DHR Electronic Criminal History Check System

PURPOSE

Continuation of the Alabama Department of Human Resources (hereinafter "DHR") electronic criminal history background check system that captures and processes prints, reviews responses, and issues suitability determination letters for DHR licensed/exempt child and adult care licensees/applicants/employees/volunteers, and others. Ala. Code § 38-13-1 et. seq. DHR anticipates an estimated 20,000 livescan/cardscan fingerprints will be obtained statewide on an annual basis, but does not guarantee a minimum number of fingerprints to be processed in regard to this Invitation to Bid ("ITB"). DHR desires to continue and possibly expand a system where a central office DHR site and county DHR office sites will scan in print cards and live scan prints and transmit those prints on private vendor equipment that is able to assure transmission quality by secured internet transmission to a FBI certified private vendor (channeling agent) that transmits to the Alabama Bureau of Investigation/Federal Bureau of Investigation (hereinafter "ABI/FBI") that sends the results back to the private vendor that manipulates the data so results and applicable documentation are sent to appropriate DHR sites where suitability determinations are generated.

ITB SPECIFICATIONS

LINES 0001-0003

Vendor shall provide the livescan/cardscan transaction collection service for DHR related (DHR Fee Paid and Non-DHR Fee Paid (i.e., DHR-provider paid transaction) fingerprint capture transmissions for 31 sites in the following counties: 1. Jefferson / 2. Mobile / 3. Madison / 4. Montgomery/ 5. Tuscaloosa / 6. Lee / 7. Calhoun / 8. Houston / 9. Baldwin / 10. Shelby / 11. Talladega / 12. DeKalb / 13. Chambers / 14. Chilton / 15. Clarke / 16. Cleburne / 17. Colbert / 18. Crenshaw / 19. Cullman / 20. Dallas / 21. Elmore / 22. Etowah / 23. Jackson / 24. Limestone / 25. Marshall / 26. Morgan / 27. Russell / 28. / St. Clair / 29. Tallapoosa / 30. Walker and / 31. DHR Central Office-Montgomery. Transmissions shall be forwarded to the ABI/FBI by an FBI-certified channeling agent (i.e., vendor) that records said transmissions, receives responses from ABI/FBI, including responses regarding subsequent convictions, processes responses, reports and transmits all responses via a secure website interface to DHR-designated sites, providing the capacity for DHR users to process and print applications, criminal history record information ("CHRI"), suitability and other applicable letters and envelopes that meet DHR specifications. ***See Attachment #1 (Alabama Department of Human Resources' Electronic Channeling Process for DHR Fee Paid Applicants Chart-1 page) and Attachment #2 (Alabama Department of Human Resources' Non DHR Fee Paid Applicant Chart-1 page); see also Attachment #3 (FBI Appendix F-9 pages) and Attachment #4 (Channeling Agent Regulations and Specifications including FBI Appendix C Configuration Drawings-8 pages).***

DHR's current livescan/cardscan transaction collection service provides electronic criminal history checks for DHR Fee Paid and Non-DHR Fee Paid applicants for licensed/exempt child and adult care licensees/applicants/employees/volunteers, and others. As indicated by the attached charts, the process for DHR Fee Paid applicants requires the completion of the application and fingerprinting at a DHR local office livescan site or fingerprint cards inked at a local law enforcement office and forwarded to the Central DHR Office. DHR Office personnel in either office enter the applicant's information into a vendor-created software program and electronically transmit the fingerprint information to the vendor. The vendor forwards the fingerprint information to the ABI. The ABI forwards the fingerprint information to FBI and subsequently returns the results to the vendor. The vendor, via its secure website, makes the CHRI results available to DHR for viewing and printing. DHR makes the suitability determination within the vendor-created program, which generates envelopes and applicable letters, including, but not limited to, suitability, investigation, and prosecutorial referral letters and attachments for printing and distribution to the applicant and the agency, as appropriate.

The process for Non-DHR Fee Paid applicants requires online pre-registration with the vendor, and printing and completing the application. A Non-DHR Fee Paid applicant may also obtain a copy of the application from the vendor's website without pre-registration or a copy of the application from DHR. Thereafter, Non-DHR Fee Paid applicants forward the completed application packet (including fingerprint cards inked at a local law enforcement office, a chain of custody form, and payment) directly to the vendor for processing. After the vendor verifies that the application packet is complete, including a signed application, the fingerprint information is essentially the same manner described above, with the exception of the vendor being responsible for addressing application deficiencies and providing a copy of the signed application to DHR.

At a minimum, the vendor is responsible for providing DHR and the Alabama Department of Public Safety (ABI) with monthly accounting reports with specific demographic information for reconciliation and invoice payment as outlined herein. Additionally, the vendor is responsible for providing DHR with monthly data importation of demographic data so that an internal registry can be maintained as specified below or otherwise specified by DHR.

DHR has previously purchased equipment and software that meets the specifications described within this ITB for each of the aforementioned 31 sites. Vendor must be certified by i3 to access, service, and maintain the equipment and software previously purchased by DHR to continue the current livescan/cardscan transaction collection service for each of the aforementioned sites without causing delay of transmissions or the issuance of suitability letters. Transition of current operations is the successful bidder's sole responsibility. The 31 livescan/cardscan workstations are comprised of the following:

A. Fingerprint Scanner: i3 DigiID Mini dual mode 500 dpi (Livescan Workstations only)

- Image quality complies with FBI specification EFTS Appendix F
- FBI certified for both civil ID flats and full criminal ten-print rolls and flats
- Sealed PC/ABS polymers case
- Single piece prism and imager with uniform capture
- 500 dpi resolution
- Lightsource – proprietary low energy green light source
- Power (max) 1.9w, current - 500mA(via USB connection)
- Operating voltage – 5.0 VDC
- RoHS compliant
- Operating temperature range, 14 degrees F to 120 degrees F
- Factory calibrated and sealed, with automatic self test/diagnostics at startup
- FCC, UL and CE certified
- Strain relief IP 68 rated connection for capture USB cable

B. Flatbed Card Scanner, Epson Perfection 4490 Photo

- Scanner Type-Flatbed color image scanner with Digital ICE ™ Technology for Film
- Photoelectric Device-Color Epson MatrixCCD™ line sensor
- Hardware Resolution-4800 x 9600 dpi with Micro Step Drive™ technology
- Maximum Resolution-12,800 x 12,800 dpi with software interpolation
- Effective Pixels-40,800 x 56,160 (4800 dpi)
- Color Hardware Bit Depth-48-bits per pixel internal, 48–bits per pixel external
- Grayscale Hardware Bit Depth-16-bits per pixel internal, 16–bits per pixel external
- Optical Density-3.4 Dmax
- Transparency Unit-2.7" x 9.3" Transparency Adapter built-in lid, 12 35mm negative, 4 35mm slide, 1 2-1/4", 6 x 12cm or 120/220mm capacity
- Buttons-4 buttons; Scan, Copy, E-mail, PDF
- Maximum Read Area 8.5" x 11.7" (21.6cm x 29.7cm)
- Light source-white cold cathode fluorescent lamp
- Interface-Hi-Speed USB 2.0
- Scanning Speed-4800 dpi high-speed mode: Monochrome 16.96 msec/line; Full color 16.96 msec/line

C. Computer Dell 360 Mini Tower Desktop

- **Intel Core2 Duo processor with 2.0 GHz 2 GB RAM**
- **80 GB Hard Drive**
- **USB 2.0 interface**
- **Windows XP operation system**

D. XPOS Keyboard, Mouse, and 17" Flat panel Monitor

E. Uninterruptible Power Supply Tripplite, 900VA/465w Rack/Tower, 120v

F. InVize ID Application Software

- Certified WSQ compression
- FBI Appendix F certified
- EFTS 7.0
- DigID L and card scanning supported

In addition to the foregoing requirements, the successful bidder shall operate a livescan/cardscan transaction collection service that adheres of the following:

1. Vendor shall create, control and maintain a system for livescan/cardscan transaction collection service for all DHR-related electronic criminal history checks transmissions for the aforementioned sites and other sites, as designated by DHR. Vendor's system shall facilitate DHR user's ability to electronically process applications by DHR Fee Paid and Non-DHR Fee Paid Applicants, including, but not limited to, the generation and printing of suitability inquiries, determinations, and notices. The system shall also facilitate the DHR user's ability to input, search, and import data, as specified.
2. The vendor-created, controlled and maintained system shall channel EFTS transactions from the i3 live scan and card scan systems and transmit data to the ABI in a secure fashion. Results will be provided by ABI via SMTP and shall be retrieved by the vendor over a VPN. The vendor shall post the results to a secure website for retrieval by ABI and DHR-authorized agents.
3. All vendor-created, controlled and maintained system shall carry ABI/FBI data over them and operate according to the 2010 CJIS Security recommendations. All transmissions and management of CHRI shall be in compliance with FBI CJIS Security Policy Version 4.4 dated July 2007 including any requirements that are scheduled to go into effect on September 30, 2010. Compliance with the aforementioned requirements is the responsibility of the vendor.
4. Vendor livescan/cardscan transaction collection service shall comply with "ABI" electronic fingerprint transmission specifications which includes type 1 and 2 records, type 4 fingerprint images, and transaction control number ("TCN") generation, and incorporates FBI and ANSI/NIST specifications. ANSI/NIST-ITL 1-2000 Data format for the interchange of fingerprint, facial, scar mark and tattoo (SMT) information. IAFIS-IC-0010 (V3). IAFIS Wavelet scalar quantization (WSQ) grayscale fingerprint image compression specification (December 1997). All vendor-supplied equipment shall be FBI-certified according to current or updated specifications.
5. Vendor shall provide DHR users and administrators of the transaction collection service with a toll-free telephone number to call and receive assistance on issues involving any aspect of the system(including, but not limited to, collection equipment, software, CHRI channeling, and the Results webpage). Vendor shall provide Non-DHR Fee Paid applicants with a toll-free telephone number to call and receive assistance in completing the application packet and forwarding the

same to vendor only. At a minimum, toll-free telephone support must be provided Monday through Friday, 8:00 a.m. to 5:00 p.m., CST.

6. The vendor, via the vendor-created, controlled and maintained system shall archive all fingerprint images and demographic data transmitted or forwarded to vendor in response to this ITB. Said fingerprint images and demographic data shall remain the sole property of DHR. The vendor shall convert all existing fingerprint images and demographic data into a format specified and approved by DHR and submit said information to DHR or an entity specified by DHR at the expiration or termination of the contract. The vendor shall convert all demographic data into a format specified and approved by DHR and facilitate electronic data importation of the same to DHR so that an internal registry can be maintained pursuant to statutory requirements. Unless otherwise specified by DHR, vendor shall provide said electronic data importation to DHR on a monthly basis.
7. The vendor created and maintained web site shall be customized for DHR to include a graphic banner, the Non-DHR Fee Paid Criminal History Application(DHR-CHC-2177), and text relating/linking the website to the DHR website, which will contain the DHR Fee Paid Criminal History Application (DHR-CHC-2177) as well as provide the ability to complete, view and print the Non-DHR Fee Paid Application by Non-DHR Fee Paid Applicants and DHR users, as applicable. ***See Attachment #5 (Alabama Department of Human Resources' DHR Fee Paid Application-2 pages) and Attachment #6 (Alabama Department of Human Resources' Non-DHR Fee Paid Application-2 pages).***
8. The vendor, via the vendor-created, controlled and maintained system shall display on its website a data-entry screen for DHR user-input information from DHR Fee Paid Applications and for Non-DHR Fee Paid applicants for Non-DHR Fee Paid Applications. Access to the said information shall be protected by user name and password log-in. Fingerprint and demographic information transmitted electronically shall be transmitted via an encrypted virtual private network (VPN) and shall conform to DHR Security Policy for LAN-to-LAN VPN policy. ***See Policy Section 640-01, Interconnecting IT Systems located at http://www.isd.alabama.gov/POLICY/policies.aspx.*** Vendor, via the vendor-created, controlled and maintained website shall notify sender within 12 business hours of transmission difficulties or errors, including bad prints.
9. Vendor shall receive all Non-DHR Fee Paid Application packets directly from applicants. Non-DHR Fee Paid Application packets consist of the Non-DHR Fee Paid Application, fingerprint cards, the chain of custody form, and payment. Vendor created and maintained website must include a fillable PDF version of the Non-DHR Fee Paid Application so that the applicant may enter his/her demographic information directly into the system for eventual adjudication by the appropriate DHR user. Vendor shall not provide the Non-DHR Fee Paid applicant the ability to electronically sign the application. The Non-DHR FeePaid applicant must manually sign the application and forward requisite documentation and payment directly to vendor. Vendor will operate provider bank withdrawal software for Non-DHR Fee Paid transactions. The vendor shall maintain an electronic copy of the signed, hard copy of the Non-DHR Fee Paid Applications

submitted by Non-DHR Fee Paid applicants. From the vendor created, controlled and maintained website, vendor shall facilitate the DHR user's ability to print the aforementioned application. Vendor, via the vendor-created, controlled and maintained website shall notify sender within 12 business hours of transmission difficulties or errors. Vendor shall display all channeling results within five (5) business days of submission, unless fingerprinting transmission difficulties or errors have occurred. Vendor shall directly address application packet deficiencies, including, but not limited to, incomplete or unsigned applications, fingerprinting errors or rejections regarding Non-DHR Fee Paid applicants with the applicant, missing documents, or payment. Vendor shall electronically notify DHR of the deficiency only. Forwarding communications to the Non-DHR Fee Paid applicant to correct the deficiency is the sole responsibility of the vendor.

10. Vendor shall receive all Non-DHR Fee Paid Application packets directly from applicants. Non-DHR Fee Paid Application packets consist of the Non-DHR Application, fingerprint cards, the chain of custody form, and payment. If not entered by the applicant, vendor shall enter Non-DHR Fee Paid applicant's demographic information as contained on the application into the vendor-created, controlled, and maintained system for eventual adjudication by the appropriate DHR user. Vendor, via the vendor-created, controlled and maintained website shall notify sender within 12 business hours of transmission difficulties or errors. Vendor shall display all channeling results within five (5) business days of submission, unless fingerprinting transmission difficulties or errors have occurred. Vendor shall directly address application packet deficiencies, including, but not limited to, incomplete or unsigned applications, fingerprinting errors or rejections regarding Non-DHR Fee Paid applicants with the applicant, missing documents, or payment. Vendor shall electronically notify DHR of the deficiency only. Forwarding communications to the Non-DHR Fee Paid applicant to correct the deficiency is the sole responsibility of the vendor.
11. Vendor, via the vendor-created, controlled and maintained system, shall display CHRI or other results received from ABI/FBI to the appropriate DHR users, not applicants, within 12 business hours after receipt from ABI/FBI. Vendor-created, controlled and maintained system, shall display CHRI results, including an applicant's initial and subsequent CHRI results, commonly referred to as "RAPBACKS".
12. Unless otherwise specified by DHR, the vendor-created, controlled and maintained system shall generate letters and envelopes that automatically incorporate applicant names and addresses and employer/agency names and addresses from the EFTS records so that the letters are personalized for the recipient. Vendor-created, controlled, and maintained system shall import via its website a maximum of twenty (20) DHR-provided form letters for 68 locations with user customizable fields as well as standard verbiage to include the following: applicant information; employer/licensing authority addresses; applicant criminal charges; county/state office/district attorney addresses; and signature blocks, including the name, title, and location of the DHR personnel processing the application; the sending county; and the requesting county. DHR Form letters include, but are not limited to Criminal History Suitability: Criminal

History Unsuitability and Unsuitability Determination Information Notice; Record of Arrest-Additional Information Needed; Fingerprint Rejection or Application Incomplete; Updated Criminal History Report; Notice of False or Misleading Information; Report to District Attorney; and Updated Criminal History Suitability for Change of Employer. ***See Attachment #7 (DHR Criminal History Sample Form Letters-8 pages)***

13. From the vendor-created, controlled and maintained website, vendor shall facilitate the DHR user's ability to print envelopes and letters formatted according to DHR specifications, including the aforementioned form letters, print all CHRI results, and print completed and signed Non-DHR Fee Paid Applications forwarded directly to the vendor onto a local printer.
14. From the vendor-created, controlled and maintained website, vendor shall provide a means by which the DHR user may access an applicant's record information after a determination has been made in order to generate a letter changing the suitability determination based upon Central Office Review or Administrative reversal or updating a suitability letter for applicants that have changed employment. Vendor shall facilitate the DHR user's ability to print envelopes and letters formatted according to DHR specifications.
15. Vendor's operating system shall provide a "results webpage" for DHR transactions. The "results webpage" shall display the following information for each applicant: name; social security number; date of birth; case number; TCN; date entered; date sent; case type; status; response from ABI/FBI; agency; region, sending county; and requesting county.
16. The vendor's operating system shall provide a single point archive function on its "results webpage" so that transactions for all applicants may be searched, viewed, and printed at any time. Vendor's "results webpage" shall provide the DHR users the ability to narrow a search by the following criteria: applicant's last name; case number, social security, or TCN. Vendor's "results webpage" shall provide DHR users the ability to narrow a search by the following stages: in process; completed; and error. Vendor's "results webpage" shall provide DHR users the ability to narrow a search by following status: sent; not sent; error; unclassifiable; and need to close. Vendor's "results webpage" shall provide DHR users the ability to narrow a search by region. Vendor's "results webpage" shall provide DHR users the ability to sort results by the following: last name; social security number; date sent to vendor; date sent to ABI; region; agency; case types, sending county; requesting county, worker ID, and disposition. Vendor shall provide DHR users the ability to print results from its "results webpage", as specified.
17. Unless otherwise specified by DHR, vendor will issue detailed monthly billing report(s) to the DHR Central Office for all DHR-paid transactions processed during the preceding month. Billing report must include, but is not limited to, applicant name, sex, race, DOB, partial SSN, date printed, response date, case type, sending county, requesting county, worker ID, and disposition. Unless otherwise specified by DHR, vendor shall issue monthly demographic report(s) to DHR of all DHR-related transactions in the following format(s): Crystal Reports or Business Object reporting tools for ad hoc reporting. Vendor shall provide training for the aforementioned reports.

18. The vendor's operating system shall be able to support up to 40,000 transactions per year with the ability to grow to 100,000 transactions per year for multiple offices.
19. Five levels of security shall exist within the vendor's operating system: super users have ready access to all data and transactions relating to this effort, regional super users have the ability to see all data associated with the transactions under their jurisdiction (filter by system identifier), and end users can see the specific records submitted on their behalf. End users cannot see any of results status. Super users have shall have the ability to retrieve and print any transaction.
20. Unless otherwise specified by DHR, vendor's operating system shall provide the DHR Central Office site with the capacity for statewide review, display, search, print documents and data importation and storage of the information specified in and searchable by the terms referenced in Paragraph Nos. 15 through 17. Local DHR sites shall have the capacity for regional review, display, search, print and storage. DHR Central Office site shall meet all the requirements of the items above and have NIST archive software for electronic storage of 100,000 sets of prints expandable for data importation and storage.

The fee for the aforementioned service(s) shall be included in the bid. All necessary transfer and/or conversion of operations and updates of data shall be the sole responsibility of the successful bidder.

Vendor must disclose the transaction collection fee amount to be charged to Non-DHR Fee Paid applicants for the duration of the contract period and any extension periods to the contract at the time of the bid. The fee must not exceed $10 per transaction.

Installation, Training, and Technical Support must be provided by the vendor on an annual basis. A vendor who is awarded this contract must provide a minimum of two (2) hours of training each year of the contract.

Counties of the State of Alabama have been divided into three regions:
North, Central, and Southern Regions.

Training for those counties will take place at a central location determined by the DHR within each region.

Please provided your concurrence with this requirement by listing the hours of training you will provide to DHR if you were to be awarded this contract:

HOURS OF TRAINING BEING BID:_____

_____

LINE 0004

DHR has purchased one hundred (100) InVize ID software units in order to facilitate the operation of its current livescan and cardscan transaction collection service for each of the aforementioned 31 sites. The InVize ID software units meet workstation and transaction collection processing requirements stated above. Subject to funding and need, DHR reserves the discretionary option to purchase up to an additional one hundred (100) InVize ID software units, in increments of ten (10), for DHR users in current or remaining Alabama counties, as specified by DHR, so that the system will be updated and/or expanded accordingly. **Installation, training, and technical support must be provided by the vendor. Vendor must bid a minimum of one (1) hour of training per location.**

Hours of Training being bid:_____

LINE 0005

The transaction fee required by the ABI/FBI will be listed at the time of the award of the bid, but will be set by those entities. No bid price is required by vendor in regard to this fee.

GENERAL REQUIREMENTS FOR ALL ABOVE ITEMS

All questions concerning purchasing procedures related this ITB must be submitted in writing via email to:
Kati Darnell State of Alabama / Department of Finance / Division of Purchasing
E-mail: Kati.Darnell@purchasing.alabama.gov

All questions concerning line item requirements or special terms and conditions defined herein must be submitted in writing via email to:
Krystle Scott State of Alabama / Department of Human Resources
E-mail: Krystle.Scott@dhr.alabama.gov

Vendors may participate in a Bidders' Conference to be held on December 17, 2009 at 1:00 p.m. at the State Purchasing Auditorium located at RSA Union Building, 100 N. Union St., Suite 192, Montgomery, AL 36130, (334) 242-7250. DHR will supply a court reporter for said Bidder's Conference.

Vendors must provide performance demonstration at DHR site prior to final bid award. This demonstration must be performed within 3 days of email notification by the Department of Human Resources or your bid will not be considered.

Vendors must bid all additional equipment not specified in the ITB including cabling cables, connectors, devices, equipment furniture, hardware and software, peripherals, and any other items which are required for installation and to permit the proposed Live Scan Fingerprinting System to become fully operational in accordance with the specifications.

Vendors shall submit with their bid all recommendations, descriptions, any forms, drawings, narratives, and general information that a vendor deems necessary to present a clear concise bid. **Vendors must identify all resource documentation/specifications by the Line Item in the ITB.**

All Internet based hardware/software must be FBI year 2010 compliant hardware/software. ***See Attachment #8 (FBI year 2010 requirements found in CJIS Security Policy June 2007 Version 4.4 pages 8, 24-26, 28-30, and pages 5-6 of Appendix C19).***

All Hardware/Software must be ABI/FBI certified at time of bid. In order for the vendor's bid to be accepted, the system bid must be certified by the Alabama Department of Public Safety ("DPS"). **Vendor must provide a copy of its DPS certification at the time of the bid.**

Vendor must be able to provide all items listed above in the entire bid announcement with or without partners.

The vendor shall have sole responsibility for the complete effort specified in the contract. Payment will be made only to the vendor. The vendor shall have sole responsibility for all payments due any subcontractor. The vendor is responsible for the professional quality, technical accuracy and timely completion and submission of all deliverables, services or commodities required to be provided under the contract. The vendor shall, without additional compensation, correct or revise any errors, omissions, or other deficiencies in its deliverables and other services. The approval of deliverables furnished under this contract shall not in any way relieve the vendor of responsibility for the technical adequacy of its work. The review, approval, acceptance or payment for any of the services shall not be construed as a waiver of any rights that the State may have arising out of the vendor's performance of this contract.

The vendor is not permitted to issue news releases pertaining to any aspect of the services being provided under this contract without the prior written consent of the DHR Commissioner. The vendor shall not use DHR's name, logos, images, or any data or results arising from this contract as a part of any commercial advertising without first obtaining the prior written consent of the DHR Commissioner.

All vendors who bid on this ITB must have a minimum of five (5) years experience providing and supporting law enforcement and criminal justice system solutions. **Please provide at least five (5) references to support this requirement with contact information such as, entity name, a contact name for the entity, address, telephone and facsimile number and e-mail address.** Vendors must also have AFIS Livescan certification (AFIS Interface Control Document for Foreign Livescan [May 16, 2005: 0026-1269; Revision F] prior to submitting a response to the ITB.

In the event that DHR or the contractor discovers any material omission in the provisions of this ITB that is believed to be essential to the successful performance of the contract, each must so inform the other in writing. DHR and the contractor will the follow the procedures outlined in the provisions of the contract addressing change orders.

Hardware/Software and website shall be installed and operational within 5 days of contract award.

Training: The vendor shall provide an on-site training program, including necessary user documentation, materials and supplies. Vendor shall state the number of hours included for this training. The vendor must provide on-site, hands-on and in-depth systems administrator training. The vendor shall state the number of hours included for this training. **The vendor must identify the number of hours they are bidding for training purposes.**

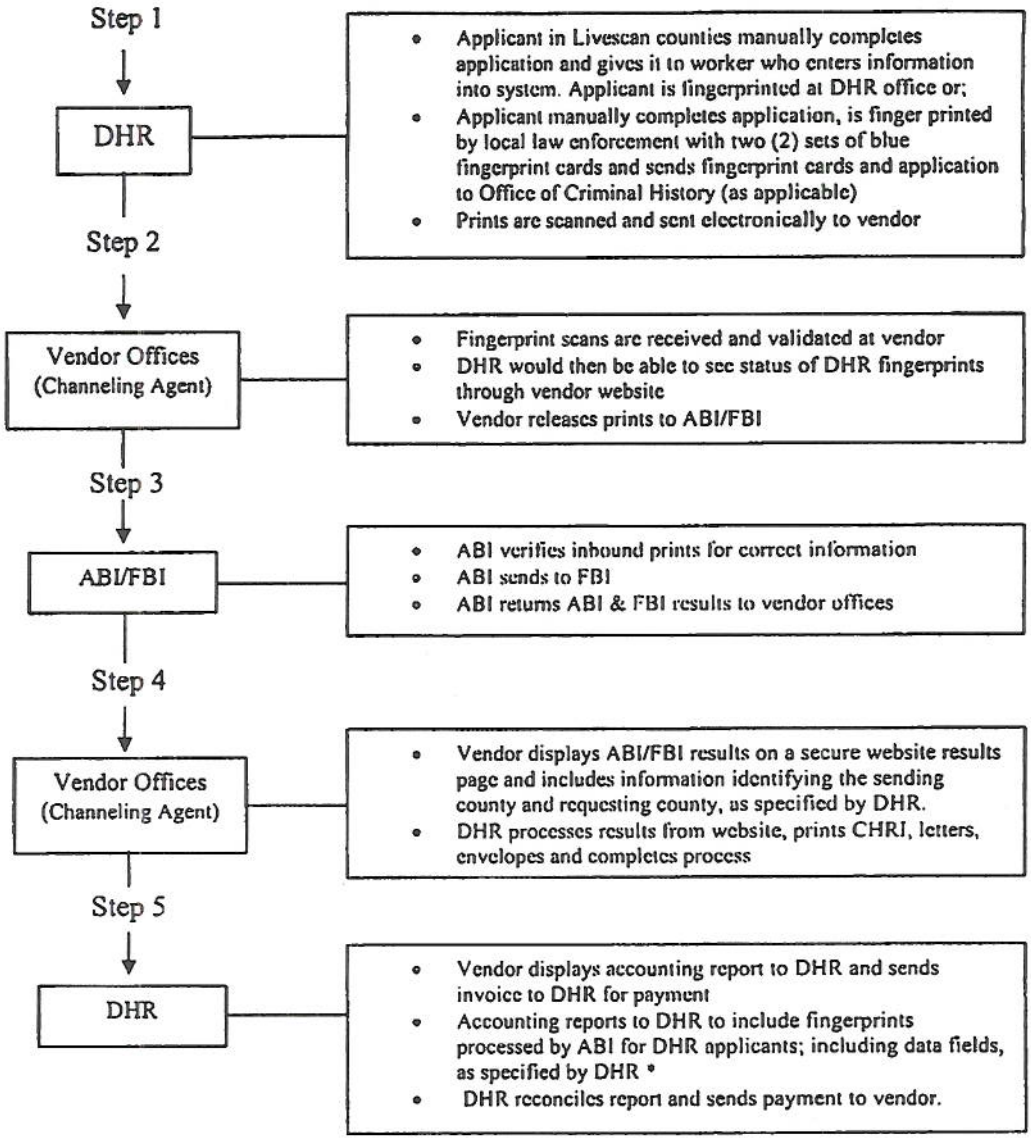
Warranty: Any Vendor bidding on this system must certify that it will provide a one (1) year warranty for any parts and labor against manufacturer defects in materials and workmanship commencing at the time of installation. One (1) year warranties remain in effect for equipment and software purchased for the aforementioned 31 sites. Those warranties provide coverage for labor and parts against manufacturer defects in materials and workmanship commencing at installation or at the time of repair, whichever was last. Contract vendor will be provided a list of installation dates for all existing equipment and software. **Vendor must provide a copy of its manufacturer and labor and parts warranty with at the time of the bid.**

Maintenance and Support: Any Vendor bidding on this system must certify that it will provide maintenance and support for the proposed system for the term of the contract and any period of contract extension for the equipment and software installed by vendor. Any vendors bidding on this system must be certified by i3 to operate, maintain, and support inVize ID application software and i3 DigiID equipment or certify that it will provide facilitation for the referenced support and maintenance by i3 or an entity certified by i3 to perform any necessary maintenance and support for the system for the duration of the contract. Any vendors bidding on this system must certify that its support for the proposed system shall include a toll free technical support help line that will operate, Monday through Friday, 8:00 a.m. to 5:00 p.m., CST. **Vendor must provide a copy of its maintenance and support terms and conditions to include the toll free number at the time of the bid. Vendor must also provide a copy of its certification by i3 to operate, maintain, and support the aforementioned equipment and software at the time of the bid.**

The term of the contract shall be for a period of two (2) years. The anticipated "Contract Effective Date" is provided on the signatory page of this ITB. If delays in the procurement process result in a change to the anticipated Contract Effective Date, the bidder agrees to accept a contract for the full term of the contract. The contract may be extended for all or part of three (3) one-year periods by the mutual written consent of the

contractor and DHR. **All bid prices must be held firm through the issuance and term of the original contract and the period(s) of contract extension.**

Alabama Department of Human Resources Electronic Fingerprint Channeling Process for DHR Fee Paid Applicants



* Data fields to be included unless otherwise specified;

- Applicants full name
- Partial SSN (Social Security Number)
- DOB (Date of Birth)
- ORI (originating county transmitting points)
- CRI (County responsible for information; i.e. processing prints)
- TCN Tracking Control Number)
- Worker ID
- Data Sent
- Price
- Case Type

Alabama Department of Human Resources Electronic Fingerprint Channeling Process for Non-DHR Fee Paid Applicants

Step 1

DHR

Applicant receives instructions, application and fingerprint cards from local DHR offices, Office of Criminal History, or State Office of Day Care. (as appropriate); Applicant manually completes application or applicant can obtain and partially complete application on DHR's vendor websites.

Step 2

Vendor Pre-Registration Website

- Vendor assigns control number for chain of custody (COC) form unique to online applicant via website after payment is received. (echeck, money order, cashiers check, credit card)
- Online applicant prints COC form and application.
- Online applicant completes and signs application or
- Applicant mails a completed application and payment to vendor
- Vendor will enter applicants information into system and return COC form to applicant.

Step 3

Law Enforcement Printing Office

- Applicant goes to law enforcement printing office
- 2 sets of fingerprints are taken on blue fingerprint cards
- Applicant sends both fingerprint cards, application (as applicable) and COC form to vendor using traceable means (FedEx, UPS, USPS, etc.)

Step 4

Vendor Offices (Channeling Agent)

- Fingerprint cards and COC forms are received by vendor
- Vendor verifies control number on COC and payment method
- Fingerprint cards are scanned by vendor and sent into vendor system
- Vendor scans in application and posts application on the results page of website for DHR to download and print
- Vendor releases prints to ABI/FBI

Step 5

ABI/FBI

- ABI verifies inbound prints for correct information
- ABI sends to FBI
- ABI returns ABI & FBI results to vendor offices

Step 6

Vendor Offices (Channeling Agent)

- DHR would then be able to see status of Non-DHR fingerprints through vendor website. Vendor displays ABI/FBI results on a secure website results page and includes information identifying the sending and requesting counties.
- DHR processes results from website, prints application, CHRI, letters, envelopes and completes process

Step 7

ABI/DHR

- Vendor provides accounting report to ABI and sends payment
- Accounting reports to DHR & ABI to include fingerprints processed by ABI for Non-DHR applicants, including data fields specified by DHR. (same as data fields specified on DHR Fee Paid channeling process document)

APPENDIX F

IAFIS IMAGE QUALITY SPECIFICATIONS

1.0 SCOPE AND PURPOSE

These specifications apply to fingerprint scanner systems and printers that will supply fingerprint data to the Integrated Automated Fingerprint Identification System (IAFIS), and to printers and displays within the IAFIS. They provide objective criteria for insuring image quality.

Electronic images must be of sufficient quality to allow for: (1) conclusive fingerprint comparisons (identification or non-identification decision); (2) fingerprint classification; (3) automatic feature detection; and (4) overall Automated Fingerprint Identification System (AFIS) search reliability.

The fingerprint comparison process requires a high fidelity image without any banding, streaking or other visual defects. Finer detail such as pores and incipient ridges are needed since they can play an important role in the comparison. Additionally, the gray-scale dynamic range must be captured with sufficient depth to support image enhancement and restoration algorithms.

The image quality requirements have associated test procedures, which are described in the document *Test Procedures for Verifying IAFIS Scanner Image Quality Requirements*. These procedures will be used by the Government in acceptance testing to ensure compliance with the requirements, and in performance capability demonstrations as an indication of capability to perform. Equipment shall be tested to meet the requirements in normal operating modes, e.g., scanners shall not be tested at slower than normal operating speeds to meet modulation transfer function specifications. A vendor may recommend alternate testing methods.

2.0 FINGERPRINT SCANNERS

The following subsections describe the image quality performance characteristics required for a fingerprint scanner (live scan and card scan). These specifications require that the scanner shall capture fingerprints at a minimum resolution in both the detector row and detector column directions (also known as 'along-scan' and 'cross-scan' directions) of 500 pixels/inch, plus or minus 5 pixels per inch. The final output delivered image from the scanner system shall have a resolution of 500 pixels/inch, plus or minus 5 pixels per inch, and each pixel shall be gray level quantized to 8 bits. [Requirement described in the ANSI standard: *Data Format for the Interchange of Fingerprint Information*, ANSI/NIST-CSL 1-1993.]

2.1 Geometric Image Accuracy

The absolute value of the difference "D", between the actual distance "X" between any two points on a target and the

distance "Y" between those same two points as measured on the output scanned image of that target, shall meet the following requirements for the value D:

D 0.0007, for 0 X 0.07

D 0.01X, for 0.07 X 1.50

where: D, X, Y are in inches and D = Y - X

The requirement corresponds to a positional accuracy of ± 1% for distances between 0.07 and 1.5 inches, and a constant ± 0.0007 inches (1/3 pixel) for distances less than or equal to 0.07 inches. The geometric image accuracy shall be measured using precision 1 cycle per millimeter Ronchi targets on white Mylar reflective base manufactured by Applied Image, Inc.[4]

2.2 Modulation Transfer Function

The measured modulation trans fer function (MTF) of the scanner, in both the detector row and detector column directions, and over any region of the scanner's field of view, shall have modulation values which fall within the ranges given in the following MTF table, at the given spatial frequencies:

cyc/mm	MTF
1	.905 to 1.00
2	.797 to 1.00
3	.694 to 1.00
4	.598 to 1.00
5	.513 to 1.00
6	.437 to 1.00
8	.312 to 1.00
10	.200 to 1.00

The MTF shall be measured using test chart number M-13-60-1X manufactured by Sine Patterns, Inc.[5]. The single, representative sine wave modulation in each imaged sine wave frequency pattern is determined from the sample modulation values collected from within that pattern. The sample modulation values are computed from the maximum and minimum levels corresponding to the 'peak' and adjacent 'valley' in each sine wave period. These maximum and minimum levels represent the corresponding locally averaged image gray levels mapped through a calibration curve into target reflectance space, where the local average of gray levels is computed in a direction orthogonal to the sinusoidal variation direction. Sample image modulation is then defined as:

[4]Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

[5]Sine Patterns, 236 Henderson Drive, Penfield, NY 14526, Phone (716) 248-5338

(maximum - minimum) / (maximum + minimum)

The calibration curve is constructed by performing a least squares linear regression curve fit between the image gray levels of the 14 density patches in the test target and the corresponding target reflectance values. The scanner MTF at each frequency is then defined as:

MTF = representative image modulation / target modulation

[Target modulations and target density patch values are supplied with the test target by the manufacturer.]

2.3 Signal-to-Noise Ratio

Both the ratio of signal to white noise standard deviation and the ratio of signal to black noise standard deviation of the digital scanner shall be greater than or equal to 125 using the following procedure:

1) A random 0.25 inch x 0.25 inch test field within the image area is chosen and the white reference target, Munsell[6] N9-white matte, is placed in the test field.

2) A white test population of 8-bit reflectance values from at least 1000 samples within the test field are collected. The average value and standard deviation are computed from this test population.

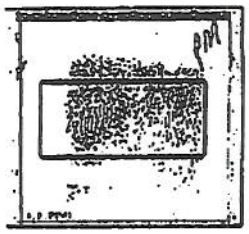
3) Steps 1 and 2 are repeated for the black reference target, Munsell N3 - black matte.

4) The signal to noise ratio (SNR) is computed as the difference between average white and average black values, alternately divided by the white noise standard deviation ('white SNR') and the black noise standard deviation ('black SNR').

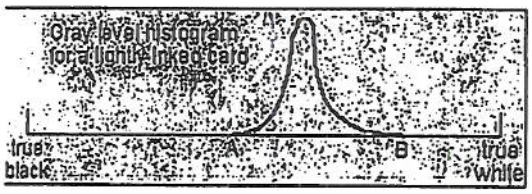
Note: The scanner shall be set up such that the white reference target is below scanner saturation level, and the black reference target is above scanner dark current level. Also, care should be taken, via direct visual or visual display observation, to avoid areas of dust, pinholes, scratches, or other imperfections on the target when selecting the sub-area for the 1000 samples.

[6] Munsell-Macbeth, P.O. Box 230, Newburgh, NY 12551, Phone (914) 565-7660

2.4 Gray-Scale Range of Image Data



At least 80% of the captured individual fingerprint images shall have a gray-scale dynamic range of at least 200 gray levels and at least 99% shall have a dynamic range of at least 128 gray levels. For this requirements section, 'dynamic range' is defined as the total number of gray levels that have signal content from the fingerprint image. Fingerprint card format lines, boxes, and text shall be excluded from the dynamic range computation and white surround in the immediate vicinity of a given fingerprint shall be included in the dynamic range computation (dashed box at right). Compliance with these dynamic range requirements shall be verified using a stratified sample of fingerprint cards assembled by the Government.



The intent is to avoid excessively low contrast images. Live-scan systems and card scanners at a booking station can control dynamic range by rolling the prints properly. However, with central site or file conversion systems, where a variety of card types and image qualities are encountered, adaptive processing may be necessary. The 8-bit quantization of the gray-scale values for very low contrast fingerprints needs to more optimally represent the reduced gray-scale range of such fingerprints. In the example histogram accompanying this section, the gray-scale values divide up the range from A to B. The parameters A and B are stored with the image to provide an audit trail.

2.5 Gray-scale Linearity

Using the 14 gray patches in the Sine Patterns, Inc. test target M-13-60-1X as the scanner input (independent variable), with their manufacture-supplied reflectance values, none of the corresponding 14 scanner output gray levels (dependent variable) shall deviate by more than 7.65 gray levels from a linear, least squares regression line fitted between the two variables. The output sample values within an area of at least 0.25 x 0.25 inches shall be utilized to compute the average output gray level for each patch.

2.6 Output Gray Level Uniformity

Output gray level uniformity shall be determined by scanning both a white reference target, Munsell N9 - white matte, and a black reference target, Munsell N3 - black matte. The scanner shall be set up such that the white reference target is below scanner saturation level, and the black reference target is above scanner dark current level in the respective tests. Using the white target as the scanner input, the following three requirements shall be met:

(1) The outputs of any two adjacent rows or columns of length 9 pixels or greater shall not have mean gray levels that differ by more than 2.5 gray levels.

(2) For all pixels within a 0.25 inch x 0.25 inch area ('quarter inch area') located in any region of the total scanner field of view, no individual pixel's gray level shall vary from the mean gray level by more than 22.0 gray levels.

(3) For any two non-contiguous quarter inch areas located anywhere in the total scanner field of view, the mean gray levels of the two quarter inch areas shall not differ by more than 12.0 gray levels.

And, using the black target as the scanner input, the following three requirements shall be met:

(1) The outputs of any two adjacent rows or columns of length 9 pixels or greater shall not have mean gray levels that differ by more than 1.0 gray levels.

(2) For all pixels within a 0.25 inch x 0.25 inch area ('quarter inch area') located in any region of the total scanner field of view, no individual pixel's gray level shall vary from the mean gray level by more than 8.0 gray levels.

(3) For any two non-contiguous quarter inch areas located anywhere in the total scanner field of view, the mean gray levels of the two quarter inch areas shall not differ by more than 3.0 gray levels.

CJIS-RS-0010 (V7)

105

January 29, 1999

3.0 LATENT PRINT SCANNERS

The following subsections describe the image quality performance characteristics required for a latent print scanner operating in a 1000 pixels/inch mode. These specifications require that the scanner shall capture fingerprints at a minimum resolution in both the detector row and detector column directions (also known as 'along-scan' and 'cross-scan' directions) of 1000 pixels/inch. The final output delivered image from the scanner system (at the 1000 ppi setting) shall have a resolution of 1000 pixels/inch, plus or minus 10 pixels per inch, and each pixel shall be gray level quantized to a minimum of 8 bits. The complete latent print specification consists of all requirements given in this Section, plus all non-conflicting requirements given in Section 2.0 Fingerprint Scanners.

3.1 Geometric Image Accuracy

The absolute value of the difference "D", between the actual distance "X" between any two points on a target and the distance "Y" between those same two points as measured on the output scanned image of that target, shall meet the following requirements for the value D:

D 0.0005, for 0 X 0.07

D 0.0071X, for 0.07 X 1.50

where: D, X, Y are in inches and D = Y - X

The requirement corresponds to a positional accuracy of ± .71% for distances between 0.07 and 1.5 inches, and a constant ± 0.0005 inches (½ pixel) for distances less than or equal to 0.07 inches. The geometric image accuracy shall be measured using precision 1 cycle per millimeter Ronchi targets on white Mylar reflective base manufactured by Applied Image, Inc.[7]

3.2 Modulation Transfer Function

The measured modulation transfer function (MTF) of the scanner, in both the detector row and detector column directions, and over any region of the scanner's field of view, shall have modulation values which fall within the ranges given in the following MTF table, at the given spatial frequencies:

cyc/mm	MTF
1	0.925 to 1.00
2	0.856 to 1.00
3	0.791 to 1.00
4	0.732 to 1.00
5	0.677 to 1.00
6	0.626 to 1.00
8	0.536 to 1.00

[7]Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

cyc/mm	MTF
10	0.458 to 1.00
12	0.392 to 1.00
14	0.336 to 1.00
16	0.287 to 1.00
18	0.246 to 1.00
20	0.210 to 1.00

The MTF shall be measured using test chart number M-13-60-1X manufactured by Sine Patterns, Inc.[8]. The single, representative sine wave modulation in each imaged sine wave frequency pattern is determined from the sample modulation values collected from within that pattern. The sample modulation values are computed from the maximum and minimum levels corresponding to the 'peak' and adjacent 'valley' in each sine wave period. These maximum and minimum levels represent the corresponding locally averaged image gray levels mapped through a calibration curve into target reflectance space, where the local average of gray levels is computed in a direction orthogonal to the sinusoidal variation direction. Sample image modulation is then defined as:

(maximum - minimum) / (maximum + minimum)

The calibration curve is constructed by performing a least squares linear regression curve fit between the image gray levels of the 14 density patches in the test target and the corresponding target reflectance values. The scanner MTF at each frequency is then defined as:

MTF = representative image modulation / target modulation

[Target modulations and target density patch values are supplied with the test target by the manufacturer.]

[8]Sine Patterns, 236 Henderson Drive, Penfield, NY 14526, Phone (716) 248-5338

4.0 IAFIS DISPLAY SPECIFICATIONS

Two types of displays are required. One is for the ten-print examiner and document processing. The other is for the latent examiner.

4.1 Ten-print / Document Processing Display

The ten-print/document processing display shall meet the following performance levels:

Parameter	Value	Comments
Colors	256	8 bits/pixel
Number ofaddressable pixels	1280 x 1024	
Pixel size	0.28 mm (max)	width at 50% amplitudeat center of display
Active display area	14" x 10.5" (min)	Landscape mode
Display refresh	at least 72 Hznoninterlaced	Minimizes flickerrate
Video bandwidth	at least100 MHz	
Luminance	33 fL (min)	of white area
Video pulse rise & fall time	3 nanosec. (max)	ensures no visible smearing
Geometric pixel location error	±1.5% (max)	No point varies more then 1.5%from its correct position
Operator controls	brightness, contrast	on front panel
Brightness Uniformity	±15% of meandeviation (max)	over entire display at low, medium and high brightness

---

4.2 Latent Print Comparison Display

The other display is for use by the FBI's latent fingerprint examiners. Because this display will be used to support latent fingerprint comparisons, the resolution and brightness (luminance) requirements are higher. The display shall be a monochrome cathode ray tube display, which shall meet the following performance levels:

Parameter	Value	Comments
Gray levels	8 bits/pixel @CRT video input	
Number of addressable pixels	1600 x 1200	
Pixel size	0.19 mm (max)	width at 50% amplitude at center of display
Active display area	14" x 10.5" (min)	Landscape mode
Display refresh rate	at least 72 Hz noninterlaced	Minimizes flicker
Video bandwidth	at least 100 MHz	
Luminance	50 fL (min)	of white area
Video pulse rise & fall time	3 nanosec. (max)	ensures no visible smearing
Geometric pixel location error	±1.5% (max)	No point varies more then 1.5% from its correct position
Operator controls	brightness, contrast	on front panel
Brightness Uniformity	±15% of mean deviation (max)	over entire displa y at low, medium and high brightness

The ambient lighting in the work area is expected to be a combination of natural and fluorescent lighting.

CJIS-RS-0010 (V7)

109

January 29, 1999

5.0 PRINTER SPECIFICATIONS

The fingerprint examiners in the IAFIS environment will depend upon softcopy images to make comparisons and will require hardcopy images in certain instances. Some contributors will print cards from live scan or card scan devices for submission to the FBI. In all such cases the images will be mapped from their digital form to high resolution printing devices. The printed images must be of sufficient quality to support all phases of identification, including conclusive fingerprint comparisons (identification or non-identification decision).

Two classes of printing devices are required. The first is intended to support fingerprint card reproduction. These printers will be used within the IAFIS environment and by submitters who choose to print and mail their live scan results. The printers should provide high throughput, low-cost-per-copy, non-fading output. This monochrome printer shall perform at the following minimum levels:

Gray levels 16

Paper size 8" x 8" (min)

Resolution 500 dots/inch (min.), where each pixel is capable of producing 16 gray levels

A second class of printer is required to support the investigative fingerprint comparison function. Continuous tone monochrome output is required. This printer shall perform at the following minimum levels:

Gray levels 8-bit continuous-tone gray-scale

Paper Production of output paper print shall not require liquid processing

Paper size 8" x 11"

Resolution At least 500 pixels per inch, where each pixel is capable of producing 256 gray levels from an 8 bits/pixel input

CJIS-RS-0010 (V7)

110

January 29, 1999

Issued in Kansas City, Missouri, on December 7, 2004.

Sandra J. Campbell,

Acting Manager, Small Airplane Directorate, Aircraft Certification Service.

[FR Doc. 04-27521 Filed 12-15-04; 8:45 am]

BILLING CODE 4910-13-C

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

28 CFR Part 906

[NCPPC 107]

Outsourcing of Noncriminal Justice Administrative Functions

AGENCY: National Crime Prevention and Privacy Compact Council.

ACTION: Interim final rule; request for comments.

SUMMARY: The Compact Council, established pursuant to the National Crime Prevention and Privacy Compact (Compact), is publishing an Interim Final Rule ("interim rule") to permit the outsourcing of noncriminal justice administrative functions involving access to criminal history record information (CHRI). Procedures established to permit outsourcing are required to conform with the Compact Council's interpretation of Articles IV and V of the Compact.

DATES: This rule is effective December 31, 2004. Comments must be received on or before February 14, 2005.

ADDRESSES: Send all written comments concerning this interim rule to the Compact Council Office, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306; Attention: Todd C. Commodore. Comments may also be submitted by fax at (304) 625-5388. To ensure proper handling, please reference "Noncriminal Justice Outsourcing Docket No. 107" on your correspondence. You may view an electronic version of this interim rule at *www.regulations.gov*. You may also comment via electronic mail at *tcommodo@leo.gov* or by using the *www.regulations.gov* comment form for this regulation. When submitting comments electronically you must include NCPPC Docket No. 107 in the subject box.

FOR FURTHER INFORMATION CONTACT: Ms. Donna M. Uzzell, Compact Council Chairman, Florida Department of Law Enforcement, 2331 Philips Road, Tallahassee, Florida 32308-5333, telephone number (850) 410-7100.

SUPPLEMENTARY INFORMATION:

Comments Invited

This interim rule is being adopted without prior notice and prior public comment. However, to the maximum extent possible, the Compact Council provides an opportunity for public comment on regulations issued without prior notice. Accordingly, the Compact Council invites interested persons to participate in this rulemaking by submitting written comments, data, or views. See addresses above for information on where to submit comments.

The Compact Council will consider all comments received on or before the closing date for comments and will consider comments filed late to the extent practicable. The Compact Council may change this rulemaking in light of the comments received.

Background

The National Crime Prevention and Privacy Compact (Compact), 42 U.S.C. 14616, establishes uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes. The Compact was approved by the Congress on October 9, 1998, (Pub. L. 105-251) and became effective on April 28, 1999, when ratified by the second state. Article VI of the Compact provides for a Compact Council that has the authority to promulgate rules and procedures governing the use of the Interstate Identification Index (III) System for noncriminal justice purposes. This interim rule will permit a third party to perform noncriminal justice administrative functions relating to the processing of CHRI maintained in the III System, subject to appropriate controls, when acting as an agent for a governmental agency or other authorized recipient of CHRI.

In recent years, government and other statutorily authorized entities seeking improved efficiency and economy have become increasingly interested in permitting third party support services for noncriminal justice administrative functions. This is due in large part to the escalating demand for fingerprint-based risk assessments for authorized licensing, employment, and national security purposes over the last several years. The escalating numbers of noncriminal justice fingerprint submissions has resulted in increased workloads for local, state, and federal government entities. In addition, under OMB Circular No. A-76, the federal government is encouraged wherever feasible to use private sector services.

The Compact requires the FBI and each Party State to comply with III System rules, procedures, and standards duly established by the Compact Council concerning record dissemination and use, system security, and privacy protection. In that regard, the Compact specifies that any record obtained may be used only for the official purposes for which the record was requested. The Compact Council believes that, under the Compact, private contractors may be used to perform noncriminal justice administrative functions requiring access to CHRI provided there are appropriate controls expressly preserving the sole official purpose of the record request. With appropriate standards and requirements, the benefits of outsourcing may be attained without degradation to the security of the national III System of criminal records. For example, under this interim rule, subject to some exceptions, contracting agencies or organizations will not be permitted to have direct access to the III System by computer terminal or other automated means which would enable them to initiate record requests. Further, the interim rule provides that tasks necessary to perform noncriminal justice administrative functions will be monitored to assure the integrity and security of such records. Under the interim rule, safeguards will be required to ensure that private contractors may not access, modify, use, or disseminate such data in any manner not expressly authorized by a government agency or a statutorily authorized recipient of CHRI. Such procedures will establish conditions on the use of the CHRI and will limit dissemination of the CHRI to ensure that such CHRI is used only for authorized purposes. Such procedures also will provide for accurate and current data distribution and require proper maintenance and handling, including the removal and destruction of obsolete or erroneous information that has been brought to its attention. These conditions are necessary to ensure the confidentiality of such information.

Further, this interim rule permits the outsourcing of noncriminal justice administrative functions authorized under Articles IV and V of the Compact. Article IV provides generally for authorized record disclosure; Article V provides record request procedures as related to noncriminal justice criminal history record checks pursuant to the Compact. This interim rule outlines the basic structured framework for minimum standards to ensure that outsourced contracts satisfy the security and privacy required by the Compact Council when criminal history record

checks of the III are conducted for noncriminal justice purposes. The contracting parties are not at liberty to supercede these minimum standards with lesser standards; however, contracting parties are free to adopt more stringent standards than required by this regulation.

To ensure such minimum standards are followed, the interim rule provides that contracts and agreements providing for the outsourcing authorized by the interim rule "shall incorporate by reference a security and management control outsourcing standard approved by the Compact Council after consultation with the United States Attorney General." See 28 CFR 906.2(c). Therefore, in conjunction with the interim rule, the Compact Council established Security and Management Control Outsourcing Standards (Outsourcing Standards), published in a notice elsewhere in today's edition of the Federal Register, specifying the standards that must be followed under the interim rule. The Compact Council developed two Outsourcing Standards—one for Contractors having access to CHRI on behalf of an authorized recipient for noncriminal justice purposes and one for Contractors serving as channelers of noncriminal justice criminal history record check requests and results. The first Outsourcing Standard ("Security and Management Control Outsourcing Standard for Contractors Having Access to CHRI on Behalf of an Authorized Recipient for Noncriminal Justice Purposes") will be used by Contractors authorized to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI's Criminal Justice Information Services (CJIS) Wide Area Network (WAN). The second Outsourcing Standard ("Security and Management Control Outsourcing Standard for Channelers Only") will be used by Contractors authorized access to CHRI through a direct connection to the FBI's CJIS WAN. The Outsourcing Standards were developed by the Compact Council in coordination with the FBI's CJIS Division and relevant subcommittees of the CJIS Advisory Policy Board (APB). The APB is an advisory committee with representatives of state, local, and federal contributors and users of the FBI's National Crime Information Center information systems, including the III. The Compact Council has also invited comments on the Outsourcing Standards, in addition to inviting comments on this interim rule.

Administrative Procedures and Executive Orders

Administrative Procedure Act

This rule is published by the Compact Council as authorized by the National Crime Prevention and Privacy Compact (Compact), an interstate and Federal-State compact which was approved and enacted into law by Congress pursuant to Pub. L. 105–251. The Compact Council is composed of 15 members (with 11 state and local governmental representatives). The Compact specifically provides that the Compact Council shall prescribe rules and procedures for the effective and proper use of the III System for noncriminal justice purposes, and mandates that such rules, procedures, or standards established by the Compact Council be published in the Federal Register. *See* 42 U.S.C. 14616, Articles II(4), VI(a)(1) and VI(e). This publication complies with those requirements.

Although not subject to the notice and comment requirements of the Administrative Procedure Act, the Compact Council generally provides an opportunity for notice and comment before issuing regulations. This rulemaking, however, is being issued as an interim rule because of imminent plans by the Transportation Security Administration (TSA) to implement a program to conduct criminal history record information (CHRI) checks of certain commercial drivers. Pursuant to section 1012 of the USA PATRIOT Act (Pub. L. 107–56), a state "may not issue to any individual a license to operate a motor vehicle transporting in commerce a hazardous material unless [TSA] * * * has first determined * * * that the individual does not pose a security risk warranting denial of the license." TSA has informed the Compact Council that it plans to publish new regulations that implement procedures to be used when conducting required security risk assessments for hazmat drivers that will be effective January 31, 2005. Any delays in conducting the required background checks will pose a risk to the public and national security and be contrary to the public interest. According to TSA, it will need to perform as many as 2.7 million background checks as part of its hazmat program. As a result, TSA has informed the Compact Council that it will need to utilize private contractors to handle this large volume of CHRI checks. Therefore, because of the short time available before the TSA hazmat program is implemented, and because the Compact Council will not reconvene until after the TSA's implementation of the program, the Compact Council finds there is good cause to publish this interim rule that will permit TSA and other authorized agencies/entities to outsource noncriminal justice administrative functions pursuant to the provisions of this interim rule. The Compact Council welcomes any relevant comments concerning this interim rule and will consider such comments before issuing the final rule.

Executive Order 12866

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 12866 is not applicable.

Executive Order 13132

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 13132 is not applicable. Nonetheless, this rule fully complies with the intent that the national government should be deferential to the States when taking action that affects the policymaking discretion of the States.

Executive Order 12988

The Compact Council is not an executive agency or independent establishment as defined in 5 U.S.C. 105; accordingly, Executive Order 12988 is not applicable.

Unfunded Mandates Reform Act

Approximately 75 percent of the Compact Council members are representatives of state and local governments; accordingly, rules prescribed by the Compact Council are not Federal mandates. No actions are deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

The Small Business Regulatory Enforcement Fairness Act (Title 5, U.S.C. 801–804) is not applicable to the Compact Council's rule because the Compact Council is not a "Federal agency" as defined by 5 U.S.C. 804(1). Likewise, the reporting requirement of the Congressional Review Act (Subtitle E of the Small Business Regulatory Enforcement Fairness Act) does not apply. *See* 5 U.S.C. 804.

List of Subjects in 28 CFR Part 906

Administrative practice and procedure, Intergovernmental relations, Law Enforcement, Privacy.

■ Accordingly, chapter IX of title 28 Code of Federal Regulations is amended by adding part 906 to read as follows:

PART 906—OUTSOURCING OF NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

Sec.
906.1 Purpose and authority.
906.2 Third party handling of criminal history record information.

Authority: 42 U.S.C. 14616.

§ 906.1 Purpose and authority.

The purpose of this part 906 is to establish rules and procedures for third parties to perform noncriminal justice administrative functions involving access to Interstate Identification Index (III) information. The Compact Council is establishing this rule pursuant to the National Crime Prevention and Privacy Compact (Compact), title 42, U.S.C., chapter 140, subchapter II, section 14616. The scope of this rule is limited to noncriminal justice background checks in so far as they are governed by the provisions of the Compact as set forth in 42 U.S.C. 14614 and 14616.

§ 906.2 Third party handling of criminal history record information.

(a) Except as prohibited in paragraph (b) of this section, criminal history record information obtained from the III System for noncriminal justice purposes may be made available:

(1) To a governmental agency pursuant to a contract or agreement under which the agency performs activities or functions for another governmental agency that is authorized to obtain criminal history record information by a federal statute, federal executive order or a state statute that has been approved by the United States Attorney General; and

(2) To a private contractor, or other nongovernmental entity or organization, pursuant to a contractual agreement under which the entity or organization performs activities or functions for a governmental agency authorized to obtain criminal history record information as identified in paragraph (a)(1) of this section or for a nongovernmental entity authorized to obtain such information by federal statute or executive order.

(b) Criminal history record information provided in response to fingerprint-based III System record requests initiated by authorized governmental agencies or nongovernmental entities for noncriminal justice purposes may be made available to contracting agencies or organizations manually or electronically for such authorized purposes. Such contractors, agencies, or organizations shall not be permitted to have direct access to the III System by computer terminal or other automated means which would enable them to initiate record requests, provided however, the foregoing restriction shall not apply with respect to: (1) Persons, agencies, or organizations that may enter into contracts with the FBI or State criminal history record repositories for the performance of authorized functions requiring direct access to criminal history record information; and (2) any direct access to records covered by 42 U.S.C. 14614(b).

(c) The contracts or agreements authorized by paragraphs (a)(1) and (a)(2) of this section shall specifically describe the purposes for which criminal history record information may be made available to the contractor and shall incorporate by reference a security and management control outsourcing standard approved by the Compact Council after consultation with the United States Attorney General. The security and management control outsourcing standard shall specifically authorize access to criminal history record information; limit the use of the information to the purposes for which it is provided; prohibit retention and/or dissemination of the information except as specifically authorized in the security and management control outsourcing standard; ensure the security and confidentiality of the information; provide for audits and sanctions; provide conditions for termination of the contractual agreement; and contain such other provisions as the Compact Council, after consultation with the United States Attorney General, may require.

(d) The exchange of criminal history record information with an authorized governmental or nongovernmental entity or contractor pursuant to this part is subject to cancellation for use, retention or dissemination of the information in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the Compact Council in consultation with the United States Attorney General.

Dated: November 29, 2004.

Donna M. Uzzell,

Compact Council Chairman.

[FR Doc. 04–27488 Filed 12–15–04; 8:45 am]

BILLING CODE 4410–02–P

DEPARTMENT OF DEFENSE

Department of the Army

32 CFR Part 635

RIN 0702–AA42–U

Law Enforcement Reporting

AGENCY: Department of the Army, DoD.

ACTION: Final rule.

SUMMARY: The Department of the Army is publishing our rule concerning law enforcement reporting. The regulation prescribes policies and procedures on preparing, reporting, using, retaining, and disposing of Military Police Reports. The regulation prescribes policies and procedures for offense reporting and the release of law enforcement information.

DATES: Effective Date: January 18, 2005.

ADDRESSES: Headquarters, Department of the Army, Office of the Provost Marshal General, ATTN: DAPM–MPD–LE, 2800 Army Pentagon, Washington, DC 20310–2800.

FOR FURTHER INFORMATION CONTACT: Nathan Evans, Policy Analyst, Arlington, VA at (703) 693–2126.

SUPPLEMENTARY INFORMATION:

A. Background

In the July 16, 2004 issue of the Federal Register (69 FR 42626) the Department of the Army issued a proposed rule to publish 32 CFR part 635. This final rule prescribes procedures and responsibilities for law enforcement reporting. The Department of the Army received responses from two commentors. No substantive changes were requested or made. The Department of the Army has added two sections since the publication of this part as a proposed rule. Section 635.29 was added to support Department of Defense guidance and the recommendations from the Army G–1 Domestic Violence Task Force. This section encourages provost marshals to enter into memoranda of understanding with local civilian law enforcement agencies to improve sharing of information. Section 635.30 was added to provide guidance on the handling and disposition of lost, unclaimed or abandoned property. The subsequent sections have been re-numbered.

B. Regulatory Flexibility Act

The Department of the Army has determined that the Regulatory Flexibility Act does not apply because the rule does not have a significant economic impact on a substantial number of small entities within the

Appendix

C

CJIS SECURITY POLICY (CSP) REQUIREMENTS
AUTHENTICATION*

	INTERNET	WIRELESS	NON-WIRELESS
SECURE (procured pre-9/30/05)	Advanced Authentication or VPN- CSP Section 7.3.3, 7.6	LoginID/password CSP Section 7.3.3, 7.6, 7.9(c)	LoginID/password CSP Section 7.3.3
SECURE (procured post-9/30/05	Advanced Authentication or VPN- CSP Section 7.3.3, 7.6	Advanced authentication or VPN - CSP Section 7.3.3,7.6,7.9(c)	Advanced authentication or VPN
NON- SECURE (procured pre-9/30/05)	Advanced Authentication only - CSP Section 7.3.2, 7.6	LoginID/password CSP Section 7.3.2, 7.6, 7.9(c) Mobile Devices Advanced Auth& PIN 7.3.2 b)	LoginID/password - CSP Section 7.3.2
NON-SECURE (procured post-9/30/05)	Advanced Authentication only - CSP Section 7.3.2, 7.6	Advanced Authentication only CSP Section 7.3.2, 7.6, 7.9 (c), Mobile Devices Advanced Auth& PIN 7.3.2 b)	Advanced authentication only - CSP Section 7.3.2

*In situations fitting more than one designation, most stringent requirement applies. After 9/30/2010 Systems providing access to CJIS data require Advanced Authentication.

ENCRYPTION (in bits) ***

	INTERNET	WIRELESS	NON-WIRELESS
SECURE AND NON-SECURE (procured pre-9/30/2002)	128 CSP Section 7.3.2,7.3.3,7.6,7.8	56 until 9/30/2002 128 after 9/30/2005 CSP Section 7.9(b) FIPS 140-2 after 9/30/2005 Section 7.9(a)	128 CSP Section 7.3.2,7.3.3,7.8
SECURE AND NON-SECURE (procured 10/1/2002-9/30/2005)	128 CSP Section 7.3.2,7.3.3,7.6,7.8	128 CSP Section 7.3.2,7.3.3,7.8,7.9 FIPS 140-2 after 9/30/2005 Section 7.9(a)	128 CSP Section 7.3.2,7.3.3,7.8
SECURE AND NON-SECURE (procured post 9/30/2005)***	128 & FIPS 140-2 CSP Section 7.3.2,7.3.3,7.6,7.8	128 & FIPS 140-2 CSP Section 7.3.2,7.3.3,7.8	128 & FIPS 140-2 CSP Section 7.3.2,7.3.3,7.8

**The encryption requirement is not applicable to non-wireless private systems wholly owned and operated or managed by criminal justice agencies.

***After 9/30/2010 All systems= encryption requires 128 bit & FIPS 140-2

DHR CRIMINAL HISTORY CHECK APPLICATION
Part 1 of 2

DHR FEE PAID

Mail Application (Parts 1 & 2) and Fingerprint Cards to:

Alabama Department of Human Resources
Office of Criminal History
P.O. Box 304000
Montgomery, Alabama 36130-4000
(334) 353-5400

Type or print legibly

Social Security Number:	Reference ID Number:	
First Name:	Middle:	Last:
All Other Names Used:		Phone #:
Address:		
City:	State:	Zip Code:
Date of Birth:	Race:	Sex:

Applying For: *(Check One)*	Employment	Home Study	Household Members	License/Approval	Therapeutic Programs	Volunteer Work
	❑ Adult Day Care ❑ Child Placement Agency ❑ Day Care Center ❑ DHR ❑ DHR Other ❑ Elder Care ❑ Foster Care ❑ Health Services ❑ Home Day Care ❑ Preventive Services ❑ Residential Care Agency ❑ Other	❑ DHR Adoption ❑ ICPC ❑ Private Adoption ❑ Relative Placement ❑ Other	❑ DHR Adoption ❑ Foster Care ❑ Home Day Care ❑ Private Adoption ❑ Relative Placement ❑ Other	❑ Adult Day Care ❑ Day Care Center ❑ Elder Care ❑ Foster Care ❑ Home Day Care ❑ Other	❑ Foster Care ❑ Mental Health Services ❑ Relative Placement ❑ Other	❑ Board Member ❑ DHR ❑ Internship ❑ Other

Affidavit For Release of Information

I do hereby for myself, my heirs, executors, and administrators release and forever discharge the Alabama Department of Human Resources and its officers and agents from any and all claims, actions, or causes of action, which may arise as a consequence of the release of the criminal history information.

I am possessed of sound mind and legally competent to execute this release. I hereby authorize the Alabama Department of Human Resources to release any and all criminal history information.

I certify that I have read this release and that I understand the significance of the same and in witness thereof I have voluntarily signed my name on this _____ day of _____ 20 _____.

Signature: _____

NOTE This document must be witnessed by two persons or notarized by a Notary Public.

Name of Witness #1 _____ Name of Witness #2 _____

Address of Witness #1 _____ Address of Witness #2 _____

City, State, Zip _____ City, State, Zip _____

OR

Sworn to and subscribed before me on this _____ day of _____, 20_____.

Signature of Notary Public _____

My commission expires _____, 20 _____.

Fingerprint Technician:

_____ Fingerprint Card Issued

_____ Live Scan Transmission

Signature _____

Date _____

DHR CRIMINAL HISTORY CHECK APPLICATION
Part 2 of 2

Name of Requesting Agency: _____
(employer, adoption agency, foster home licensing agency, child or adult care center, volunteer coordinating agency, etc.)

Address: _____

Telephone No: _____ **DHR Licensing or Approving Office:** _____

Alabama law requires that a criminal history background check be conducted on applicants for certain DHR positions and on all persons who hold a license or work in a Department of Human Resources licensed child care or adult care home, a foster or adoptive home approved by the Department of Human Resources, or a licensed child placing agency, including all officers and agents of the entity. You are required to provide full, accurate and complete information on your criminal conviction history upon application for a license or employment. This information shall be used to determine your suitability to provide care for children, the elderly, or disabled individuals. Unless a criminal history background check and suitability determination have previously been obtained, you must complete a DHR Criminal History Check Application (Parts 1 & 2) with fingerprints at the time of application for employment. Refusal to complete these documents or providing false information shall result in refusal of employment, approval, or licensure. The term conviction includes a determination of guilt by a trial, by a plea of guilty, or a plea of nolo contendere. Any individual determined to have submitted false information will be referred to the district attorney or law enforcement for investigation and possibly prosecution. An individual who intentionally falsifies any information on a statement is guilty of a class A misdemeanor, punishable by a fine of not more than two thousand dollars ($2,000) and imprisonment for not more than one year.

Convictions for any of the following crimes shall make an individual unsuitable for approval related to employment, adoption, foster home licensure, child or adult care licensure, or volunteer work:

1. Murder, manslaughter, or criminally negligent homicide.
2. A sex crime.
   A sex crime includes the following:
   a) Enticing a child to enter a vehicle, room, house, office, or any other space for immoral purposes, as proscribed by Section 13A-6-69 of the Code of Alabama 1975.
   b) Incest, when the offender is an adult and the victim is a minor, as proscribed by Section 13A-13-3 of the Code of Alabama 1975.
   c) Kidnapping of a minor, except by a parent, in the first or second degree, as proscribed by Section 13A-6-43 or Section 13A-6-44 of the Code of Alabama 1975.
   d) Promoting prostitution in the first degree or second degree, as proscribed by Section 13A-12-111 or Section 13A-12-112 of the Code of Alabama 1975.
   e) Rape in the first or second degree, as proscribed by Section 13A-6-61 or Section 13A-6-62 of the Code of Alabama 1975.
   f) Sexual misconduct, as proscribed by Section 13A-6-65 or the Code of Alabama 1975.
   g) Sexual torture, as proscribed by Section 13A-6-65 of the Code of Alabama 1975.
   h) Sexual abuse in the first or second degree, as proscribed by Section 13A-6-66 or Section 13A-6-67 of the Code of Alabama 1975.
   i) Sodomy in the first or second degree, as proscribed in Code 13A-6-63 or Section 13A-6-64 of the Code of Alabama 1975.
   j) Soliciting a child by computer for the purposes of committing a sexual act and transmittal of obscene material to a child by computer as proscribed by Sections 13A-6-110 and 13A-6-111 of the Code of Alabama 1975.
   k) Violation of the Alabama Child Pornography Act, as proscribed by Sections 13A-12-191, 13A-12-192,13A-12-196, or 13A-12-197 of the Code of Alabama 1975.
   l) Any solicitation, attempt, or conspiracy to commit any of the offenses listed in paragraphs a. to k., inclusive.
   m) A crime listed in the Community Notification Act, Chapter 20 of Title 15 of the Code of Alabama 1975.
3. A crime that involves the physical or mental injury or maltreatment of a child, the elderly, or an individual with disabilities.
4. A crime committed against a child.
5. A crime involving the sale or distribution of a controlled substance.
6. Robbery.
7. Conviction for a violation or attempted violation of an offense committed outside the State of Alabama for a sex crime or any other crime if the offense would be a crime in Alabama.

Criminal History Statement

Have you ever had a suitability determination made by the Department of Human Resources in connection with a previous criminal history check? Yes (___) No (___) If yes, send the form to DHR.

Have you ever been convicted of a crime? Yes (___) No (___) If yes, state on the lines below the date, crime, location, punishment imposed, and whether the victim was a child, elderly or a disabled individual.

_____

_____

Signature: _____ **Date:** _____

Print Name: _____ **SSN#** _____

DHR CRIMINAL HISTORY CHECK APPLICATION
Part 1 of 2
NON-DHR FEE PAID

Mail Application (Parts 1 & 2), Payment, and Fingerprint Cards to:	Make Money Order or Cashier's Check payable to:

Type or print legibly

Social Security Number:	**Reference ID Number:**	
First Name:	**Middle:**	**Last:**
All Other Names Used:		**Phone #:**
Address:		
City:	**State:**	**Zip Code:**
Date of Birth:	**Race:**	**Sex:**

	Employment	Home Study	Household Members	License/Approval	Therapeutic Programs	Volunteer Work
Applying For: *(Check One)*	☐ Adult Day Care ☐ Child Placement Agency ☐ Day Care Center ☐ DHR ☐ DHR Other ☐ Elder Care ☐ Foster Care ☐ Health Services ☐ Home Day Care ☐ Preventive Services ☐ Residential Care Agency ☐ Other	☐ DHR Adoption ☐ ICPC ☐ Private Adoption ☐ Relative Placement ☐ Other	☐ DHR Adoption ☐ Foster Care ☐ Home Day Care ☐ Private Adoption ☐ Relative Placement ☐ Other	☐ Adult Day Care ☐ Day Care Center ☐ Elder Care ☐ Foster Care ☐ Home Day Care ☐ Other	☐ Foster Care ☐ Mental Health Services ☐ Relative Placement ☐ Other	☐ Board Member ☐ DHR ☐ Internship ☐ Other

Affidavit For Release of Information

I do hereby for myself, my heirs, executors, and administrators release and forever discharge the Alabama Department of Human Resources and its officers and agents from any and all claims, actions, or causes of action, which may arise as a consequence of the release of the criminal history information.

I am possessed of sound mind and legally competent to execute this release. I hereby authorize the Alabama Department of Human Resources to release any and all criminal history information.

I certify that I have read this release and that I understand the significance of the same and in witness thereof I have voluntarily signed my name on this _____ day of _____ 20 _____.

Signature: _____

***NOTE* This document must be witnessed by two persons <u>or</u> notarized by a Notary Public.**

Name of Witness #1	Name of Witness #2
Address of Witness #1	Address of Witness #2
City, State, Zip	City, State, Zip

OR

Sworn to and subscribed before me on this _____ **day of** _____, **20**_____.

Signature of Notary Public

My commission expires _____, **20** _____.

Fingerprint Technician:

_____ Fingerprint Card Issued

_____ Live Scan Transmission

_____
Signature

_____
Date

DHR CRIMINAL HISTORY CHECK APPLICATION
Part 2 of 2

Name of Requesting Agency: _____
(employer, adoption agency, foster home licensing agency, child or adult care center, volunteer coordinating agency, etc.)

Address: _____

Telephone No: _____ **DHR Licensing or Approving Office:** _____

Alabama law requires that a criminal history background check be conducted on applicants for certain DHR positions and on all persons who hold a license or work in a Department of Human Resources licensed child care or adult care home, a foster or adoptive home approved by the Department of Human Resources, or a licensed child placing agency, including all officers and agents of the entity. You are required to provide full, accurate and complete information on your criminal conviction history upon application for a license or employment. This information shall be used to determine your suitability to provide care for children, the elderly, or disabled individuals. Unless a criminal history background check and suitability determination have previously been obtained, you must complete a DHR Criminal History Check Application (Parts 1 & 2) with fingerprints at the time of application for employment. Refusal to complete these documents or providing false information shall result in refusal of employment, approval, or licensure. The term conviction includes a determination of guilt by a trial, by a plea of guilty, or a plea of nolo contendere. Any individual determined to have submitted false information will be referred to the district attorney or law enforcement for investigation and possibly prosecution. An individual who intentionally falsifies any information on a statement is guilty of a class A misdemeanor, punishable by a fine of not more than two thousand dollars ($2,000) and imprisonment for not more than one year.

Convictions for any of the following crimes shall make an individual unsuitable for approval related to employment, adoption, foster home licensure, child or adult care licensure, or volunteer work:

1. Murder, manslaughter, or criminally negligent homicide.
2. A sex crime.
   A sex crime includes the following:
   a) Enticing a child to enter a vehicle, room, house, office, or any other space for immoral purposes, as proscribed by Section 13A-6-69 of the Code of Alabama 1975.
   b) Incest, when the offender is an adult and the victim is a minor, as proscribed by Section 13A-13-3 of the Code of Alabama 1975.
   c) Kidnapping of a minor, except by a parent, in the first or second degree, as proscribed by Section 13A-6-43 or Section 13A-6-44 of the Code of Alabama 1975.
   d) Promoting prostitution in the first degree or second degree, as proscribed by Section 13A-12-111 or Section 13A-12-112 of the Code of Alabama 1975.
   e) Rape in the first or second degree, as proscribed by Section 13A-6-61 or Section 13A-6-62 of the Code of Alabama 1975.
   f) Sexual misconduct, as proscribed by Section 13A-6-65 or the Code of Alabama 1975.
   g) Sexual torture, as proscribed by Section 13A-6-65 of the Code of Alabama 1975.
   h) Sexual abuse in the first or second degree, as proscribed by Section 13A-6-66 or Section 13A-6-67 of the Code of Alabama 1975.
   i) Sodomy in the first or second degree, as proscribed in Code 13A-6-63 or Section 13A-6-64 of the Code of Alabama 1975.
   j) Soliciting a child by computer for the purposes of committing a sexual act and transmittal of obscene material to a child by computer as proscribed by Sections 13A-6-110 and 13A-6-111 of the Code of Alabama 1975.
   k) Violation of the Alabama Child Pornography Act, as proscribed by Sections 13A-12-191, 13A-12-192,13A-12-196, or 13A-12-197 of the Code of Alabama 1975.
   l) Any solicitation, attempt, or conspiracy to commit any of the offenses listed in paragraphs a. to k., inclusive.
   m) A crime listed in the Community Notification Act, Chapter 20 of Title 15 of the Code of Alabama 1975.
3. A crime that involves the physical or mental injury or maltreatment of a child, the elderly, or an individual with disabilities.
4. A crime committed against a child.
5. A crime involving the sale or distribution of a controlled substance.
6. Robbery.
7. Conviction for a violation or attempted violation of an offense committed outside the State of Alabama for a sex crime or any other crime if the offense would be a crime in Alabama.

Criminal History Statement

Have you ever had a suitability determination made by the Department of Human Resources in connection with a previous criminal history check? Yes (___) No (___) If yes, send the form to DHR.

Have you ever been convicted of a crime? Yes (___) No (___) If yes, state on the lines below the date, crime, location, punishment imposed, and whether the victim was a child, elderly or a disabled individual.

_____

_____

Signature: _____ **Date:** _____

Print Name: _____ **SSN#** _____

Date

Name of Applicant
Street Address
City, State Zip Code

RE: **Criminal History Suitability**

A criminal history check has been conducted on the above individual by the **Alabama Bureau of Investigations (ABI) and the Federal Bureau of Investigations (FBI)** pursuant to the Code of Alabama 1975, Section 38-13-1, et seq. Based on the results of the ABI and FBI criminal history checks for the above individual, **you meet the suitability criteria** regarding approval of applicants for employment, adoption, foster home licensure, child or adult care licensure, or volunteer work under the above state statute. A suitability determination does not include certain convictions. An individual may have certain types of conviction and still receive a letter of suitability. A copy of your Criminal History Search Results (RAP Sheet) and the state law are available at the DHR Office of Criminal History.

Further inquiries should be mailed to the address below:

Alabama Department of Human Resources
Office of Criminal History
P. O. Box 304000
Montgomery, AL 36130-4000

You may also call 334-353-5400 to speak with someone if you have any questions.

Sincerely,

Office of Criminal History

c: DHR Licensing or Approving Office

Date

Name of Applicant
Street Address
City, State Zip Code

RE: **Criminal History Unsuitability**

A criminal history check has been conducted on the above individual by the **Alabama Bureau of Investigations (ABI) and the Federal Bureau of Investigation (FBI)** pursuant to Code of Alabama 1975, Section 38-13-1, et seq. Based on the results of the ABI and FBI criminal history checks for the above individual, **you do not meet the suitability criteria** regarding approval of applicants for employment, adoption, foster homes, child or adult care licensure, or volunteer work under the above state statute. A copy of your Criminal History Search Results (RAP Sheet) and the state law are attached. You may request a reversal of determination. The request must be submitted in writing to the address below within 30 days from the date of this letter.

Alabama Department of Human Resources
Office of Criminal History
P. O. Box 304000
Montgomery, AL 36130-4000

You may also call 334-353-5400 to speak with someone if you have any questions.

Sincerely,

Office of Criminal History

c: DHR Licensing or Approving Office (Letter Only)

Unsuitability Determination Informational Notice

(This Notice is to be sent with Unsuitability Letters Only)

In regard to a determination of unsuitability, Ala. Code (1975) § 38-13-7(e) provides as following:

(e) Within 30 days of the date of notification, an individual determined unsuitable for approval, licensure, employment, or volunteer work by the Department of Human Resources based upon a disqualifying conviction may request in writing reversal of the determination of unsuitability if the conviction is not for a sex crime or a crime committed against a child, an elderly individual, or an individual with disabilities. An individual with a conviction excluded by federal law from being approved as a foster or adoptive parent, as any other child care or adult care provider, or volunteer may not be considered for reinstatement. In the case of a felony conviction, 10 years shall have lapsed since the sentence was served or the probation or parole ended, whichever is later, with no subsequent conviction. In the case of a misdemeanor conviction, five years shall have lapsed since the sentence was served, or the probation or parole ended, whichever is later, with no subsequent conviction. The individual shall affirmatively demonstrate to the Department of Human Resources successful rehabilitation by clear and convincing evidence. In determining whether an individual has affirmatively demonstrated successful rehabilitation, all of the following shall be considered:

(1) Nature and responsibility of the position which the convicted person would hold or has held.

(2) Nature and seriousness of the offense committed.

(3) Circumstances under which the offense occurred.

(4) Date of the offense.

(5) Age of the person when the offense was committed.

(6) Whether the offense was an isolated or repeated incident.

(7) Social conditions which may have contributed to the offense.

(8) An available probation or parole record, report, or recommendation.

(9) Evidence of rehabilitation, including good conduct in prison or in the community, counseling or psychiatric treatment received, acquisition of additional academic or vocational schooling, successful business or employment history, and the recommendation of his or her supervisors.

(f) The Department of Human Resources and the Department of Public Safety may adopt rules and regulations to implement the procedures and requirements of this chapter pursuant to the Administrative Procedure Act, Section 41-22-1, et seq.

(Act 2000-775, p. 1775, §7.)

Date

Name of Applicant
Street Address
City, State Zip Code

RE: **Record of Arrest - Additional Information Needed**

As a result of your fingerprints being submitted for a criminal history check to the Alabama Bureau of Investigations (ABI)and the Federal Bureau of Investigations (FBI), files indicate a record of your arrest as follows:

Date:_____ Arresting Agency:_____
Charge:_____

Before your suitability status can be determined as required by Code of Alabama 1975, Section 38-13-1, et seq, the following information is needed from you:

1. A court-certified copy of the case action summaries showing the judgments, convictions, and sentencing or other outcomes of your case(s).
2. The same information regarding any other arrests.
3. A notarized personal explanation regarding the circumstances surrounding your cases. You should include the dates involved, the places of conviction, and any other factors that should be considered. Indicate if the victim was a child, elderly, or disabled.
4. If you have received a Pardon for any of these charges or other charges, include a copy of the Pardon Certificate/Letter.

If we are not in receipt of the requested information within 45 days from the date of this letter, we will consider your application as unsuitable and close the case. Mail the information to:

Alabama Department of Human Resources
Office of Criminal History
P. O. Box 304000
Montgomery, AL 36130-4000

You may also call 334-353-5400 to speak with someone if you have any questions.

Sincerely,

Office of Criminal History

Date

Name of Employer
Street Address
City, State Zip Code

RE: **Fingerprints Rejection or Application Incomplete**
Name of Employee

We are attempting to process the above employee's application for a criminal history check and are in need of additional information/documents to complete the procedure. See the items circled below:

1. The ABI fingerprints have been rejected and must be redone.
   The applicant must submit 2 new DHR fingerprint cards. Cards are enclosed.
2. The FBI fingerprints have been rejected and must be redone.
   The applicant must submit 2 new DHR fingerprint cards. Cards are enclosed.
3. The DHR Criminal History Check Application (Parts 1 & 2) has not been received.
4. The DHR Criminal History Check Application (Parts 1 & 2) is incomplete. See the highlighted areas.
5. The fee payment was not received.
6. Other _____

All paperwork in the package, including this letter, must be returned with the new fingerprint cards and/or application. Return the information to the address below:

Alabama Department of Human Resources
Office of Criminal History
P. O. Box 304000
Montgomery, AL 36130-4000

You may also call 334-353-5400 to speak with someone if you have any questions.

Sincerely,

Office of Criminal History

c: Applicant

Date

Name of Applicant
Street Address
City, State Zip Code

RE: **Updated Criminal History Report**

The Office of Criminal History has received information from the Alabama Bureau of Investigations (ABI) that you have an additional crime(s) on your criminal history record. This subsequent crime(s) may affect your suitability determination as stated in the previously issued suitability letter. The ABI files indicate a record of your arrest as follows:

Date:_____ Arresting Agency:_____

Charge:_____

Social Security Number: XXX-XX-_____ Category:_____

You must provide a final disposition from the arresting agency/court for the above charge. Once this information is received, we will issue a suitability or unsuitability letter. If we are not in receipt of the requested information within 45 days from the date of this letter, we will issue an unsuitability letter and close the case. Mail the requested information to:

Alabama Department of Human Resources
Office of Criminal History
P. O. Box 304000
Montgomery, AL 36130-4000

You may also call 334-353-5400 to speak with someone if you have any questions.

Sincerely,

Office of Criminal History

c: Employer, DHR Licensing or Approving Office

Letterhead Paper for DHR Office

Date

Name of Applicant
Street Address
City, State Zip Code

RE: Notice of False or Misleading Information

Pursuant to the Code of Alabama 1975, Section 38-13-4 and Section 38-13-9, a person who knowingly, willfully, and intentionally makes or transmits a false or misleading report or information concerning past convictions or who fails to report subsequent convictions, or who submits false information concerning past convictions on an application for employment, approval, or licensure or other form required for disclosure of criminal conviction may be subject to loss of employment and loss of any license issued by the Department of Human Resources or child placing agency.

Any individual determined to have submitted false information in regard to an application for employment, approval, or licensure or other form required for disclosure of criminal conviction shall be referred to the district attorney or law enforcement for investigation and possible prosecution. A person convicted of these actions under the aforementioned Code sections shall be guilty of a Class A misdemeanor, punishable by a fine of not more than $2000 and imprisonment for not more than one year.

An investigation of your criminal history revealed (*Provide any details of investigation that are available, such as past convictions not listed on the applicant's DHR Criminal History Check Application.)*

Pursuant to the aforementioned Code sections and the information submitted or obtained in regard to your request for employment, approval, or licensure, your application has been referred to the local district attorney for investigation and possible prosecution.

Sincerely,

Name of Worker
Title
Office of Criminal History

c: DHR State Office of Criminal History
DHR Licensing or Approving Office

Letterhead Paper for DHR Office

Date

Name of District Attorney
Street Address
City, State Zip Code

RE: Name of Applicant
SSN and DOB of Applicant

Pursuant to the Code of Alabama 1975, Section 38-13-4 and Section 38-13-9, the above-referenced individual is being referred to your office for investigation and possible prosecution for knowingly, willfully, and intentionally making or transmitting a false or misleading report or information concerning past convictions as required under the Alabama law regarding criminal background checks.

Per the aforementioned Code sections, a person convicted of these actions under the aforementioned Code sections shall be guilty of a Class A misdemeanor, punishable by a fine of not more than $2000 and imprisonment for not more than one year.

An investigation revealed (*Provide any details of investigation that are available, such as past convictions not listed on the applicants' Mandatory Criminal History Checks Notice. Attach a copy of the signed form to the letter to the District Attorney.)*

Please contact me at (*telephone number*) to discuss this matter further.

Sincerely,

Name of Worker
Title
Office of Criminal History

c: DHR State Office of Criminal History
DHR Licensing or Approving Office

Letterhead Paper for DHR Office

Date

Name of District Attorney
Street Address
City, State Zip Code

RE: Name of Applicant
SSN and DOB of Applicant

Pursuant to the Code of Alabama 1975, Section 38-13-4 and Section 38-13-9, the above-referenced individual is being referred to your office for investigation and possible prosecution for knowingly, willfully, and intentionally making or transmitting a false or misleading report or information concerning past convictions as required under the Alabama law regarding criminal background checks.

Per the aforementioned Code sections, a person convicted of these actions under the aforementioned Code sections shall be guilty of a Class A misdemeanor, punishable by a fine of not more than $2000 and imprisonment for not more than one year.

An investigation revealed (*Provide any details of investigation that are available, such as past convictions not listed on the applicants' Mandatory Criminal History Checks Notice. Attach a copy of the signed form to the letter to the District Attorney.)*

Please contact me at (*telephone number*) to discuss this matter further.

Sincerely,

Name of Worker
Title
Office of Criminal History

c: DHR State Office of Criminal History
DHR Licensing or Approving Office

U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

CJIS SECURITY POLICY

June 2007
Version 4.4

Approved by the
CJIS Advisory Policy Board
December 2006

This policy outlines the minimum security requirements set forth by the CJIS Division. Each CSA may

CJIS systems and all appropriate IT personnel shall receive security awareness training within six (6) months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

4.4 Physical Security

4.4.1 Computer Facility Security

The computer site and related infrastructures (e.g., information system servers, controlled interface equipment, associated peripherals, communications equipment, wire closets, patch panels, etc., including police vehicles if they house equipment which provides access to the CJIS network) must have adequate physical security at all times to protect against any unauthorized access to or routine viewing of computer devices, access devices, and printed and stored data. Also see Section 7.0 Technical Security for the definition of a physically secure location.

4.4.2 Mobile/Remote Devices

All mobile/remote devices, including all handheld and small form factor devices such as Personal Digital Assistants (PDAs), purchased after September 30, 2005 shall meet the approved form of data encryption and advanced authentication. All remote clients shall meet this requirement by September 30, 2010.

Policy shall be established by the CSA regarding the security for mobile and remote devices. Please refer to Appendix C (C.17), "Best Practices - Guidance for Handheld Device Security Policies" for guidance and information on this topic.

4.4.3 Visitors Access

All visitors to computer centers and/or terminal areas shall be escorted by authorized personnel at all times.

4.5 Personnel Security

4.5.1 Personnel Background Screening for Systems Access and Computer Terminal/ Records Storage Areas Access

a) To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days upon initial employment or assignment for all personnel who have authorized access to FBI CJIS systems and those who have direct responsibility to configure and maintain computer systems and networks with direct access to FBI CJIS systems. Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check. All requests for systems access shall be made as specified by the CSO. The CSO, or their

security features, roles, and environmental considerations (e.g., whether always used on-line, always used off-line, usually used off-line with the capability of going on-line, etc.), the implementation of tokens shall meet existing *CJIS Security Policy* (e.g., identification, encryption, and access control).

Definition:

Paper (Inert) Token - Made of inert material such as paper or plastic. The only authentication information on the token can be read or identified by a human; there is no machine readable authentication information on the token. The paper (inert) token typically is made of paper on which a grid or table is printed. Authentication data, text characters or images, are contained in the grid squares or boxes.

The paper (inert) token is typically used as a reference card in response to an authentication challenge question sent to the user terminal device. The user reads the information from the appropriate grid or series of grids and enters them into the terminal device in response to the authentication challenge question.

Policy for Paper (Inert) Tokens:

While each of the tokens may have somewhat different security requirements, security features, roles, and environmental considerations, the implementation of tokens shall meet existing *CJIS Security Policy* (e.g., identification, encryption, and access control).

7.3.2 Non-secure Locations

a) As of September 30, 2005, any procurement or upgrade for a system which is considered part of--or is accessing a criminal justice information system (CJIS)--from any Internet, wireless, or dial-in connection from a location that is <u>not</u> physically secured, shall use advanced authentication as defined in this policy. All systems <u>must</u> meet the advanced authentication and encryption standards by September 30, 2010. Please see Appendix C (C.19) for guidelines to clarify the meaning of system upgrade as applied in the CJIS Security Policy.

b) All mobile devices such as Personal Digital Assistants (PDA), cellular phones transmitting CJIS data, and mobile data computers or other portable clients which have been removed from a police vehicle shall, at a minimum, also incorporate the use of a unique password or other personal identifier (PIN) as well as meet the advanced authentication requirement.

7.3.3 Secure Locations

As of September 30, 2005, any procurement or upgrade for a system which is considered part of--or is accessing a criminal justice information system between--secure locations via the Internet, wireless, or dial-in connection from a remote location, shall use, at a minimum, a Virtual Private Network (VPN) or

If passwords are used for authentication, organizations shall ensure the following secure password attributes:

a) Passwords shall be a minimum length of eight (8) characters on systems procured after September 30, 2005, and on all systems by September 30, 2010.

b) Passwords shall not be a dictionary word or proper name.

c) Passwords and the Userid shall not be the same.

d) Passwords shall be changed within a maximum of every 90 days.

e) All systems procured after September 30, 2005 shall prevent password reuse of the last ten (10) passwords.

f) Passwords shall not be transmitted in the clear outside the secure domain.

See Appendix C (C.7) for additional information on "Robust Passwords, Best Practices."

7.5 Access Control

The Interface Agency shall develop and maintain the security documentation to address access control. See Appendix C (C.8) for implementation guidelines regarding "Access Control Criteria and Access Control Mechanisms."

7.6 Internet Access

The CSA is authorized to grant Internet access, to include Internet dial-up access, and to support CJIS processing when a minimum set of technical and administrative requirements have been met, to include advanced authentication and encryption. To assure the security of CJIS systems from unauthorized Internet access and to preserve the confidentiality, integrity, and availability of CJIS information as it is processed, CJIS transactions shall be permitted over the Internet only after the following minimum requirements have been implemented:

a) Advanced authentication as defined within this policy.

b) Networks in which some terminals or access devices have CJIS access and/or Internet access (e.g., peer-to-peer relationships, large mainframes and servers that house web sites) shall be protected by firewall-type devices. These devices shall implement a minimum firewall profile in order to provide a point of defense and a controlled and audited access to servers, both from inside and outside the CJIS networks.

c) Data which is at risk on access devices and workstations shall have the residual CJIS data protected by the methods of removal, encryption, or erasure.

d) All CJIS data transmitted through any Internet connection shall be immediately protected with a minimum of 128-bit encryption.

e) All Internet contracts after September 30, 2005 shall support a minimum of 128-bit encryption which has been certified by the National Institute of Standards and Technology (NIST) or Canada's Communications Establishment (CSE) to ensure that cryptographic modules meet FIPS Publication140-2 for ASecurity Requirements for Cryptographic Modules.@

For more information on minimum firewall profiles, see Appendix B (B.3) "Firewall Security Web Sites," and Appendix C (C.4) "Firewall Terms and Definitions."

7.7 Dial-up Access

The Interface Agency's responsibilities for dial-up access are as follows:

a) The Interface Agency may authorize employees and/or authorized third parties (e.g., vendors, etc.) to use dial-up connections to gain access to the Interface Agency's network.

b) Dial-up access shall be strictly controlled using an authentication mechanism as previously defined in this policy.

c) Advanced authentication for dial-up access shall be included in all procurements after September 30, 2005.

d) Dial-back functions shall be recognized as insufficient because they are easily compromised.

e) The Interface Agency shall have written procedures for dial-up access and track those who are authorized users. The Interface Agency shall also develop and maintain the security documentation to address user identity and agency association, the authorization of the user and the level of access authorized, the purpose of use, and the location of fixed-based dial-up sites.

f) If known, the location of the remote dial-up sites shall be noted for documentation purposes.

g) Each authorized dial-up user shall be issued a unique identifier.

h) All CJIS transactions and messages sent and received on the dial-up system (successful and unsuccessful) shall be logged.

i) The system shall be able to identify the transaction from the automated transaction log for all dial-up circuits.

j) Automatic logging shall include session initiation and termination messages, failed access attempts, and all forms of access violations such as attempts to access data beyond the level of authorized access.

k) Access to the transaction log shall be highly controlled.

l) The transaction logs shall be maintained for a minimum of twelve (12) months for the purpose of a security audit review.

m) All hosts which are connected to internal networks via dial-up shall use the most up-to-date anti-virus software. This includes personal computers.

n) Personal equipment which is used to connect to internal networks shall meet the requirements set forth by the Interface Agency for remote access.

7.8 Encryption

a) All CJIS data transmitted through any public network segment or over dial-up or Internet connections (does not include radio frequency transmissions) shall be immediately protected with a minimum of 128-bit encryption. This requirement also applies to any private data circuit that is shared with non-criminal justice users and/or is not under the direct management control of a criminal justice agency.

b) Any procurement after September 30, 2005 shall require a minimum of 128-bit encryption with NIST or CSE certification of the cryptographic module to ensure it meets FIPS Publication 140-2 for "Security Requirements for Cryptographic Modules" at any Security Level. Systems that transmit data over radio frequencies to a network with access to CJIS data that are procured after September 30, 2005, shall also be subject to this encryption requirement. Any minimum of 128-bit encryption procured before September 30, 2005 does not require NIST or CSE certification until September 30, 2010.

c) The FBI shall provide and manage encrypted sessions between the FBI Segment and the CSA.

d) The CSO shall ensure and oversee the management of encryption between the CSA and their users. In line with item 7.8 (a) above, encryption may terminate either at a router or firewall within a secured location, or the data may be encrypted from client to client. While client to client encryption is encouraged, it is not a requirement as long as the CJIS data passing as clear text is doing so within a secured facility behind a properly configured firewall.
Please see Appendix C (C.18) for an acceptable method to determine product conformance to the FIPS

140-2 encryption requirements in this policy.

7.8.1 Management of Encryption Keys

The ISO shall document or oversee the documentation of key management procedures. The key management procedures shall describe key generation, key distribution, key disposal, emergency procedures, key recovery, and key escrow.

See Appendix C (C.9) for "Guidelines and Recommendations for Effective Encryption Key Management."

7.9 Wireless

a) All wireless upgrades contracted after September 30, 2002 shall support a minimum of 128-bit encryption for all data. Any procurement for wireless devices after September 30, 2005, shall require a minimum of 128-bit encryption with NIST or CSE certification of the cryptographic module to ensure it meets FIPS Publication 140-2 for ASecurity Requirements for Cryptographic Modules.@ Any wireless device with a required minimum of 128-bit encryption procured before September 30, 2005, does not require NIST or CSE certification until September 30, 2010.

b) All currently-in-use symmetric and asymmetric mobile data terminal crypto-systems shall have key lengths of at least 56 bits or more; however, these currently-in-use systems shall meet the minimum 128-bit encryption requirement for data by the close of September 30, 2005 when sanctions for noncompliance will take effect. See Appendix C (C.6) for more details pertaining to the "Sunset Clause."

For your information:

- Asymmetric encryption is the same as public-key cryptography (i.e., a form of cryptography in which each user has a public key and a private key). Messages are sent encrypted with the receiver's public key, and the receiver decrypts them using the private key. Using this method, the private key never has to be revealed to anyone other than the user.

- *In symmetric cryptography, both ends have the same encryption key, meaning it uses the same key for encryption and decryption.*

c) All wireless links or server access points must be protected by authentication to ensure protection from unauthorized system access.

For additional guidance and information see Appendix C (C.10) for "Wireless Implementation Guidelines."

7.10 Firewalls

NOTE: All wireless upgrades and new wireless devices communicating through public networks must immediately employ, at a minimum, a personal/software based firewall where commercially available by more than one vendor. Any wireless devices procured before April 30, 2007 do not require a personal/software based firewall until September 30, 2010.

7.10.1 Network Firewalls

a) Networks in which some terminals, and/or access devices have CJIS access and/or Internet access (e.g., peer to peer relationships, large mainframes and servers that house web sites) shall be protected by network firewall type devices. These devices shall implement a minimum firewall profile in order to provide a point of defense and a controlled and audited access to servers, both from inside and outside the CJIS networks.

b) Network firewall architectures shall prevent unauthorized access to CJIS data and all network components providing access to the FBI CJIS WAN, either directly or indirectly through connections to other networks. Network firewall policies shall be concerned with securing the total site. This must include all forms of access, wireless, dial in, off site, Internet access, and others.

c) Network firewall operating system builds shall be based upon minimal feature sets. (It is extremely important that all unnecessary operating system features are removed from the build prior to network firewall implementation, especially compilers.) All unused networking protocols shall be removed from the network firewall operating system build.

d) Any appropriate operating system patches shall be applied before any installation of network firewall components, and procedures shall be developed to ensure that the network firewall patches remain current while the network firewall retains its statefulness.

e) All unused network services or applications shall be removed or disabled. Only network services that are required shall be permitted through the network firewall. Allowed services shall be documented as to the service allowed, the description of service, and the business requirement for service.

f) All unused user or system accounts shall be disabled.

g) All default vendor accounts shall have the passwords changed prior to the network firewall going on line.

h) Unused physical network interfaces shall be disabled or removed from the server chassis.

CJIS SECURITY POLICY (CSP) REQUIREMENTS
AUTHENTICATION*

	INTERNET	WIRELESS	NON-WIRELESS
SECURE (procured pre-9/30/05)	Advanced Authentication or VPN- CSP Section 7.3.3, 7.6	LoginID/password CSP Section 7.3.3, 7.6, 7.9(c)	LoginID/password CSP Section 7.3.3
SECURE (procured post-9/30/05	Advanced Authentication or VPN- CSP Section 7.3.3, 7.6	Advanced authentication or VPN - CSP Section 7.3.3,7.6,7.9(c)	Advanced authentication or VPN
NON- SECURE (procured pre-9/30/05)	Advanced Authentication only - CSP Section 7.3.2, 7.6	LoginID/password CSP Section 7.3.2, 7.6, 7.9(c) Mobile Devices Advanced Auth& PIN 7.3.2 b)	LoginID/password - CSP Section 7.3.2
NON-SECURE (procured post-9/30/05)	Advanced Authentication only - CSP Section 7.3.2, 7.6	Advanced Authentication only CSP Section 7.3.2, 7.6, 7.9 (c), Mobile Devices Advanced Auth& PIN 7.3.2 b)	Advanced authentication only - CSP Section 7.3.2

*In situations fitting more than one designation, most stringent requirement applies. After 9/30/2010 Systems providing access to CJIS data require Advanced Authentication.

ENCRYPTION (in bits) ***

	INTERNET	WIRELESS	NON-WIRELESS
SECURE AND NON-SECURE (procured pre-9/30/2002)	128 CSP Section 7.3.2,7.3.3,7.6,7.8	56 until 9/30/2002 128 after 9/30/2005 CSP Section 7.9(b) FIPS 140-2 after 9/30/2005 Section 7.9(a)	128 CSP Section 7.3.2,7.3.3,7.8
SECURE AND NON-SECURE (procured 10/1/2002-9/30/2005)	128 CSP Section 7.3.2,7.3.3,7.6,7.8	128 CSP Section 7.3.2,7.3.3,7.8,7.9 FIPS 140-2 after 9/30/2005 Section 7.9(a)	128 CSP Section 7.3.2,7.3.3,7.8
SECURE AND NON-SECURE (procured post 9/30/2005)***	128 & FIPS 140-2 CSP Section 7.3.2,7.3.3,7.6,7.8	128 & FIPS 140-2 CSP Section 7.3.2,7.3.3,7.8	128 & FIPS 140-2 CSP Section 7.3.2,7.3.3,7.8

**The encryption requirement is not applicable to non-wireless private systems wholly owned and operated or managed by criminal justice agencies.

***After 9/30/2010 All systems= encryption requires 128 bit & FIPS 140-2