Solution's database **SHALL** be configurable to include additional tables and fields, as required by County business processes.
3.2	The Solution **SHALL** be able to receive table updates including validations (i.e., charge codes) and/or accept and utilize tables obtained from an external system or source (i.e., table file in a shared directory used by multiple applications) and immediately apply the new table set and validation rules.
3.3	The Solution **SHALL** keep a database log of all transactions saved and/or submitted via interface. The log will contain, at minimum: • Date/time of transmission • Transaction number • Booking number • User actions with timestamps • System actions with timestamps • Name, gender, race and date of birth of the Subject fingerprint.

Req #	Requirement
3.4	The Solution's database log **SHALL** be maintained for a configurable period of time, no less than three (3) years, as specified by County.
	4.0 – System Software and Functionality
4.1	The Solution **SHALL** include 3rd party virus protection software as defined by County. (Currently McAfee Enterprise AntiVirus™).
4.2	The Solution **SHALL** support and be capable of e-mail (sending and receiving) messaging.
4.3	The Solution **SHALL** have its own means of communication, such as an email system, to support responses in email format (i.e., Simple Mail Transfer Protocol or SMTP) with attachments in EFT, SRE, plain text, etc. formats
4.4	The Solution's PC workstations and servers located at the locations **SHALL** have McAfee endpoint security software installed and running in the background. LACRIS will provide the McAfee endpoint security software as part of its enterprise site license.
	5.0 – Reports – Centralized and Local
5.1	The reports **SHALL** be accessible utilizing the current and two most recent versions of an internet browser, IE, Chrome, Firefox, etc.
5.2	All Users **SHALL** be authenticated prior to accessing the reports.
5.3	The Solution **SHALL** ensure access to available reports is based on User's permissions.
5.4	The Solution **SHALL** provide a list and description of the default reports.
5.5	The Solution **SHALL** provide for ad hoc reporting with all fields available.
5.6	The Solution **SHALL** provide a report building tool, including 10 concurrent software licenses, and necessary training.
5.7	The Solution **SHALL** provide a web-based administration and reporting module.
5.8	The Solution **SHALL** have a three (3) year retention for all booking forms.
5.9	The Solution **SHALL** restrict data in a report to the User's specific permissions and/or groups that the User has rights to, (i.e., reports containing data only from their Law Enforcement [LE] agency).
	6.0 – System Audit Capability
6.1	The Solution **SHALL** provide a visual auditing tool to enhance Administrator's ability to identify issues with submitted images, both fingerprints and photos.
6.2	The Solution's audited data **SHALL** be retained for a minimum of three (3) years.
6.3	The Solution **SHALL** allow for external interface transactions to perform complete and partial record sealing and expunging in CBS. (i.e., MBIS can send a notification to CBS, and CBS will seal the record so Users cannot view the booking forms in CBS).

Req #	Requirement
6.4	The Solution's audit tools **SHALL** allow Administrator to send warning notifications to a User, lock out a User, and restrict a User's permissions.
	7.0 – System Dashboard
	(Note: There are no Minimum Solution Requirements within this Section 7.0)
	8.0 – Types of Transactions (TOTs)
8.1	The Solution **SHALL** be capable of submitting the following TOTs to the County's MBIS via interface: • All California State TOTs • State and County TOT's currently used in Los Angeles County, including but not limited to: ➢ ID2 ➢ ID4 ➢ Release ➢ Quick-ID ➢ Pre-ID ➢ Local Applicant Submission ➢ Update ➢ Test Record Submission ➢ Registrant ➢ DNS (option 2)
8.2	The Solution **SHALL** be capable of a DNA submission to Cal-DOJ for criminal (CRM) transaction types, as follows: • CRM TOT • As a stand-alone transaction • As a converted transaction, modified to a CRM TOT
8.3	The Solution **SHALL** be able to receive, via interface response notifications from external systems (e.g., Cal-DOJ, FBI and MBIS), process the notification within CBS, and print for booking record.
	9.0 – Quick-ID Functionality
9.1	The Quick-ID Solution **SHALL** include (2) desktop devices in a configuration described in Section 13.0 below, capable of submitting a hand/fingerprint(s) and an iris capture to the MBIS for identification verification, using the QID Type of Transaction (TOT).
9.2	The Quick-ID Solution **SHALL** be able to receive, process, and print response notifications from MBIS.
9.3	The Quick-ID Solution **SHALL** be able to receive, process, and print a booking photo from the County's Digital Mugshot System (DMS) or MBIS, based on the submitted biometric match (e.g. State, FBI or County identifiers).

Req #	Requirement
	10.0 –Hardware
10.1	The Solution equipment hardware **SHALL** be new (unused) and current model.
10.2	The Livescan equipment SHALL be supplied with all components specified in Sections 12, 13 and 14 below, delivered complete and functionally ready to operate.
10.3	All equipment **SHALL** work on standard 120 volt circuit and be Underwriters Laboratory (UL) approved; maximum 20 amps.
10.4	The Livescan equipment **SHALL** include an uninterrupted power supply (UPS) unit and a power conditioner, including surge suppression rated at 2,500 amps, which will provide power to each Livescan device (may exclude camera or printer) for a minimum of 15 minutes.
10.5	Each Livescan device **SHALL** have all the necessary accessories (e.g., power cord, cabling) to make the device fully functional at installation.
10.6	The Livescan device and its peripherals **SHALL** utilize existing sites' current configuration without physical modification to the facilities (i.e. new conduit, moving power, moving light bar, installation of a pedestal).
10.7	Each Livescan device **SHALL** have its own Cisco managed network switch that can be monitored by Sheriff's Data Network (such as model WS-C2960C-8PC-L or agreed upon by Sheriff's Data Network).
10.8	The software on the Livescan device **SHALL** be the same software that Cal-DOJ Certified.

Req #	Requirement
	11.0 – Hardware – General Livescan Devices (Quantity: 163)
11.1	The Solution **SHALL** include the following attributes for ***163 Livescan Devices***: • PC • Monitor-24" Touch Screen Flat Panel (maximum) with 12" display height (minimum) • Full-function, QWERTY wired keyboard with a numeric pad, separate function keys, and navigation keys. • Webcam, minimum 2.0 megapixels resolution, either built in the Monitor or wired-type and mounted to the Monitor (for face biometric login authentication) • Wired Optical Mouse • Wired 2D barcode reader • Wired magnetic stripe card reader • Wired Digital Signature Pad • 1000ppi Hand/finger capture scanner(s) • Iris Camera, mounted in clear view (Requirement #19.0) • A locking mechanism to prevent User from manually turning off Livescan device • Foot pedals located on both front corners of the cabinet (to allow User access regardless of left or right print capture positioning) • Casters with locking mechanism Uninterrupted Power Supply and monitoring software (Requirements #s 1.16, 1.17, and 10.4)
11.2	The Solution **SHALL** include at least (1) one additional method other than foot pedals (e.g., button or switch) to activate scanners.
11.3	The Solution's general Livescan device **SHALL** be housed in a ruggedized cabinet with the following maximum dimensions: • 72 inches height (including all peripherals) • 32 inches width • 30 inches depth
	12.0 – Hardware – Coroner Livescan Devices (Quantity: 2)

Req #	Requirement
12.1	The Solution **SHALL** include the following attributes for ***2 Coroner Devices***: • PC • Monitor-24" Touch Screen Flat Panel (maximum) with 12" display height (minimum) • Full-function, QWERTY wired keyboard with a numeric pad, separate function keys, and navigation keys. • Webcam, minimum 2.0 megapixels resolution, either built in the Monitor or wired-type and mounted to the Monitor (for face biometric login authentication) • Wired Optical Mouse • Wired 2D barcode reader • Wired magnetic stripe card reader • Wired Digital Signature Pad • Minimum 500ppi Hand/finger capture scanner(s) adapted to the Coroner's unique business need • A locking mechanism to prevent User from manually turning off Livescan device • Foot pedals located on both front corners of the cabinet to allow User access regardless of left or right print capture positioning • Casters with locking mechanism • Uninterrupted Power Supply (Requirements #s 1.16, 1.17, and 10.4)
12.2	Coroner's fingerprint capture equipment **SHALL** be adapted and configured to Coroner's unique business need.
12.3	The Solution's coroner Livescan device **SHALL** be housed in a ruggedized cabinet with the following maximum dimensions: • 72 inches height (including all peripherals) • 32 inches width • 30 inches depth

Req #	Requirement
	13.0 – Hardware – Quick-ID Devices (Quantity: 2)
13.1	The Solution's Quick-ID device **SHALL** include the following attributes (Quantity 2): • PC • Monitor-24" Touch Screen Flat Panel (maximum) with 12" display height (minimum) • Full-function, QWERTY wired keyboard with a numeric pad, separate function keys, and navigation keys. • Webcam, minimum 2.0 megapixels resolution, either built in the Monitor or wired-type and mounted to the Monitor (for face biometric login authentication) • Wired Optical Mouse • Wired 2D barcode reader • Wired Digital Signature Pad • Minimum 500ppi Hand/finger capture scanner(s) • Iris camera (Requirement #18.0) • 1 Wired foot pedal with capture and save capability • Uninterrupted Power Supply (Requirements #s 1.16, 1.17, and 10.4).
	14.0 – Hardware – Central Server Configuration
14.1	The Solution's Central Server Configuration **SHALL**: • Be contained in a Contractor-provided single server rack, with redundant power sources provided by LASD's data center • Include all the servers and internal networking necessary for the entire CBS Solution functionality, installed in the rack • Have redundant networking capabilities to the Department's PAC50 Network • Include two communication protocols to the Contractor's second data center site, as follows: a. Contractor-provided direct point-to-point communication line ***b.*** VPN connection via the internet (as backup)

Req #	Requirement
	15.0 – Printer Functionality
15.1	The Solution **SHALL** be able to print within an agency and to the following network-type printers, including existing agency printers currently on hand (Refer to Section 16.0 for printer requirements). • FBI certified laser printer • Color laser printer • Non-FBI certified laser printer • Wristband printer • Paperless printer Solution
15.2	The Solution **SHALL** have the capability of printing to multiple printers and be configurable at any time by County, to print only those response messages, booking forms, Subject wrist bands, etc. that are requested by each agency or location.
15.3	The printers **SHALL** have the capability of receiving print jobs from multiple Livescan or biometric capture devices.
15.4	The Solution **SHALL** be capable of watermarking any image prior to packaging and submitting through the central server. Watermarking any image is configurable by Administrators based on permissions.
	16.0 – Printers – Color Laser (Quantity: 144)
16.1	The Solution's color laser printer **SHALL** have, at minimum, the following attributes: • 10/100/1000BaseTX Ethernet and USB 2.0 and/or above connections • Print speed supporting up to 22 ppm or higher • Resolution of 600 by 600 dpi • 40,000 page monthly duty cycle (minimum) • Duplex printing capable, automatic 2-sided i) Tray 1: (Multipurpose tray): Custom sizes: 3 x 5 in. to 8.5 x 14 in. (76.2 x 127 mm to 216 x 356 mm); capacity 150 pages minimum ii) Tray 2: (optional) Custom sizes: 5.8 x 8.3 in. to 8.5 x 14 in. (148 x 210 mm to 216 x 356 mm); capacity 500 pages iii) Manual feed function (optional) • Toner capacity yield of at least 6,000 sheets

Req #	Requirement
	17.0 – Paperless Storage/Print Functionality on Demand
17.1	The Solution **SHALL** be capable of storing electronic documents and be accessible through a web service, both within the local law enforcement agency and the central site as a central repository. An agency can select and print any of the electronic documents received by the Solution's Livescan device assigned to their agency, to any of that agency's printer(s).
17.2	The printerless Solution **SHALL** be capable of different output formats, including PDF, MHT, TIFF, PNG, and JPEG. It **SHALL** also support email capability.
17.3	The central repository **SHALL** retain record documents indefinitely or until sealed or expunged.
17.4	The document repository on each Livescan device **SHALL** be retained for as long as the corresponding record is available on that device.
	18.0 – MugShot Camera (Quantity: 139)
18.1	The camera **SHALL** have a minimum of 10 Megapixels and comparable to a 1/4-Type CCD Sensor, or better.
18.2	Image quality **SHALL** meet or exceed the NIST Best Practice Recommendations for the Capture of mugshots http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
18.3	The camera **SHALL** have livescan Solution software-controlled Digital SLR, where the software controls the camera's zoom, photo capture, and power management.
18.4	The Solution **SHALL** be capable of taking a whole single image and allows the User to manually crop multiple scars, marks and tattoos (SMTs) with a roping type software tool and further allow close cropping using an intuitive software design.
18.5	The camera **SHALL** have auto face-finding capability either through hardware or software Solution.
18.6	The Solution **SHALL** support auto-sizing for front and profile photos with User override capability configured by system Administrator.
18.7	The Solution **SHALL** support the capturing of up to 99 SMTs per criminal transaction.
18.8	The Solution **SHALL** require the User at the Livescan device to capture SMT photos in instances where a booking record was initiated elsewhere (i.e., agency RMS) indicated that an SMT exists on the Subject.
18.9	The User **SHALL** be able to override the initial descriptions and/or SMT location based on policy (ies) if the record was initially started elsewhere (i.e. agency RMS).
18.10	The camera **SHALL** be capable of feeding an image to, and be controlled from, multiple Livescans.
18.11	Mugshot image quality (i.e, Subject's sizing in photo) at all sites **SHALL** remain consistent throughout the County, regardless of the Livescan device setup and location, identified in 'Equipment Locations & Inventory' (Exhibit D) to the SOW. Most sites utilize a ceiling mounted three (3) point lighting system, as illustrated in 'Sample Equipment Setup Diagram' (Attachment G.1) to the SOW.

Req #	Requirement
18.12	All mugshot camera installations **SHALL** be hard-wired and able to utilize existing sites' footprint without physical modification to the facilities (i.e. new conduit, moving power, moving light bar, installation of a pedestal). Using 'Sample Equipment Setup Diagram' (Attachment G.1) to the SOW as the standard location configuration, describe how your mugshot quality component will be integrated at a site.
	19.0 – Iris Camera (Quantity: 163)
19.1	The Iris Type 17 Transaction within the Solution, **SHALL** conform to the most current "Technical Specifications Document for the Iris Pilot (IP) Project" as specified by the FBI. https://www.fbibiospecs.cjis.gov/Document/Get?fileName=Iris_Pilot_Technical_Specification_DRAFT-v2-6-8.pdf
19.2	The Iris camera **SHALL** be securely attached to the Solution's cabinet or with a locking device (i.e. security cable) for positioning the camera forward, with vendor-provided interconnection wiring/cabling from CPU to camera
19.3	The Iris camera **SHALL** capture both eyes simultaneously on the first capture, allow individual captures after alerting User when the original capture quality is poor, and/or override if necessary (i.e., artificial eye).
	20.0 – Connectivity
20.1	The Solution **SHALL** support network connectivity of 10Base-T (RJ-45) TCP/IP, UDP, SMTP.
20.2	The Solution **SHALL** have a real-time interface to the County's MBIS using a County network connection. Interfaces include, but are not limited to FTP, SMTP, Web Services, SFTP, etc.
	21.0 – Fingerprint Images – includes all fingerprint images captured
21.1	The Solution **SHALL** support 1000ppi which is required for all fingerprint images captured in Section 12 above 'General Livescan Devices,' including: • Individually rolled • 4-Finger flats • Palm print and Writer's palm (describe optics), including: i. Upper / Lower ii. Whole Hand iii. Writer's Edge
21.2	The Solution **SHALL** support 1000ppi using JPEG 2000 15:1 Compression and is backward compatible to 500 WSQ.
21.3	The Solution **SHALL** be in compliance with "Profile for 1000ppi Fingerprint Compression" Version 1.1 https://www.fbibiospecs.cjis.gov/Document/Get?fileName=J2K1000.pdf
	22.0 – Fingerprint Image Capture
22.1	If the Solution optics do not capture the whole palm (with one pass), it **SHALL** include all images that are applicable to that Solution's device (rolls, flats, upper palm, lower palm, inter-digital, and writer's edge).
22.2	The Solution **SHALL** support 4-finger flat to roll comparison (i.e., detection of fingers rolled out of sequence).
22.3	The Solution **SHALL** be within 99.5% match accuracy.

Req #	Requirement
22.4	The Solution **SHALL** support 4-finger flat to match against all captured flats and alert the User if there is not a match.
22.5	The Solution **SHALL** be configurable to allow the "out of sequence" finger to be saved.
22.6	The Solution **SHALL** provide a side-by-side view of two or more images if the image already exists, with scoring to allow the User to decide which image to save.
22.7	The Solution **SHALL** provide way of annotating the image when a capture cannot occur or is an exception (e.g., scarred, amputation). Annotation can occur either before or after capture.
	23.0 – Image Capture Times
23.1	The Solution **SHALL** provide capture times as listed below. Capture timing will be from activation of foot pedal (button, or other type of switch) or if auto capture from acceptance of last image captured until the quality check is done and displayed on screen: • Flat single finger - 2 seconds • Rolled images - 3 seconds • Upper Palm - 3 seconds • Lower Palm – 3 seconds
23.2	The Solution **SHALL** provide capture times, as listed below. Capture timing will be from activation of foot pedal (button, or other type of switch) to support upper palm and the four (4) finger flat images, and display on the screen: • Upper Palm - 3 seconds • Whole hand - 6 seconds
	24.0 – Fingerprint Image Quality Override
24.1	The Solution **SHALL** check every image capture for quality.
24.2	The Solution **SHALL** allow the User to override and accept what the system determines to be a poor image, and log this action.
24.3	The Solution **SHALL** be configurable to force the User to try and obtain a better quality image by a configurable number of times.
24.4	When the User's statistics drop below a configurable acceptable level, the Solution **SHALL** restrict the User's account.
24.5	The User's access **SHALL** be turned off when their statistics fall below a configured acceptable level.
24.6	The Solution **SHALL** allow the User to save the best print of all re-rolled prints.
24.7	The Solution **SHALL** track each User's image quality results.

Req #	Requirement
	25.0 – User and Administrator Calibration Checks
25.1	If capture scanners are not self-calibrating, the Solution **SHALL** allow Users to check and perform a scanner calibration for each attached scanner capture type. This calibration process **SHALL** not exceed one (1) minute.
25.2	If capture scanners are not self-calibrating, the Solution **SHALL** alert Users to perform scanner calibration by a configurable schedule (i.e., after twenty-five (25) bookings or twenty-one (21) days, whichever is earlier).
	26.0 – General Interface, Network, Hardware, and Software
26.1	The Solution **SHALL** support automatic updates at the device level.
26.2	The Solution **SHALL** be capable of synchronizing with time servers for all devices utilizing Network Time Protocol (NTP.)
26.3	The Solution **SHALL** display to the User, an intuitive status indicator for designated interfaces on which the Livescan device relies to communicate, indicating their connectivity.
26.4	The Solution **SHALL** still process a transaction when the network and/or AJIS interface is unavailable, and **SHALL** alert the User (i.e., warning message) advising them when working in an offline mode.
26.5	The Solution **SHALL** allow Users to log into the Livescan devices when the network and/or AJIS interface is unavailable.
26.6	The Solution **SHALL** have software version control and be capable of an automated procedure to ensure that all devices are running the same software, drivers, firmware, module, or other components.
26.7	The Solution **SHALL** have a table version control and be capable of handling more than one version of tables (agency and/or location-specific table values).
26.8	The Solution **SHALL** be compliant with the most recent version of the following standards: • NIST - Types 1, 2, 4, 8, 9, 10, 14, 15, and 17, as well as additional future types within 6 weeks of publication • EBTS • Cal-DOJ NIST • FBI/CJIS • LA County NIST (Attachment G.5) to the SOW • American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) http://www.nist.gov/itl/iad/ig/ansi_standard.cfm Note: The Solution **SHALL** remain compliant with the above standards, throughout the term of the Contract, as new versions are published.
26.9	The Solution **SHALL** support custom print formats (e.g., Los Angeles County booking slip, wristbands, medical screening forms, certificate of release, bail deviation form, and additional charge form) shown in 'Sample Booking Forms' (Attachment G.3) to the SOW.

Req #	Requirement
26.10	The Solution **SHALL** allow system Administrators to design custom report formats using a 3rd Party Report Writer (i.e., Crystal Reports), and print them based on permissions.
26.11	All licenses for any third party software required for this Solution **SHALL** be included.
26.12	The Solution **SHALL** save partially completed bookings and allow a User to retrieve and continue the booking process after a Subject's fingerprint identification, from conditions such as: • After a local identification with 99.5% match accuracy • After an MBIS identification
26.13	The Solution **SHALL** be capable of retrieving an incomplete booking transaction from a Livescan device than originally started.
26.14	The Solution **SHALL** support the ability to block the editing of a record when the fingerprint identification falls below the 99.5% match threshold.
26.15	The Solution **SHALL** support the ability to allow limited editing without fingerprint identification.
26.16	The Solution **SHALL** support Barcode Scanning and printing (two-dimensional capable) for the following example purposes: • To aid in data entry • To initiate a demographic download • To be used with any TOT or function • For wristband printing • All booking documentation • For ID Card
26.17	The Solution **SHALL** support completed booking review on the Livescan device, prior to submission/transmission of booking record.
26.18	The Solution **SHALL** be capable of supporting a touch screen monitor.
26.19	The Solution **SHALL** be compliant with Global Justice XML Data Dictionary Version 3.0 or most current.
26.20	The Solution **SHALL** support screen lock after configurable number of minutes.
26.21	The Solution **SHALL** support biometric logins with any combination of the following: • User's account credentials (User ID and password) • User's fingerprint, captured with Livescan's fingerprint scanner • User's iris, captured with Livescan's iris camera • User's face, captured with Livescan's webcam
26.22	The Solution **SHALL** be capable of reading a magnetic stripe card (primarily used for a Subject's Driver's License).

Req #	Requirement
26.23	The Solution **SHALL** provide advance warning via e-mail notification to the LACRIS Help Desk when the Solution is detecting eminent failure/or system degradation.
26.24	The Solution Livescan device **SHALL** retain the 2,500 most recent transaction records and 100,000 submitted NIST files.
26.25	The Solution **SHALL** support RAID configurations of either RAID 5, RAID 6, RAID 10 or RAID 50 to protect against data loss and system downtime in the event of mechanical failure of one (1) hard drive.
26.26	The Solution **SHALL** not delete any previous transaction record unless it was successfully transmitted to all designated destinations with ensured delivery and/or by system Administrator.
26.27	The Solution **SHALL** provide a warning to the User when three (3) attempts to send a transaction have failed and/or were unsuccessfully transmitted to all the designated systems; it **SHALL** also send an e-mail to the system Administrators of the failed submissions.
26.28	All of the Solution's network communications **SHALL** meet the 'Sheriff's Data Network System Security Standards' to the SOW.
26.29	The Solution **SHALL** encrypt County specified data, including criminal, throughout the Solution.
26.30	The Solution **SHALL** provide a notification/messaging function that allows the LACRIS Help Desk to post priority messages directly to the Livescan devices informing the User of current system issues. (e.g., Cal-DOJ is down, planned system shutdowns, etc.)
	27.0 – Automated Booking Segment (ABS) Module
27.1	**The Solution** SHALL include a browser-based, web-enabled, data entry module, referred to in this Section as the Automated Booking Segment(ABS) Module (ABSM), accessible from any County-provided computer device with network connectivity on a County-specified secured network
27.2	The Solution's ABSM **SHALL** be fully integrated with the CBS software installed on the Livescan devices, where CBS booking records from either the Livescan device or a web browser, will be: • Created, assigning a unique booking number • Retrieved • Edited • Saved • Copied as a new booking record (and new booking number) • Printed (in hardcopy, TIFF, and PDF)

Req #	Requirement
27.3	The Solution's ABSM **SHALL** resemble the County's current Automated Booking System's workflow and GUI, 'Sample Booking Forms (Attachment G.3) to the SOW, taking the following into consideration: • Login/security protocols • The order of the GUI screens • Screen navigation • The placement of data fields per screen • The field tabbing sequence in a screen • Mandatory fields required in each screen before proceeding to the next screen • Drop-down table values
27.4	The Solution's ABSM **SHALL** include a Participating Agency-specific tiered electronic approval workflow process, not to exceed 5 levels, as follows: • Initiating User completes a booking record consisting of multiple forms, as provided in 'Sample Booking Forms (Attachment G.3) to the SOW, **and submits to** next level for review/approval • Next level User reviews the booking record and will either: i) Edit the record, approve and submit to next level for their approval ii) Reject the record for correction by the initiating User, providing a rejection explanation in an ABS free-text field • Every User in the approval process will have their own work queue, and booking records that have not obtained final level approval shall be displayed with record status • The booking record can be edited and saved (as the most current record) by any level in this workflow process • The booking record shall, at the Agency's discretion for each of their Users, be completely paperless or allow some or all of the record be printed in hardcopy • Electronic approvals (in lieu of signatures) are applied to the booking record when User verifies/approves record • Approved booking records are automatically routed to the next level review or final record approval • The above workflow process is configurable in CBS' System Administration module by agency, level approvals, etc.

Req #	Requirement
27.5	The Solution's ABSM **SHALL i**nclude data entry fields that mirror the look and workflow of the County Booking Forms, 'Sample Booking Forms (Attachment G.3) to the SOW, requiring: • Mandatory data entry fields • Different field types (drop down values, table dictionary driven, date and date/time, radio buttons, free text, etc.), with validation rules • Alike data fields across booking form screens auto-populate, for reducing data entry
27.6	The Solution's ABSM **SHALL** assign and display on each screen both the booking number and unique ABS to CBS transaction number.
27.7	The Solution's ABSM **SHALL** auto-save a partially completed booking record when moving from one screen field to the next and, when required, every thirty (30) seconds within the same field.
27.8	The Solution's ABSM **SHALL** lock a booking record for a County-defined time period, and allow a System Administrator to unlock the record.
27.9	The Solution's ABSM **SHALL** alert the originating record User, upon returning to the booking record, that the record was updated by another User, identifying the other User.
27.10	The Solution's ABSM **SHALL** as part of the booking process, prompt a User working in the field to attach a Subject's biometric identifier into the booking record. Allow User to override this step once User enters a reason (e.g., Subject has amputations).
27.11	The Solution's ABSM **SHALL** submit a fingerprint capture via the Mobile Gateway interface 'System Interfaces' (Exhibit C) to the SOW, and attach to the booking record for verifying the Subject during the livescan process.
27.12	The Solution's ABSM **SHALL** include navigation tools (e.g., screen tabs, command buttons) for the User to navigate from one data entry screen to another.
27.13	The Solution's ABSM **SHALL** include intuitive touchscreen capabilities for any County-provided computer device that has this technology.
27.14	The Solution **SHALL** be capable of tracking each User who views, edits, or prints specified forms.
27.15	The Solution's ABSM **SHALL** be configurable to include additional tables and fields, with or without drop down menus, when required by County to conform to changing business practices.
	28.0 – Records Management System (RMS) and External System Interfaces
28.1	The Solution **SHALL** interface with external systems, as identified and summarized in 'System Interfaces' (Exhibit C) to the SOW.
28.2	The Solution **SHALL** support two-way interfacing to multiple Participating Agency RMSs (multiple interfaces), where updates made in the agency's RMS also updates the booking record in the Livescan device.

Req #	Requirement
28.3	The Solution **SHALL** allow a single Livescan to communicate simultaneously to multiple RMS interfaces (e.g., Site A's Livescan creates a record but submits it to three different RMS interfaces [Sites A, B, and C]).
28.4	The Solution **SHALL** interface with County's AJIS for modifying any allowable fields after the initial booking and fingerprint verification of subject; automatic locking of edit feature after a configurable amount of time and/or events with admin override. This type of modification would deny User to resend NIST file to MBIS without authorization.
28.5	The Solution **SHALL** include terminal emulator functionality (i.e., TCP/IP) on the Livescan device(s), for sending/receiving messages to/from JDIC.
28.6	The Solution **SHALL** support JDIC messaging, FTP, SMTP, SQL and XML as these are anticipated to be the primary methods for interface.
28.7	The Solution **SHALL** support standard XML protocols for the local Participating Agencies' RMS, as follows: • GJXDM - the current XML protocol utilized by 20+ agencies • NIEM - the newest and more robust protocol for all replacement RMS connections, as chosen by the Participating Agency • FTP (File Transfer Protocol)
28.8	The Solution **SHALL** be "Single Data Entry." A booking record may begin on the Livescan device, local RMS, or AJIS.
28.9	The Solution **SHALL** support a query from any Participating Agency's RMS to CBS's database via a SQL database view on each Livescan, as well as the central database servers, for importing into the RMS new records and modified records from CBS.
28.10	The Solution **SHALL** handle the functionality above 27.9 in the following formats: • Cal-DOJ NIST with and without Type 10, 'Cal-DOJ NIST' • Los Angeles County NIST with and without Type 10, 'County NIST Data Types' (Attachment G.4) to the SOW
28.11	The Solution **SHALL** support an interface with the County's consolidated booking system (currently AJIS) using TCP/IP (current), database-stored procedure calls, or web services such as GJXDM/NIEM.
	29.0 – Continuity of Operations
29.1	The Solution's central server functionality for the CBS Production environment **SHALL** be replicated at a secondary vendor-provided site.
29.2	The Solution's secondary site **SHALL** be located outside Los Angeles County, for meeting County's Disaster Recovery provisions.

Req #	Requirement
29.3	The Solution's secondary site **SHALL** be CJIS compliant and located either in the vendor's designated Data Center or a CJIS-compliant cloud.
29.4	The Solution's secondary site **SHALL** be redundant to the Solution's primary site at LASD's Data Center for a seamless system failover, in instances when the primary site is down for an extended period of time.
29.5	The Solution's secondary site **SHALL** be load balanced as active/active environments, with the Solution's primary site at LASD's Data Center, for maintaining system performance during heavy Solution use.
29.6	The Solution's secondary site **SHALL** include all hardware, Software licensing, and maintenance (including interfaces, O/S, database, virus scan, report writer and other 3rd party software).
29.7	The Solution's secondary site **SHALL** include, at the vendor's expense, a direct network communication line from LASD's Data Center to the secondary site location.
29.8	The solution **SHALL** support the option to automatically forward all positive identification responses received by a Livescan to Participating Agencies' RMS via web services (e.g. GJXDM/NIEM) and FTP, based on the Participating Agency's RMS capability for updating the RMS record.
29.9	The Solution **SHALL** meet all System Performance measurements specified Exhibit C (Service Level Agreement), Schedule C.4 (Solution Performance Requirements).