CETS #:	
Agency Reference #:	CBE 606906-23

INTERLOCAL CONTRACT BETWEEN PUBLIC AGENCIES

A Contract Between the State of Nevada
Acting by and through its

Public Entity #1:	**Department of Public Safety, Records Communications and Compliance Division**
Address:	**333 West Nye Lane #100**
City, State, Zip Code:	**Carson City, NV 89706**
Contact:	**Kami Thompson**
Phone:	**775-684-6259**
Fax:	**N/A**
Email:	**k.thompson@dps.state.nv.us**

Public Entity #2:	**Clark County, Nevada on Behalf of Department of Human Resources**
Address:	**500 S. Grand Central Pkwy. / P.O. Box 551791**
City, State, Zip Code:	**Las Vegas, NV 89155**
Contact:	**Dino Cui**
Phone:	**702-455-3193**
Fax:	**N/A**
Email:	**Dino.Cui@clarkcountynv.gov**

WHEREAS, NRS 277.180 authorizes any one or more public agencies to contract with any one or more other public agencies to perform any governmental service, activity or undertaking which any of the public agencies entering into the contract is authorized by law to perform; and

WHEREAS, it is deemed that the services hereinafter set forth are both necessary and in the best interests of the State of Nevada.

NOW, THEREFORE, in consideration of the aforesaid premises, the parties mutually agree as follows:

1. **REQUIRED APPROVAL**. This Contract shall not become effective until and unless approved by appropriate official action of the governing body of each party.

2. **DEFINITIONS**

TERM	DEFINITION
State	The State of Nevada and any State agency identified herein, its officers, employees and immune contractors.
Contracting Entity	The public entities identified above.
Fiscal Year	The period beginning July 1st and ending June 30th of the following year.
Contract	Unless the context otherwise requires, 'Contract' means this document titled Interlocal Contract Between Public Agencies and all Attachments or Incorporated Documents.

CETS #:	
Agency Reference #:	CBE 606906-23

3. **CONTRACT TERM.** This Contract shall be effective as noted below, unless sooner terminated by either party as specified in ***Section 4, Termination***.

Effective From:	August 1, 2024	To:	May 31, 2028

4. **TERMINATION.** This Contract may be terminated by either party prior to the date set forth in ***Section 3, Contract Term,*** provided that a termination shall not be effective until **30** days after a party has served written notice upon the other party. This Contract may be terminated by mutual consent of both parties or unilaterally by either party without cause. The parties expressly agree that this Contract shall be terminated immediately if for any reason State and/or federal funding ability to satisfy this Contract is withdrawn, limited, or impaired.

5. **NOTICE.** All communications, including notices, required or permitted to be given under this Contract shall be in writing and directed to the parties at the addresses stated above. Notices may be given: (a) by delivery in person; (b) by a nationally recognized next day courier service, return receipt requested; or (c) by certified mail, return receipt requested. If specifically requested by the party to be notified, valid notice may be given by facsimile transmission or email to the address(es) such party has specified in writing.

6. **INCORPORATED DOCUMENTS.** The parties agree that this Contract, inclusive of the following Attachments, specifically describes the Scope of Work. This Contract incorporates the following Attachments in descending order of constructive precedence:

ATTACHMENT AA:	LIVESCAN USER AGREEMENT
ATTACHMENT BB:	SCOPE OF WORK
ATTACHMENT CC:	TERMS AND CONDITIONS
ATTACHMENT DD:	LIVESCAN CONNECTION REQUEST FORM
ATTACHMENT EE:	PHYSICAL AND TECHNICAL SECURITY REQUIREMENTS FOR NEVADA LIVESCAN INSTALLATIONS

Any provision, term or condition of an Attachment that contradicts the terms of this Contract, or that would change the obligations of the State under this Contract, shall be void and unenforceable.

7. **CONSIDERATION.** The Central Repository and the Livescan Entity agree to provide the services set forth in the incorporated documents in Section 6, Incorporated Documents. Fees associated with Livescan shall be assessed by the Livescan Entity in accordance with the most current fee schedule located on the State of Nevada, Department of Public Safety's website (http://www.rccd.nv.gov).

8. **ASSENT.** The parties agree that the terms and conditions listed in the incorporated Attachments of this Contract are also specifically a part of this Contract and are limited only by their respective order of precedence and any limitations expressly provided.

9. **INSPECTION & AUDIT**

A. Books and Records. Each party agrees to keep and maintain under general accepted accounting principles full, true and complete records, agreements, books, and document as are necessary to fully disclose to the State or United States Government, or their authorized representatives, upon audits or reviews, sufficient information to determine compliance with all State and federal regulations and statutes.

B. Inspection & Audit. Each party agrees that the relevant books, records (written, electronic, computer related or otherwise), including but not limited to relevant accounting procedures and practices of the party, financial statements and supporting documentation, and documentation related to the work product shall be subject, at any reasonable time, to inspection, examination, review, audit, and copying at any office or location where such records may be found, with or without notice by the State Auditor, Employment Security, the Department of Administration, Budget Division, the Nevada State Attorney General's Office or its Fraud Control Units, the State Legislative Auditor, and with regard to any federal funding, the relevant federal agency, the Comptroller General, the General Accounting Office, the Office of the Inspector General, or any of their authorized representatives.

C. Period of Retention. All books, records, reports, and statements relevant to this Contract must be retained a minimum three years and for five years if any federal funds are used in this Contract. The retention period runs from the date of termination of this Contract. Retention time shall be extended when an audit is scheduled or in progress for a period reasonably necessary to complete an audit and/or to complete any administrative and judicial litigation which may ensue.

10. **BREACH - REMEDIES**. Failure of either party to perform any obligation of this Contract shall be deemed a breach. Except as otherwise provided for by law or this Contract, the rights and remedies of the parties shall not be exclusive and are in addition to any other rights and remedies provided by law or equity, including but not limited to actual damages, and to a prevailing party reasonable attorneys' fees and costs. It is specifically agreed that reasonable attorneys' fees shall not exceed $150.00 per hour.

11. **LIMITED LIABILITY**. The parties will not waive and intend to assert available NRS Chapter 41 liability limitations in all cases. Contract liability of both parties shall not be subject to punitive damages. Actual damages for any State breach shall never exceed the amount of funds which have been appropriated for payment under this Contract, but not yet paid, for the fiscal year budget in existence at the time of the breach.

12. **FORCE MAJEURE**. Neither party shall be deemed to be in violation of this Contract if it is prevented from performing any of its obligations hereunder due to strikes, failure of public transportation, civil or military authority, acts of public enemy, acts of terrorism, accidents, fires, explosions, or acts of God, including, without limitation, earthquakes, floods, winds, or storms. In such an event the intervening cause must not be through the fault of the party asserting such an excuse, and the excused party is obligated to promptly perform in accordance with the terms of the Contract after the intervening cause ceases.

13. **INDEMNIFICATION**. Neither party waives any right or defense to indemnification that may exist in law or equity.

14. **INDEPENDENT PUBLIC AGENCIES**. The parties are associated with each other only for the purposes and to the extent set forth in this Contract, and in respect to performance of services pursuant to this Contract, each party is and shall be a public agency separate and distinct from the other party and, subject only to the terms of this Contract, shall have the sole right to supervise, manage, operate, control, and direct performance of the details incident to its duties under this Contract. Nothing contained in this Contract shall be deemed or constructed to create a partnership or joint venture, to create relationships of an employer-employee or principal-agent, or to otherwise create any liability for one agency whatsoever with respect to the indebtedness, liabilities, and obligations of the other agency or any other party.

15. **WAIVER OF BREACH**. Failure to declare a breach or the actual waiver of any particular breach of the Contract or its material or nonmaterial terms by either party shall not operate as a waiver by such party of any of its rights or remedies as to any other breach.

16. **SEVERABILITY**. If any provision contained in this Contract is held to be unenforceable by a court of law or equity, this Contract shall be construed as if such provision did not exist and the non-enforceability of such provision shall not be held to render any other provision or provisions of this Contract unenforceable.

17. **ASSIGNMENT**. Neither party shall assign, transfer or delegate any rights, obligations or duties under this Contract without the prior written consent of the other party.

18. **STATE OWNERSHIP OF PROPRIETARY INFORMATION**. Any data or information provided by the State to Livescan Entity and any documents or materials provided by the State to Livescan Entity in the course of the Contract ("State Materials") shall be and remain the exclusive property of the State and all such State Materials shall be delivered into State possession by Livescan Entity upon completion, termination, or cancellation of this Contract.

CETS #:	
Agency Reference #:	CBE 606906-23

19. **PUBLIC RECORDS**. Pursuant to NRS 239.010, information or documents may be open to public inspection and copying. The parties will have the duty to disclose unless a particular record is made confidential by law or a common law balancing of interests.

20. **CONFIDENTIALITY**. Each party shall keep confidential all information, in whatever form, produced, prepared, observed or received by that party to the extent that such information is confidential by law or otherwise required by this Contract.

21. **FEDERAL FUNDING**. In the event, federal funds are used for payment of all or part of this Contract, the parties agree to comply with all applicable federal laws, regulations and executive orders, including, without limitation the following:

A. The parties certify, by signing this Contract, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from participation in this transaction by any federal department or agency. This certification is made pursuant to Executive Orders 12549 and 12689 and Federal Acquisition Regulation Subpart 9.4, and any relevant program-specific regulations. This provision shall be required of every subcontractor receiving any payment in whole or in part from federal funds.

B. The parties and its subcontractors shall comply with all terms, conditions, and requirements of the Americans with Disabilities Act of 1990 (P.L. 101-136), 42 U.S.C. 12101, as amended, and regulations adopted thereunder, including 28 C.F.R. Section 35, inclusive, and any relevant program-specific regulations.

C. The parties and its subcontractors shall comply with the requirements of the Civil Rights Act of 1964 (P.L. 88-352), as amended, the Rehabilitation Act of 1973 (P.L. 93-112), as amended, and any relevant program-specific regulations, and shall not discriminate against any employee or offeror for employment because of race, national origin, creed, color, sex, religion, age, disability or handicap condition (including AIDS and AIDS-related conditions.)

D. Clean Air Act (42 U.S.C. 7401–7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251–1387), as amended. Contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401–7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251– 1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

22. **PROPER AUTHORITY**. The parties hereto represent and warrant that the person executing this Contract on behalf of each party has full power and authority to enter into this Contract and that the parties are authorized by law to perform the services set forth in ***Section 6, Incorporated Documents***.

23. **GOVERNING LAW – JURISDICTION**. This Contract and the rights and obligations of the parties hereto shall be governed by, and construed according to, the laws of the State of Nevada. The parties consent to the exclusive jurisdiction of and venue in the First Judicial District Court, Carson City, Nevada for enforcement of this Contract.

24. **ENTIRE AGREEMENT AND MODIFICATION**. This Contract and its integrated Attachment(s) constitute the entire agreement of the parties and as such are intended as a complete and exclusive statement of the promises, representations, negotiations, discussions, and other agreements that may have been made in connection with the subject matter hereof. Unless an integrated Attachment to this Contract specifically displays a mutual intent to amend a particular part of this Contract, general conflicts in language between any such Attachment and this Contract shall be construed consistent with the terms of this Contract. Unless otherwise expressly authorized by the terms of this Contract, no modification or amendment to this Contract shall be binding upon the parties unless the same is in writing and signed by the respective parties hereto, approved by the Office of the Attorney General.

CETS #:	
Agency Reference #:	CBE 606906-23

IN WITNESS WHEREOF, the parties hereto have caused this Contract to be signed and intend to be legally bound thereby.

COUNTY OF CLARK:

Tick Segerblom — Date

Chair, Clark County Commissioners — Title

NEVADA DEPARTMENT OF PUBLIC SAFETY
Records, Communications and Compliance Division:

Erica Souza-Llamas — Date

RCCD Division Administrator — Title

Kristi Defer — Date

DPS ASO IV, Senior Fiscal Officer — Title

NEVADA DEPARTMENT OF PUBLIC SAFETY
Deputy Attorney General:

Approved as to form by:

Deputy Attorney General for Attorney General

On: _____ Date

CLARK COUNTY:
ATTEST:

By:_____ On:_____ Date
Lynn Marie Goya
County Clerk

Approved as to form:
Steven Wolfson, District Attorney

By: Sarah Schaerrer (Aug 8, 2024 08:09 PDT) On: Aug 8, 2024 Date
Sarah Schaerrer
Deputy District Attorney

Attachment AA

LIVESCAN PROGRAM

USER AGREEMENT

DEPARTMENT OF PUBLIC SAFETY
RECORDS, COMMUNICATIONS AND COMPLIANCE DIVISION
333 West Nye Lane #100
Carson City, Nevada 89706
Phone: (775) 684-6262 ~ Fax: (775) 687-3289
(hereinafter "CENTRAL REPOSITORY")

and

Entity

Address

City, State Zip

Contact Email

Telephone Number **Fax Number**

(hereinafter "LIVESCAN ENTITY")

WHEREAS, Livescan Entity is authorized by the state of Nevada to submit fingerprint information to the Central Repository.

WHEREAS, it is deemed that the services hereinafter set forth are both necessary and in the best interests of the State of Nevada;

NOW, THEREFORE, in consideration of the aforesaid premises, the parties mutually agree as follows:

1. REQUIRED APPROVAL. This Contract shall not become effective until and unless approved by appropriate official action of the governing body of each party.

2. DEFINITIONS.

   a) *STATE*: The State of Nevada.
   b) *LIVESCAN Entity: Entity operating within the State of Nevada that is authorized to submit electronic fingerprints via Livescan. The Livescan Entity is where the livescan device is located and used for electronic submission to the Central Repository.*
   c) *LIVESCAN COORDINATOR: The DPS RCCD employees and/or their delegates that are responsible for reviewing and monitoring the livescan program, which includes running and reviewing reports associated with unresolved livescan issues.*
   d) *LIVESCAN: Used to electronically scan and record fingerprint images directly from the finger of the applicant. The process produces fingerprint images that can be transmitted directly from the point of collection to the Central Repository. Livescan can produce multiple printed fingerprint cards on multiple card formats from one roll.*

transmitted directly from the point of collection to the Central Repository. Livescan can produce multiple printed fingerprint cards on multiple card formats from one roll.

e) *APPLICANT: Individual persons whose fingerprints and other personal information are captured by the Livescan Entity for authorized licensing, employment, and volunteer purposes.*

f) *AUTHORIZED PERSONNEL: Employees of the Livescan Entity who have access to the Livescan equipment.*

g) *AUTHORIZED PERSONNEL LIST: An individual or group of individuals, submitted to and approved by the Criminal Justice Information Services Systems Agency (CSA) pursuant to Addendum A.*

h) *FEE: Fees outlined on the State of Nevada, Department of Public Safety's website (http:www.rccd.nv.gov).*

i) *SERVICES: Livescan services which pertain to electronically transmitting the Applicants' fingerprint records and other applicant data to the Central Repository.*

j) *POLICIES: Livescan Administrative Policy & Livescan Technical Security Policy.*

3. SERVICES. In consideration of Livescan Entity's payment to the Central Repository of the fees, the Central Repository hereby agrees to provide services as stated in the attached addendum, to the User Entity. This agreement incorporates the following attachments in descending order of constructive precedence:

ATTACHMENT AA:	SCOPE OF WORK
ATTACHMENT BB:	TERMS AND CONDITIONS
ATTACHMENT CC:	LIVESCAN CONNECTION REQUEST FORM
ATTACHMENT DD:	PHYSICAL AND TECHNICAL SECURITY REQUIREMENTS FOR NEVADA LIVESCAN INSTALLATIONS

4. CONTRACT TERM. This Agreement shall be effective immediately upon final signature on this Agreement and shall remain in full force and effect for so long as the Livescan Entity maintains a Virtual Private Network (VPN) authorized by the Central Repository, unless sooner terminated by either party as set forth in this Agreement. RCCD will review this agreement biannually or as needed during the time this Agreement is in effect.

5. TERMINATION. This Contract may be terminated by either party prior to the date set forth in paragraph (4), provided that a termination shall not be effective until **30** days after a party has served written notice upon the other party. This Contract may be terminated by mutual consent of both parties. The parties expressly agree that this contract shall be terminated with reasonable notice if for any reason State and/or federal funding ability to satisfy this Contract is withdrawn, limited, or impaired. The Central Repository may immediately terminate this agreement without advance written notice if the Livescan Entity, including any of its officers, employees, agents, and any other person associated with the Livescan Entity, violates any applicable state or federal law, rule, regulation, or policy. Any noncompliance issues that occur during the probationary period will result in the immediate and permanent termination from the Livescan program.

6. TERMINATION OF PREVIOUS AGREEMENTS. The Contract is intended to supersede all previous agreements between the parties on the same subject matter. All previous contracts between the parties on the same subject matter are hereby terminated upon the effective date of this Contract.

7. NOTICE. All communications, including notices, required or permitted to be given under this Agreement shall be in writing and directed to the parties at the addresses stated above. Notices may be given: (i) by delivery in person; (ii) by a nationally recognized next day courier service, return receipt requested; or (iii) by certified mail, return receipt requested. If specifically requested by the party to be notified, valid notice may be given by facsimile transmission or electronic mail to the address(es) such party has specified in writing.

8. CONSIDERATION. The Central Repository and the Livescan Entity agree to provide the services set forth in the incorporated documents in ***Section 3, Services***. Fees associated with Livescan shall be assessed by the Livescan Entity in accordance with the most current fee schedule located on the State of Nevada, Department of Public Safety's website (http://www.rccd.nv.gov).

9. ASSENT. The parties agree that the terms and conditions listed on incorporated attachments of this Contract are also specifically a part of this Contract and are limited only by their respective order or precedence and any limitations expressly provided.

10. RIGHT TO REVIEW: The Central Repository retains the right to inspect, examine, review, audit, and copy (at any office or location where such records may be found) all Livescan Entity documentation related to the contract, without prior notice.

11. OBLIGATIONS AND DUTIES OF BOTH PARTIES. The parties agree the services to be performed shall be in accordance with the most current edition of all applicable rules, regulations, policies, procedures, and law.

    a. The Livescan Entity agrees to designate an individual to be the Point-of-Contact for its entity to act as the liaison to the Central Repository. The Livescan Entity agrees to notify the Central Repository within 10 business days, or in accordance with current Livescan Administrative Policy, in the event of any changes to the Point of Contact.
    b. All electronic or digital information relating to or derived from the Livescan must be accessible only to the Authorized Personnel, by means of password protection, encryption, or other means of authentication, and shall be maintained in a secure records environment which will be subject to technical security requirements and periodic technical audits by the Central Repository or its authorized agents.
    c. The Livescan Entity agrees to allow the Central Repository or its authorized agents to conduct compliance audits, with or without prior notice. The Livescan Entity also acknowledges and agrees it will allow any directed audits to be conducted to investigate allegations of misuse or unauthorized access by unauthorized personnel.
    d. The Livescan Entity agrees to immediately notify the Central Repository of any violations of this Agreement.

e. Accounts will be terminated by the Central Repository for failure to pay and will be sent to collections. Please refer to the Department of Public Safety Records, Communications and Compliance Division's website (http://www.rccd.nv.gov) for the most current fee schedule.
f. The Central Repository reserves the right to seek collection of all unpaid fingerprint fees by any legal means available, including the use of collections agents or civil actions. This Agreement may be suspended or terminated by either Party with written notice to the address contained herein when, in the reasonable estimation of the Central Repository, a breach of any material term of this Agreement has occurred.
g. All established policies referenced and or attached to this agreement must be adhered to all times. Failure to adhere to these policies, may result in suspension and/or termination of access to the livescan program.

12. DATA INTEGRITY. It is the responsibility of the Livescan Entity to ensure that accurate data is provided to the Central Repository. The Central Repository will not manipulate or modify data provided by Livescan Entity without express written permission from the Livescan Entity. The Livescan Entity is required and agrees to have a system in place to check the accuracy of the data provided to the Central Repository. The Central Repository will maintain and store data in accordance with established Nevada Criminal Justice Information System (NCJIS) policies and system specifications.

13. BREACH; REMEDIES. Failure of either party to perform any obligation of this Contract shall be deemed a breach. Except as otherwise provided for by law or this Contract, the rights and remedies of both parties shall not be exclusive and are in addition to any other rights and remedies provided by law or equity, including but not limited to actual damages, and to a prevailing party reasonable attorneys' fees and costs. It is specifically agreed that reasonable attorneys' fees shall not exceed $150 per hour.

14. LIMITED LIABILITY. The parties will not waive and intend to assert available NRS chapter 41 liability limitations in all cases. Contract liability of both parties shall not be subject to punitive damages. To the extent applicable, actual contract damages for any breach shall be limited by NRS 353.260 and NRS 354.626.

15. FORCE MAJEURE. Neither party shall be deemed to be in violation of the Contract if it is prevented from performing any of its obligations hereunder due to strikes, failure of public transportation, civil or military authority, act of public enemy, accidents, fires, explosions, or acts of God, including, without limitation, earthquakes, floods, winds, or storms. In such an event the intervening cause must not be through the fault of the party asserting such an excuse, and the excused party is obligated to promptly perform in accordance with the terms of the Contract after the intervening cause ceases.

16. IDEMNIFICATION AND DEFENSE. To the fullest extent permitted by law, Livescan Entity shall indemnify, hold harmless and defend, not excluding the State's right to participate, the State from and against all liability, claims, actions, damages, losses, and expenses, including, without limitation, reasonable attorneys' fees and costs, arising out of any breach of the obligations of Livescan Entity under this contract, or any alleged negligent or willful acts or omissions of Livescan Entity, its officers, employees and agents.

Livescan Entity's obligation to indemnify the State shall apply in all cases except for claims arising solely from the State's own negligence or willful misconduct. Livescan Entity waives any rights of subrogation against the State. Livescan Entity's duty to defend begins when the State requests defense of any claim arising from this Contract.

17. WAIVER OF BREACH. Failure to declare a breach or the actual waiver of any particular breach of the Contract or its material or nonmaterial terms by either party shall not operate as a waiver by such party of any of its rights or remedies as to any other breach.

18. SEVERABILITY. If any provision contained in this Contract is held to be unenforceable by a court of law or equity, this Contract shall be construed as if such a provision did not exist and the non-enforceability of such a provision shall not be held to render any other provision or provisions of this Contract unenforceable.

19. ASSIGNMENT. Neither party shall assign, transfer, or delegate any rights, obligations, or duties under this Contract without the prior written consent of all parties.

20. OWNERSHIP OF PROPRIETARY INFORMATION. Unless otherwise provided by law or this Contract, any reports, histories, studies, tests, manuals, instructions, photographs, negatives, blue prints, plans, maps, data, system designs, computer code (which is intended to be consideration under this Contract), or any other documents or drawings, prepared or in the course of preparation by either party in performance of its obligations under this Contract shall be the joint property of both parties.

21. PUBLIC RECORDS. Pursuant to NRS 239.010, information or documents may be open to public inspection and copying. The parties will have the duty to disclose unless a particular record is made confidential by law or a common law balancing of interests.

22. CONFIDENTIALITY. Each party shall keep confidential all information, in whatever form, produced, prepared, observed or received by that party to the extent that such information is confidential by law or otherwise required by this Contract.

23. PROPER AUTHORITY. The parties hereto represent and warrant that the person executing this Contract on behalf of each party has full power and authority to enter into this Contract and the parties are authorized by law to perform the services set forth in this Contract.

24. GOVERNING LAW; JURISDICTION. This Agreement and the rights and obligations of the parties hereto shall be governed by, and construed according to, the laws of the State of Nevada, without giving effect to any principle of conflict-of-law that would require the application of the law of any other jurisdiction. The parties consent to the exclusive jurisdiction of and venue in the First Judicial District Court, Carson City, Nevada for enforcement of this Agreement, and consent to personal jurisdiction in such court for any action or proceeding arising out of this Agreement.

25. ENTIRE AGREEMENT AND MODIFICATION. This Contract and its integrated attachment(s) constitute the entire agreement of the parties, and such are intended as a complete and exclusive statement of the promises, representations, negotiations, discussions, and other agreements that may have been made in connection with the subject matter hereof. Unless an integrated attachment to this Contract specifically displays a mutual intent to amend a particular part of this Contract, general conflicts in language between any such attachment and this Contract shall be construed consistent with the terms of this Contract. Unless otherwise expressly authorized by the terms of this Contract, no modification or amendment to this Contract shall be binding upon the parties unless the same is in writing and signed by the respective parties hereto, approved by the State of Nevada Office of the Attorney General.

SCOPE OF WORK

1. The Central Repository will:
    a. Establish, publish, and distribute policies, procedures, and standards regarding electronic submission of non-criminal justice fingerprints.
    b. Provide the Livescan Entity with the Livescan Administrative Policy and Livescan Technical Security Policy prior to finalizing the User Agreement and at any time in the future upon request from the Livescan Entity.
    c. Perform edits, quality control and audit of electronic submissions, reporting problems to the Livescan Entity and providing training when appropriate. Edits will only be done with express written permission from the Livescan Entity.
    d. Manage state systems including planned and emergency maintenance and support of electronic submissions and fingerprint identification.
    e. Identify processes that require the availability of support staff in accordance with Department policies and procedures.
    f. Provide error and acknowledgement messages for all Livescan transactions.
    g. Provide reports to the Livescan Entity of the Livescan Entity's fingerprint submissions upon request.
    h. Provide for printing of, or electronic archiving of, the original transaction that supports an entry to the state's systems in accordance with established retention schedules.
    i. Provide for submission of the non-criminal justice fingerprints to the FBI in accordance with the standards, specifications, and authority established by the FBI and the Central Repository.
    j. Receive, review, and approve when appropriate all proposals and requests to add Livescan equipment to the network.
    k. Provide updated technical specifications of the Central Repository, Western Identification Network and FBI and any changes herein no less than 180 days prior to implementation of system changes.
    l. Order and maintain VPN connections to enable Livescan Entities to submit fingerprint scans to and from the Central Repository. Connection interruptions may be subject to planned and emergency maintenance.
    m. Have the authority to audit the Livescan Entity and discontinue interface services pursuant to the rules, policies, regulations and law and direction of the Central Repository Division Administrator or his/her designee.
    n. Authorize the Livescan Coordinators to:
        i. Receive, review, and approve all applications for the Livescan connection.
        ii. Establish policies and training requirements associated with personnel of the Livescan Entity.
        iii. Receive and review reports from the Central Repository, agencies, and entities regarding unresolved Livescan issues.

iv. Direct the process to recommend immediate suspension of Livescan Entity services and connections to the Central Repository through the Division Administrator or his/her designee when any rule, policy or procedure, or any law of the State of Nevada or federal government applicable to the security and privacy of information is violated.
v. Direct the process to reinstate Livescan Entity services and connections upon receipt of satisfactory assurance that such violations were corrected, and steps were taken to prevent any reoccurrence.

o. Reserve the right to change fingerprint processing fees within the billing schedule upon 30 days' notice to the Livescan Entity.
p. Assign the Livescan Entity an Agency Code and account number.
q. Generate an invoice monthly for the fingerprint processing fees due from the Livescan Entity.
r. Reserve the right to suspend services with 30 days' notice if the Livescan Entity is delinquent in payment.

2. The Livescan Entity will:
   a. Adhere to policies, standards and procedures established for electronic submission of non-criminal justice fingerprints to the Central Repository.
   b. Resolve quality control problems identified and reported by the Central Repository.
   c. Maintain a list of authorized personnel who are authorized to gain login access to the Livescan device for the purpose of the Central Repository audit.
   d. Ensure all authorized Livescan operators are trained on how to properly use the Livescan equipment and resolving Livescan errors.
   e. Be responsible for the maintenance of the Livescan device and performance of quality control in a manner consistent with requirements for submission of high-quality fingerprint images at all times.
   f. Designate a coordinator and provide the contact information for the primary contact to the Central Repository regarding all issues associated with this agreement within 10 business days.
   g. Provide the Central Repository with all required information in the Livescan Connection Packet, including current operating systems of the Livescan.
   h. Be responsible for ensuring all Livescan devices are updated with vendor supported operating systems.
   i. Ensure Livescan devices are updated according to updated technical specifications received from the Central Repository, no longer than 180 days from date of receipt of specifications. Livescan Entity is responsible for all vendor costs associated to specification updates.
   j. Be responsible for all costs associated with establishing necessary network connections on behalf of the Livescan Entity, to include procuring the

necessary services, if appropriate, with a private information technology firm to establish connection protocols on behalf of the Livescan Entity.

k. Collect and remit all fingerprint processing fees from the Applicant or applicant employer, except for agencies as identified by the Central Repository. Livescan Entity will submit payment directly to the Central Repository, made payable to "DPS RCCD" via business check, money order or electronic payment within 10 days of DPS RCCD invoice date. Upon 60 days of no receipt the account will be suspended.
l. Have financial responsibility to pay for all fingerprint transactions that are billable to the Livescan Entity, including errors resulting in duplicate transmissions to the Central Repository or fingerprints processed with incorrect fingerprint codes. This excludes transactions sent from defined governmental agencies that the Central Repository will directly bill.
m. Ensure all personnel who will access and/or login to the Livescan device is subject to a fingerprint-based background check pursuant to Livescan Policies and NRS 239B.010(1)(b). Personnel who do not meet the access requirements as contained in the Livescan Administrative Policy shall not be left unattended at the Livescan device.
n. Pay for associated background checks pursuant to section 2(m) of this Scope of Work for authorized personnel.
o. Livescan Entity agrees to accept full financial responsibility for any harm caused to the State's and/or Central Repository IT infrastructure due to the negligence or willful actions or omissions of the Livescan Entity or any Livescan Entity affiliate including its employees, subcontractors, and independent contractors.

3. The Livescan Entity and Central Repository will:
   a. Agree the release of collected demographic and biometric data is prohibited to unauthorized individuals, unless requested by the Central Repository.

Nevada Department of Public Safety
Records, Communications and Compliance

Records, Communications and Compliance Division
333 West Nye Lane, Suite 100
Carson City, Nevada 89706
Telephone (775) 684-6277~ Fax (775) 687-3282
https://rccd.nv.gov/

TERMS AND CONDITIONS
FOR PRIVATE LIVESCAN SERVICE PROVIDER IN NEVADA

SCOPE: This document establishes the minimum controls deemed necessary by the Nevada Department of Public Safety (DPS) to adequately protect the security and stability of the Livescan system and privacy rights of individual applicants. The Livescan Entity may impose any additional, more stringent controls it deems necessary and/or appropriate.

The terms and conditions listed in this document shall apply to all personnel, equipment, software, networks, communication links and facilities supporting and/or acting on behalf of the Livescan Entity.

Approval to establish and maintain connectivity to the DPS network, shall be contingent upon full compliance with all requirements set forth in this document. Failure or refusal to fully comply with all requirements herein may result in a temporary or permanent termination of connection to the DPS network.

REPORTING OF VIOLATIONS: All entity and individual violations shall be promptly reported to DPS. The written notice shall include, but not be limited to, the following information:

- The nature of the violation
- The entity, operator or administrator who is responsible for the violation
- The place, time, and date or date range of the violation

NOTIFICATION OF ON-SITE SECURITY INSPECTION: Entities will be notified of on-site security inspection upon review of application data or notification of change to the livescan system configuration. An inspection of the physical and technical security requirements will be conducted during the scheduled visit. It is required that the entity's technical support representative be available during this inspection.

LIVESCAN ENTITY REQUIREMENTS

1) Entities with existing or proposed environments that include a livescan system must meet or exceed the security recommendations as outlined by this document.

2) Livescan Entity shall be responsible for the actions of any person or entity acting on its behalf and/or providing services in support of it.

3) Livescan site and related infrastructures must always have adequate physical security to reasonably protect against theft, damage, and/or unauthorized access or use by any person.

4) All equipment used for transmitting electronic applicant fingerprint data to DPS shall be segregated and screened against unauthorized use. Data integrity must be maintained in order to detect the unauthorized creation, alteration, or deletion of applicant data or images.

Entity:

_____ _____
Initial *Date*

5) Livescan system shall not be used for general purposes. A dedicated system shall be utilized for transmitting electronic applicant fingerprints to DPS. The Livescan Entity shall not use the system to run any other business application(s), unless explicitly authorized by a DPS Information Security Officer (ISO).

6) Applicant fingerprint data shall remain encrypted while data is at rest on mobile computing devices and removable storage media, or while data is in transit outside the Livescan firewall. Encryption shall be secured using a Federal Information Processing Standard (FIPS) 140-2 compliant encryption solution.

7) Any network connection authorized by DPS, which allows unencrypted applicant fingerprint data to be transmitted from the Livescan Entity, shall be secured by a firewall from both inside and outside of the network.

8) Any network connection authorized by DPS, which supports remote administration of the Livescan Entity, shall be secured by a firewall from both inside and outside of the network. This includes wireless networks used for remote administration via WAN, LAN, or Internet.

9) No device shall be permitted inside the Livescan firewall unless explicitly authorized by a DPS Information Security Officer (ISO). A dedicated printer used solely for Livescan printing and does not possess multifunction capabilities (i.e. fax, wireless, etc.) may be permitted inside the firewall without prior authorization.

10) Administrative account passwords shall not be left blank or on default and must be set to a minimum of 8 characters with complex attributes. Complex attributes for a password require a combination of numbers, upper case, lower case, and special characters.

11) Wireless form of communication is optional and may be used as part of the Livescan network but must be placed outside the designated firewall. Wireless technology shall use strong encryption and be equipped with the minimum characteristics.

- For 802.11 Communication: Must use Wi-Fi Protected Access version 2 (WPA2) with Advanced Encryption Standard (AES). Wired Equivalent Privacy (WEP) is not an authorized encryption protocol.
- For Cellular Broadband Communication: Must use a virtual private network (VPN).
- Bluetooth technology is **not** authorized.

Passwords used to establish wireless communication must have a minimum of 8 characters with complex attributes unique to any administrative account password.

12) Livescan operators are required to use only account credentials for which they have been authorized. An attempt to log into an account other than those for which an operator has been authorized is prohibited.

13) Dual (split) tunneling in any form of communication is strictly prohibited. The term split tunneling is also used to describe a multi-branch networking path.

14) Network documentation shall remain updated. The Livescan Entity must notify DPS on proposed modification to the network topology. An on-site security inspection may be required.

Entity:

_____ _____

Initial *Date*

15) Every person who, in the course of their normal duties, collect, process, facilitate, or support the transmission of applicant fingerprints to DPS, or who manage, administer, access, develop, or maintain the systems supporting the Livescan Entity, shall complete a state and national fingerprint-based record check.

VERIFICATION OF LIVESCAN VENDOR REQUIREMENTS: Livescan Entity will complete the following checklist to verify completeness of DPS requirements. DPS shall review any applicable items that are not marked to determine if the proposal sufficiently meets the basic requirements. DPS may request clarification(s) or correction(s) and if necessary, may deem the Livescan Entity as non-responsive and reject the proposal.

Authorized Recipient:

BASIC TECHNICAL REQUIREMENTS	**Check all that apply**
1) Operating system has current support commitment by the manufacturer.	☐
2) Operating system can receive distributed operating system updates, patches, and hotfixes.	☐
3) Operating system is protected by comprehensive anti-virus program at all times.	☐
4) Unnecessary operating system services or applications have been disabled.	☐
5) Livescan system is enforcing unique user authentication.	☐
6) Livescan system is enforcing complex password with a minimum of 8 characters.	☐
7) Operating system is enforcing password protected screensaver within a 1 to 15 minute lockout timeframe.	☐
8) Firewall is performing Stateful Packet Inspection (SPI) and is configured to explicitly allow only permissible protocols and traffic inherent in the Livescan network environment.	☐

Livescan Entity Name: _____

Address: _____

_____

Entity Representative: _____
PLEASE PRINT Last Name First Name Middle

Entity Representative Signature: _____

Date: _____

Attachment DD

Nevada Department of Public Safety
Records, Communications and Compliance

Records, Communications and Compliance Division
333 West Nye Lane, Suite 100
Carson City, Nevada 89706
Telephone (775) 684-6277 – Fax (775) 687-3282
www.rccd.nv.gov

Livescan Connection Request Form

*(Note: Request form must be completed for **each** livescan device connection)*

Forms must be completed in their entirety.
Incomplete forms will result in the request for livescan connection being rejected.

Livescan Entity Information

Entity Legal Name: _____

Nature of Business: _____

Type of Business: ☐**Law Enforcement** ☐**State Agency** ☐**Local Agency** ☐**Other***
(Please check only one box)

ADDITIONAL INFORMATION REQUIRED:
If Other is selected, describe the purpose for which you will be submitting fingerprints to the Records Communications and Compliance Division. _____

Website Address: ☐**N/A** _____

Physical Address: _____
City, State, Zip _____

Mailing Address: _____
City, State, Zip _____
☐**Same as Physical Add.**

Main Point of Contact:

Name: _____
Title: _____
Telephone #: _____
Fax #: _____
Email: _____

IT Point of Contact:
☐**Same as Main Point of Contact**

Name: _____
Title: _____
Telephone #: _____
Fax #: _____
Email: _____

Nevada Department of Public Safety Livescan Coordinator(s):
Nicole Davis | ☎ (775) 684-6227 | ✉ ndavis@dps.state.nv.us
Maria Uribe | ☎775-684-6231 | ✉ maria.uribe@dps.state.nv.us

Livescan Entity Information *(continued)*

Additional Point of Contact: ☐ **N/A**

Name: _____

Title: _____

Telephone #: _____

Fax #: _____

Email: _____

Livescan Vendor Information *(to be completed by the livescan Vendor ONLY)*

Company Name: _____

Website Address: _____

Point of Contact:

Name: _____

Title: _____

Telephone #: _____

Email: _____

Device Type: _____

Device Model #: _____

Is the device referenced above a portable or stationary livescan system? ☐ **Portable** ☐ **Stationary**

Device Operating System
(i.e.: Windows10 etc.): _____

Are BOTH the livescan device and software certified by the Federal Bureau of Investigation (FBI) as listed and outlined on *https://fbibiospecs.fbi.gov/certifications-1/cpl* ? ☐ **Yes** ☐ **No**

Is the Hardware and Software already in use in Nevada? ☐ **Yes** ☐ **No**

If yes, provide a list of each using entity: _____

_____

_____

_____

_____

Livescan Installation Information

What is the IP Address for the livescan device connection? _____

Is the livescan device going to be used to collect criminal fingerprints? ☐ **Yes** ☐ **No**

Is the livescan device going to be used to collect applicant fingerprints? ☐ **Yes** ☐ **No**

Will the livescan device interface with a Records or Case Management System? ☐ **Yes** ☐ **No**

If yes, please list the Management System vendor's name: _____

Make of the local entity firewall: _____

Model of the local entity firewall: _____

Nevada Department of Public Safety Livescan Coordinator(s):
Nicole Davis | ☎ (775) 684-6227 | ✉ ndavis@dps.state.nv.us
Maria Uribe | ☎775-684-6231 | ✉ maria.uribe@dps.state.nv.us

Is the firewall already implemented and in use? ☐Yes ☐No

Proposed Schedule

Anticipated date livescan device, including firewall/VPN and internet connection will be installed: _____

Anticipated date for livescan system testing: _____

Anticipated date the entity would like the livescan device to go into production ("go-live")": _____

_____ _____

Signature – Livescan Entity Project Manager *Date*

_____ _____

Name Printed - Livescan Entity Project Manager *Title*

_____ _____

Signature – Livescan Entity Administrator/Executive *Date*

_____ _____

Name Printed - Livescan Entity Administrator/Executive *Title*

Nevada Department of Public Safety Livescan Coordinator(s):
Nicole Davis | ☎ (775) 684-6227 | ✉ ndavis@dps.state.nv.us
Maria Uribe | ☎775-684-6231 | ✉ maria.uribe@dps.state.nv.us

Attachment EE

Nevada Department of Public Safety
Records, Communications and Compliance

Records, Communications and Compliance Division
333 West Nye Lane, Suite 100
Carson City, Nevada 89706
Telephone (775) 684-6277 ~ Fax (775) 687-3282
https://rccd.nv.gov/

Physical and Technical Security Requirements for Nevada Livescan Installations

The following are hardware and service requirements required for establishing a connection to the Nevada Department of Public Safety (DPS) for the purposes of submitting fingerprints electronically.

For Entities that Connect Directly to Nevada ONLY

- Entities connected to or through SilverNet (state government and criminal justice agencies only) should supply their EITS routable address (10.0.0.1 – 10.255.255.254).
- Entities using an Internet connection need to supply a static IP address that is routable on the Internet. Of the IP address range from 0.0.0.0 to 223.255.255.255, the following address ranges are NOT routable on the Internet:
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
  - ➢ The State of Nevada will then assign and provide the internal subnet IP address that will be used for each livescan connection.
- A firewall capable of creating an IPSEC VPN tunnel that also meets Federal Information Processing Standards (FIPS) 140-2 for the encryption engine. DPS strongly recommends using the Cisco ASA series. Using this product will enhance the ability for "canned" configurations. If you want to see if your device meets the FOPS 140-2 standard, check the list at:
  http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

  At this site, the products are listed by date of approval and not by manufacturer or model so you may need to hunt around for your specific product. If you find another product, there should be text that says "Validated to FIPS 140-2". If your product is not in the list or the entry for your product lacks this endorsement, you may not use that product to connect to Nevada DPS.
  - All livescan equipment to include printers, need to be "inside" or "behind" a firewall that protects them from the rest of the Entity network.
  - The firewall must establish a LAN-to-LAN IPSEC VPN tunnel with DPS. The tunnel shall not be shared with any other network traffic. An exception to this requirement is terminals used exclusively for JLink access.
  - The encryption for the VPN tunnel shall have been demonstrated to meet FIPS 140-2 encryption standards.
  - The firewall shall not have any inbound exceptions other than those used for internally managing the livescan, if any.

Physical Security for ALL Livescan Entities

- The livescan should be in a physically secure area.
- All entry points to the secure area should be marked with signs or placards that say "Restricted Area – Authorized Personnel Only" or similar language.
- A physically secure area that is accessible only by those who are authorized to use the device, plus those who have passed fingerprint-based background investigations. All others must be continuously escorted while in the livescan area. This includes custodians and maintenance workers of all kinds.
- A physically secure area is one in which unauthorized access cannot be gained by the use of ordinary tools and access would show obvious signs of damage. Some common items to check are:
  - Access doors should have their hinges inside the secure space.
  - Check for possible access through "drop" ceilings.
  - Mitigating measures typically consist of motion detectors connected to burglar alarms and/or video surveillance connected to a DVR.
- **If you are planning to use a mobile livescan unit**, and/or you are thinking of connecting your livescan wirelessly, or your livescan unit might possibly be stored in a non-secure location, please call DPS first so we can discuss the requirements with you before you purchase your livescan unit.

Nevada Specification Requirements

All livescans must be configured to the current Nevada Specifications prior to connection and be able to transmit SMTP. Your livescan must also have the ability to retrieve messages using a POP3 account. You and/or your vendor may obtain these specifications from one of the Livescan Coordinators listed on the livescan Connection Cover Letter.

Site Security Inspection

Before DPS will allow your site to connect to the DPS network, the Information Security Officer (ISO) or the ISO's designee may evaluate the security assessment in lieu of performing a physical site security inspection or as otherwise prescribed by the Division.

To be ready for an on- site security check by DPS staff:

- All physical security measures must be in place
- Your connection to SilverNet, DPS, or Internet service, as applicable, must be in place.
- All the network components for your local network up to and including the firewall that provides separation between livescan devices and the general purpose network must be in place, including all configuration.
- The livescan and/or printers do NOT need to installed or on-site for a security check for new installations.

Security Notes

- No wireless access may be installed inside the livescan firewall.
- Any hard drive or non-volatile memory must be sanitized before the livescan can be stored in a non-secured location or transported by a person who is not authorized to access the livescan unit.
- The firewall should restrict outbound access to just the VPN tunnel, along with whatever is required to automate management of the livescan unit, whenever possible.

Turning Up Service
All activities, the administrative provisioning for livescan system settings, site security checks, establishing connectivity, and turning service on or off, are all initiated with a call to the DPS Fingerprint Examiner Unit. The primary contact is Nicole Davis (775) 684-6227. The Fingerprint Examiner Unit will coordinate all of the activities with all necessary stakeholders and will be a central point of contact for you.

All security issues discovered during the site security inspection must be addressed before submitting fingerprints electronically.

Compliance Auditing
Your site may be checked at any time to ensure compliance with current policies affecting livescan use, and we use the opportunity to provide education about any changes in policy. If any security issues are brought up during these visits, please act and respond promptly. This will keep you securely connected for fingerprint submission.

Thanks!

Nevada Department of Public Safety
Records, Communications and Compliance

Records, Communications and Compliance Division
333 West Nye Lane, Suite 100
Carson City, Nevada 89706
Telephone (775) 684-6277 – Fax (775) 687-3282
www.rccd.nv.gov

FOR OFFICIAL USE ONLY

Livescan Security Questionnaire

Forms must be completed in their entirety.
Incomplete forms will result in the request for livescan connection being rejected.

Entity Information

Entity Name: _____

Physical Address: _____
City, State, Zip _____

Mailing Address: _____
City, State, Zip _____
☐ **Same as Physical Add.**

Main Point of Contact:

Name: _____

Title: _____

Telephone #: _____

Fax #: _____

Email: _____

IT Point of Contact: ☐ ***Same as Main Point of Contact***

Name: _____

Title: _____

Company Name: _____

Telephone #: _____

Fax #: _____

Email: _____

Additional Point of Contact:

Name: _____

Title: _____

Company Name: _____

Telephone #: _____

Email: _____

Signature:

Main Point of Contact Signature: _____

Name Printed: _____

Date: _____

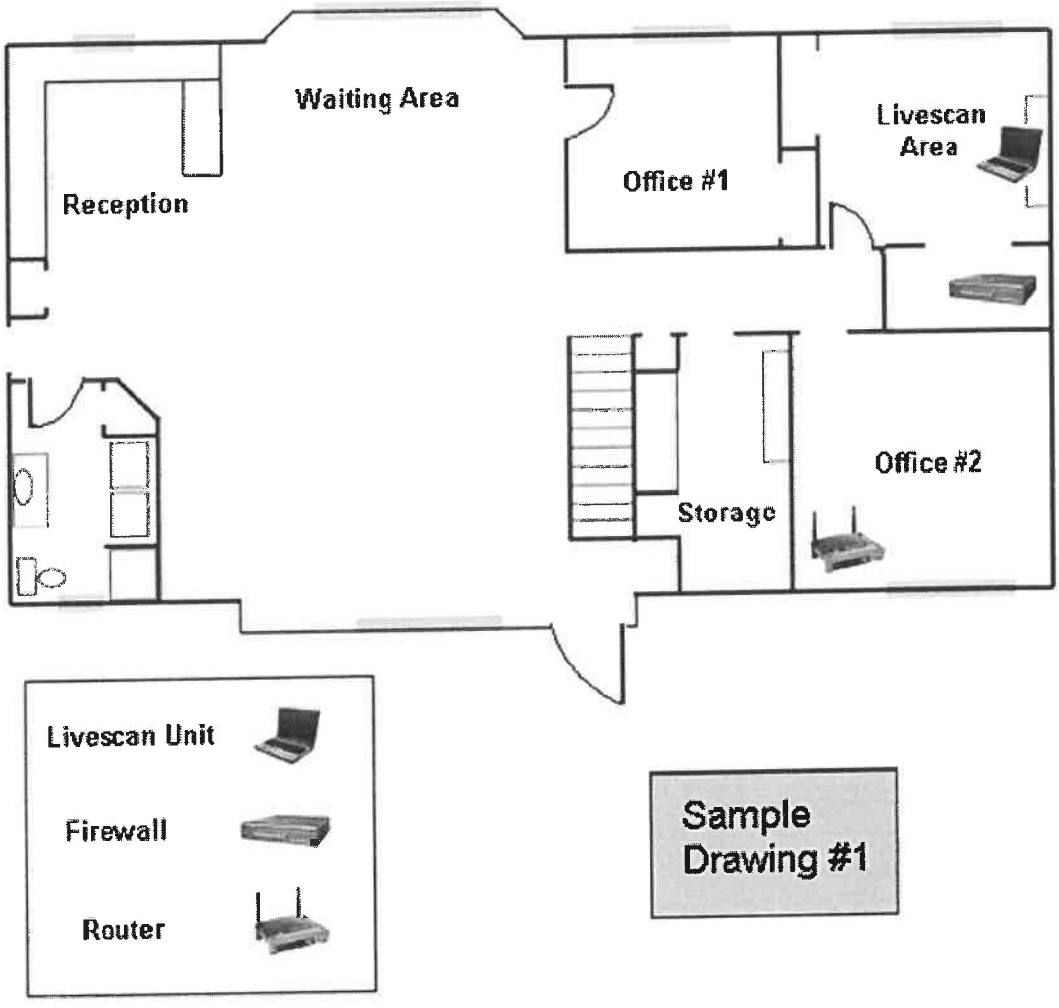
FOR OFFICIAL USE ONLY

1.1	Is the Livescan unit in a physically secure location such that only authorized personnel who have passed fingerprint-based background check may have unescorted access to the area?	☐Yes ☐No
1.2	Is the networking equipment (including the firewall) to the Livescan unit in a physically secured location such that only authorized personnel who have passed fingerprint-based background check may have unescorted access to the area?	☐Yes ☐No
1.3	Does the Livescan Entity share wiring/networking closets with other businesses within the building?	☐Yes ☐No

Please submit the following two (2) drawings

2.1 Drawing #1 – **Building layout**

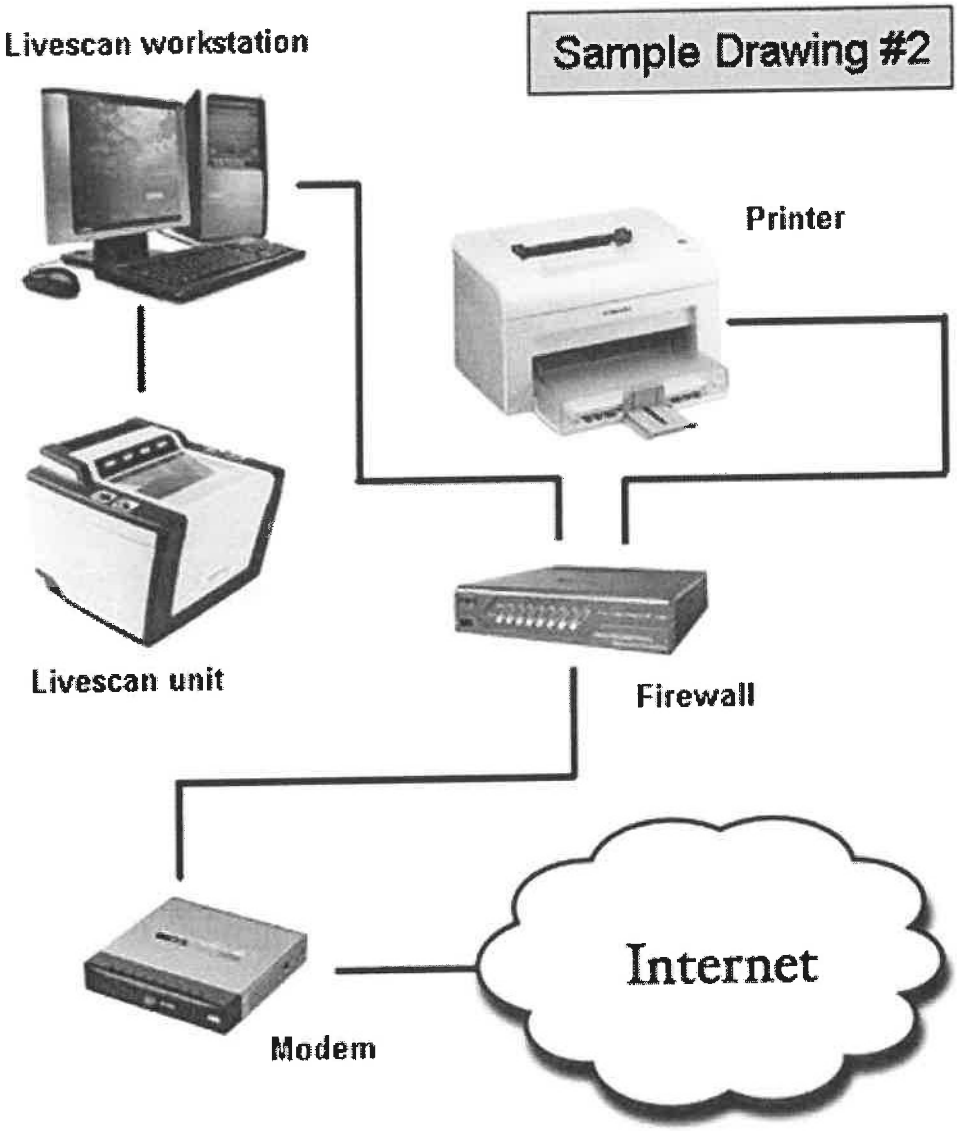
1) Please provide a diagram that illustrates the floor plan of your Livescan area. Include the security measures in place to create a physically secure area (e.g. doors, locks, surveillance cameras, etc.)
Note: Handwritten drawing are acceptable.



EXAMPLE continued:

2.2 Drawing #2 – **Networking**

1) Please provide a diagram that depicts the networking components (including peripherals) used for the Livescan system. Include all devices installed behind the designated Livescan firewall.
Note: Handwritten drawing are acceptable.



Note: *Show the entire network configuration depicting the inter-connectivity of all communication paths (e.g. firewalls, routers, switches, hubs, etc.) Please label each networking device accordingly.*

3.1	How are the systems within the Entity's Livescan network **remotely** maintained or accessed? **(Check)** ☐ Telnet ☐ SSH ☐ RDP ☐ Dameware ☐ VNC ☐ PC Anywhere ☐ None ☐ Other _____

4.1	**Who** maintains the network and firewall? Name: _____ Title: _____ Company: _____

5.1	Provide a description of the **anti-virus software** used to protect the Livescan system. Anti-virus vendor name: _____ Version #: _____

6.1	Provide a description of the **firewall** used to protect the Livescan system. _____ Software: _____ Hardware: _____ Manufacturer: _____ Model: _____ Firmware Version: _____ **For Software-based Firewall Only** ☐ NIST Common Criteria ☐ ICSA Labs Certified ☐ Checkmark Certified ☐ Not Certified

6.2	Please indicate the location of the virtual private network (VPN) termination? ☐ On the firewall/router: Site-to-site tunneling configuration ☐ On the Livescan workstation(s): Client-to-site tunneling configuration

STOP!

If you have a Mobile/portable device(s) you must complete the following page.

For mobile/portable devices only ☐N/A

7.1	Please provide **description** of environment used to secure the mobile Livescan device when not in use.

7.2	How is the portable Livescan device secured while conducting **field work** (e.g. during meal breaks, within travel, in-between appointments, etc.)? Please explain.

8.1 Provide a description of the **wireless router/broadband adapter** used:

Manufacturer: _____

Model: _____

Firmware Version: _____

Type of Wireless Technology Used

☐802.11 (WiFi)

☐Wireless broadband

8.2 Provide a description of the **software firewall** used to protect mobile/portable Livescan terminal.

Manufacturer: _____

Version: _____

Software Firewall Certification

☐NIST Common Criteria

☐ICSA Labs Certified

☐Checkmark Certified

☐Not Certified

8.3 Please indicate each communication interface(s) capable of transmitting data? **(Check all that apply)**

☐Ethernet ☐Wireless 802.11 ☐Wireless Broadband Adapter

☐Bluetooth ☐Dial-up/POTS ☐Infared

☐Other _____

8.4 Please indicate the communication interface(s) that have been disabled. **(Check all that apply)**

☐Ethernet ☐Wireless 802.11 ☐Wireless Broadband Adapter

☐Bluetooth ☐Dial-up/POTS ☐Infared