LIVE SCAN DATA TRANSMISSION SPECIFICATION
GEORGIA BUREAU OF INVESTIGATION

Date of Issue: 10/30/96
Revised 9/14/99
Revised 6/12/2001
Revised 1/31/2002
Revised 1/10/2005
Revised 2/4/2005
Revised 10/30/2006
Revised 3/29/2007
Revised 1/20/2010
Revised 1/21/2011
Revised 2/24/2011
Revised 5/2/2011

Revision Update

October 30, 2006 …… Changes to Section 3.4; 3.6.3.1; 3.6.3.2 and 3.6.3.3

October 30, 2006 …… NATMS – changed to NIST File Collector (NFC)

March 29, 2007---------- Changes to Section 3.4 (.tbl to .txt); 3.6.2 deleted last sentence. 3.6.3 added sentence. 3.6.3.1 Message formats added Name (mrj), GBI TCN and FBI TCN (mfi); deleted SAN (mrj and mid). 3.6.3.2 replaced all _ END _ with _ _ END _ _; added TNETTCN to acknowledgment file.

August 1, 2007 ---------- Changes to Section 3.6.3.1POP 3 Mail Formats; added OTN to MID message format. Removed <Attachment> from bottom of MFI response message format.

January 20, 2010 ---------- Removed Appendices J, L, M, O, Q, BB, CC, DD, EE, FF, GG, II, JJ, KK

January 20, 2010 ---------- Directed to Download from valtabs.txt directory Appendices F, J,L, M, N, O, P, Q, S, U, GG, II, JJ,

January 21, 2011 _____ Changes to Section 3.4 FTP Common Partition Layout cnt.txt ; added information. 3.6.3.1 POP3 Mail Format; added FBI Name Search Message (MFN); MID (GBI) Ident response changed; FBI Name Search Response (MFN) and FBI Name Search Form added.

January 21, 2011 ---------- Appendix V added COR and JCOR TOT

February 24, 2011 ---------- Section 3.6.1 MID (FBI) Identification Response added “DHS Identification Response”.

May 2, 2011 ---------- CJIS Security Policy Version 5.0 Password Policy

CONTENTS

APPENDICES

Appendix A - Electronic Biometric Transmission Specification
(www.fbibiospecs.org)

Appendix B - WAVELET Scaler Quantization Specification

Appendix C - American National Standard Institute Standard
www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf)

Appendix D - Edit Criteria

Appendix E - Arrest Disposition Number (ADN)
Removed 3/26/2007

Appendix F - Translation Table for Caution
Download from valtabs.txt directory

Appendix G - CCH Field Identifier Translation Table

Appendix H - Court Disposition Numeric (CDN)
Removed 3/26/2007

Appendix I - Court Provision Number (CPN)
Removed 3/26/2007

Appendix J - Translation for Table for Eye Color
Removed 1/20/2010
Download from valtabs.txt directory

Appendix K - Translation Table for General Offense Character (GOC)
Removed 3/26/2007

Appendix L - Translation Table for Hair
Removed 1/20/2010
Download from valtabs.txt directory

Appendix M - Translation Table for Miscellaneous Identifying Number (MNU) Field
Removed 1/20/2010
Download from valtabs.txt directory

Appendix N - Offense Code Listing
Download from valtabs.txt directory

Appendix O - Translation Table for Race

Removed 1/20/2010
Download from valtabs.txt directory

Appendix P - Translation Table for Reject Code
Download from valtabs.txt directory

Appendix Q - Translation Table for Sex
Removed 1/20/2010
Download from valtabs.txt directory

Appendix R - Translation Table for Skin
Removed 3/26/2007

Appendix S - Scars, Marks & Tattoos (SMT) Code Listing
Download from valtabs.txt directory

Appendix T - Supervision Status Number (SSN)
Removed 3/26/2007

Appendix U - Translation Table For Turned Over To
Download from valtabs.txt directory

Appendix V - Translation Table for TOT Type 1 Transactions

Appendix W- Translation Table for TOT Type 1 Responses

Appendix X - Administrative Message Code Table

Appendix Y - Identification Response Code Table

Appendix Z - Acknowledgement Message Code Table

Appendix AA – NFS Protocol Version 3
Removed 1/31/2002

Appendix BB - Transmission Control Protocol
Removed 1/20/2010

Appendix CC - Internet Protocol Specification
Removed 1/20/2010

Appendix DD - Post Office Protocol Version 3
Removed 1/20/2010

Appendix EE - Network Processor & Multi-Protocol Network Program
2210 & 6611

Removed 1/20/2010

Appendix FF - Protocol Standards Defined by IEEE 802 & FDDI (c)
1992-1995 Microsoft Corp.
Removed 1/20/2010

Appendix GG - Ethernet Network
1994 Black Box Corp.
Removed 1/20/2010

Appendix HH – Translation Table for Purpose Code
Removed 2/4/2005
Download from valtabs.txt directory

Appendix II - U. S. States and Territories
Removed 1/20/2010
Download from valtabs.txt directory

Appendix JJ - Foreign Countries
Removed 1/20/2010
Download from valtabs.txt directory

Appendix KK - Type 10 Facial Image Edit Criteria
Removed 1/20/2010
See EBTS Type 10 Facial and Type 15 Palm Print Record Layout

1.0 INTRODUCTION

For nearly a century, fingerprinting has been the primary means of personal identification and during this period, the content, format, and quality of fingerprint cards has often been revised and refined. Yet, for the past fifty years, the basis for the exchange of fingerprint, identification, and arrest data between criminal justice agencies has been fingerprints captured using an ink process. Within the last ten years, however, technology has provided a new fingerprint capture method to replace the inked card process. This new technology enables live scan electronic capture of fingerprints.

The live scan system produces records by electronically scanning fingerprint images and capturing the images from live fingerprints. This process requires no ink and uses advanced electronics to ensure accurate image capture for better quality images. This technology has the potential to save time and effort at booking stations and to greatly improve the quality of post - arrest fingerprints. Live scan can also permit the timely identification of individuals at booking stations and applicant processing.

Live scan systems also represent the major input component for the electronic submission of images to the state and national identification systems of the future. The electronic interface allows a subject's fingerprint images to be transmitted to other sites within minutes. These electronic images are then received by a site's AFIS (Automated Fingerprint Identification System) and an automatic search is initiated to determine proper identification.

The live scan fingerprint image capture process features a continuous real time image preview capability that allows the fingerprint image to be displayed on the monitor before, during and after capture, providing immediate verification of the quality of the fingerprint captured. The operator rolls each finger on a flat lens platen for complete fingerprint image capture. An on - screen display of the fingerprint capture sequence helps the operator roll the individual's fingers in sequential order.

Previous live scan devices went directly from image capture to print processing. Print process involved a "clean - up" of images prior to printing and certain data concerning ridge boundaries and pores were eliminated as part of this clean - up process. Newer live scan models are designed to submit electronic images prior to print processing. The shift towards direct transmission of the captured image prior to print processing, allows for a more complete fingerprint image since valuable

fingerprint information such as ridge boundaries and pores are not eliminated as a result of the print process.

In the future, every image electronically submitted to the state must be compressed using the WAVELET Scaler Quantization Compression Algorithm. This algorithm consists of a class of encoders for converting source fingerprint image data to compressed image data; a decoder process for converting compressed image data to reconstructed fingerprint image data; and coded representations for compressed image data. (Refer **to WSQ specifications Appendix B**)

The WSQ compression algorithm was selected for it's compatibility with fingerprint data and GCIC will not accept uncompressed electronic images. The compression rate for fingerprint images will be 15:1, however, GCIC will accept electronic images captured with a compression rate of 5:1 for those devices certified at the Minimum Image Quality Requirement level established by the FBI.

2.0 STANDARDS

Live scan systems must comply with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications (IQS). IAFIS is developed according to standards which establish an infrastructure for the exchange of fingerprint identification information between local, state and federal users, and between those users and the FBI. To exchange fingerprint identification data effectively across jurisdictional lines or between dissimilar systems made by different manufactures, standards are needed to specify a common format for the data exchange. Therefore, live scan devices are required to meet the FBI's IAFIS standards and those amended by GBI to include the following.

- **The American National Standard Institute (ANSI/NIST) National Institute of Standards and Technology, Data Format for the Interchange of Fingerprint, Facial and other Biometric Information** (ANSI/NIST—ITL 1-2007)

  This document provides guidelines for the exchange of biometric information between various federal, state, local tribal and international AFIS systems.

- **Electronic Biometric Transmission Specification (EBTS),** (IAFIS-DOC-01078-9.0 November 30, 2009)

  This document specifies the file and record content, format, and data codes necessary for the exchange of fingerprint and biometric identification information between federal, local and state users and the FBI. It provides a description of all requests and responses associated with electronic fingerprint identification services. It also establishes error messages, specific compression algorithms for the exchange of fingerprint image information, and image quality assurance methods.

- **The WAVELET Scaler Quantization (WSQ) Gray Scale Fingerprint Image Compression Specification** (IAFIS - IC - 0110v2 February 16, 1993).

  Specifies a class of encoders for converting source fingerprint image data to compressed image data; a decoder process for converting compressed image data to reconstructed fingerprint image data; and coded representations for compressed image data.

- **Georgia Bureau of Investigation Live Scan Data Transmission Specification** (GBI June 1996).

  This document contains specifications that govern how live scan devices will electronically submit fingerprint and text data to the Georgia Bureau of Investigation's NIST File Collector (NFC).

- **Criminal Justice Information Services Security Policy Version 5.0 Standard Authentication (Password)** (2/9/2011)

  Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. Passwords shall:
  1. Be a minimum length of eight (8) characters on all systems.
  2. Not be a dictionary word or proper name.
  3. Not be the same as the Userid.
  4. Expire within a maximum of 90 calendar days.
  5. Not be identical to the previous ten (10) passwords.
  6. Not be transmitted in the clear outside the secure location.
  7. Not be displayed when entered.

3.0 LIVE SCAN DATA TRANSMISSION SPECIFICATION

3.1 Scope

This section contains specifications that govern how live scan devices will submit fingerprint and text data to the Georgia Bureau of Investigation NIST File Collector (NFC). The discussion is limited to software and procedural considerations.

3.2 Overview

Each live scan device will submit National Institute of Standards and Technology (NIST) format text and images to the GBI NFC using the File Transfer Protocol (FTP). Before a live scan device can connect to the NFC it will be provided with the following items:

- Device ID
- Group ID
- Password
- TCP/IP address
- Name of the Host to access (must use Domain Name Service)
- A maximum transmit packet size
- The name of the “common” partition to retrieve its environment file from.

When these data items are obtained, the live scan device will use the following procedure each time it initially connects to the network:

- On initial connection, verify that it has the latest versions of validation tables by retrieving files found in the common partition.
- Update tables on the live scan that are out-of-date by retrieving updated files found in the common partition.

- Retrieve and read an “environment” file in the common partition that contains the name of a partition to which submissions will be sent.

For each submission the live scan device will:

- Write the NIST data to the live scan device id directory.
- Write a signal file to a predefined directory.

After the NFC has recognized the submission and assigned a control number to it, the control number will be made available to the live scan device.

3.3 Data Transfer Using File Transfer Protocol (FTP)

Each live scan device submitting text and image data to the NFC will do so using the File Transfer Protocol across the Georgia Technology Authority (GTA) Router Network or via a secure encrypted Internet Protocol service. It is important that the live scan device utilizes a version of FTP software that allows for passive transfers via a firewall or proxy.

The NFC will make two types of disk partitions available through the FTP mechanism. The first type will be a common partition with read-only access. It will contain the latest versions of GBI data validation tables and environmental information that will tell live scan devices which partition to write their submissions to. The second type of partition will be used to receive submissions from the network. There will be only one common partition. There will be at least one submission partition. The number of submission partitions will depend on the workload.

Each live scan device will be assigned a unique three character device identifier that must be used in all submissions to the NFC. The device will also be assigned to a logical group and the group will be assigned to one of the FTP submission partitions. Each group will be assigned an unique four character group identifier.

The NFC will not mount any resources shared by the live scan device. It is, therefore, the responsibility of the live scan device to initiate all data transfers to the NFC and download all validation tables from the NFC. In general, data destined for the NFC will be copied by the live scan device to the FTP partition.

All text and image data submissions will be transmitted to the shared partition in accordance with the specifications found in the section “FTP Partition Layout”.

Copies of tables used by the live scan device to validate text data prior to submission will be made available in a FTP partition. It is the responsibility of the live scan device to examine the directory containing these tables and insure that the latest versions are downloaded. The live scan device will copy new tables from the FTP partition as needed. See “FTP Partition Layout” and “Validation Revision Control File” for details.

3.4 FTP Common Partition Layout

The name of the common partition, which is read-only, will be **/lscommon.**

The common partition will contain a LS Configuration File for each group of live scan devices. The LS Configuration File will contain one line of text that will be the name of the partition to which the devices in the group will write submissions. All of these files will be kept in a directory called **envfiles**. The name of the file will be the group id assigned to the live scan device.

For example, a live scan device assigned to group **abc7** will retrieve and read the contents of the LS Configuration File called **envfiles/abc7**. The first line of the file will contain, beginning in column one, the name of the partition to which the device will write its submissions.

Permissions on these files will be such that the live scan device will have access only to its own file. The purpose of these environmental files is to allow the NFC system administrator to manage the distribution of disk space usage on the shared partitions. The live scan device must read its environment file when it first connects to the network. The live scan device administrator will be notified in advance of any changes to the mount points.

The environment file contains the following three elements:

- Path to partition
- Minimum check interval in minutes
- Maximum check interval in minutes

The check interval dictates the minimum and maximum frequency in which the submitting device should check the out directory and POP3 mailbox for new messages.

The environment file should be checked upon initial connection to the NFC. If the device receives a shut down message, it should disconnect and recheck the environment file upon reconnect in case the information is changed between shutdown and restart. If the NFC is shut down, the device should connect to check for a restart status no more often than the last minimum check interval it had retrieved for the NFC. If the NFC still does not start, the device should disconnect again and check later.

The second directory will be used to distribute the latest versions of the data validation tables. This directory will be called **valtabs** and will be at the same level as **envfiles**.

The **valtabs** directory will contain a copy of each validation table and a control file that will contain the implementation date of the latest version of each validation table. The validation tables are to be downloaded daily at a minimum. The validation tables and the control file will all be stored as flat files with one line of text per entry.

The control file will be called **revcon.dta**. It will contain a header record consisting of a eleven (11) character current table set version number which is the implementation date and time of the table set (always a past date). The following lines will contain one line for each validation table. Each line will start with an eleven (11) character table version number consisting of the year, date, and time of implementation (always a past date) of the table and the name of the table beginning in column twelve (12). Each live scan device will be responsible for ensuring that it is using the latest version of each table. The year will be 0000-9999, date will be in Julian (001-366) format, time will be in hours and minutes based on a 24 hour clock. The **valtabs revcon.dta** file should be checked whenever the device makes an initial connection and the NFC is found to be running. It should then check no more often than the minimum check frequency and no less often than once a day. If the **revcon.dta** file indicates that devices tables are out of date, that

device should not submit a transaction until its tables are brought up to date.

In summary the common partition will be structured as follows:

/lscommon	start point of common partition
envfiles	directory containing assignment files
1a34	LS Configuration File for devices in group 1a34
nc01	LS Configuration File for devices in group nc01
	more partition assignment files
valtabs	directory containing current validation tables
revcon.dta	version control file

Example Tables

cnt.txt	contributing agency type table ***NOTE:*** *The **CNT** valtabs table is changing its format. The size of the agency name is changing from 30 characters to 45 characters. The city and state will shift to the right. The new format will be the following:* *ORI = 9 characters* *Agency Name = 45 characters* *City = 30 characters* *State = 2 characters*
rfp.txt	applicant type table
sex .txt	sex type table
rac.txt	race type table
eye.txt	eye color table
hai.txt	hair color table
offense.txt	offense type table
smt .txt	scars, marks, tattoos type table

cau.txt	caution type table
reject.txt	reject type table
mnu .txt	miscellaneous number type table
pob.txt	place of birth type table
purpose.txt	purpose code type table
state.txt	state type table
citizen.txt	citizenship type table
tot .txt	turned over to type table
type1 .txt	type 1 table
type1res .txt	type 1 response type table
cch .txt	cch field identifier type table
	remaining tables

3.5 FTP Submission Partition Layout

This section describes the layout of the submission partition.

In the event that the submitting device is a live scan store and forward concentrator with multiple live scan devices underneath, a group id will be assigned to that concentrator. The concentrator's individual live scan devices will be the only device subdirectories contained within that group id. Submitting of NIST text and image data will be the same as below, noting that the live scan store and forward must write the data to the proper live scan device subdirectory associated with the submission.

Each live scan device will be assigned to a group and each group will be assigned to each subdirectory on one of the FTP partitions dedicated to the live scan network. Each device in the group will be further assigned to a subdirectory beneath the group directory. From the NFC's point of view, the name of the subdirectory will contain the name of the mount point of the partition, the group identifier and the identifier assigned to the live scan device. For example, if the mount point is **/ls1** and the device id is **abc** and the

device assigned to group **def3** then the name of the subdirectory will be

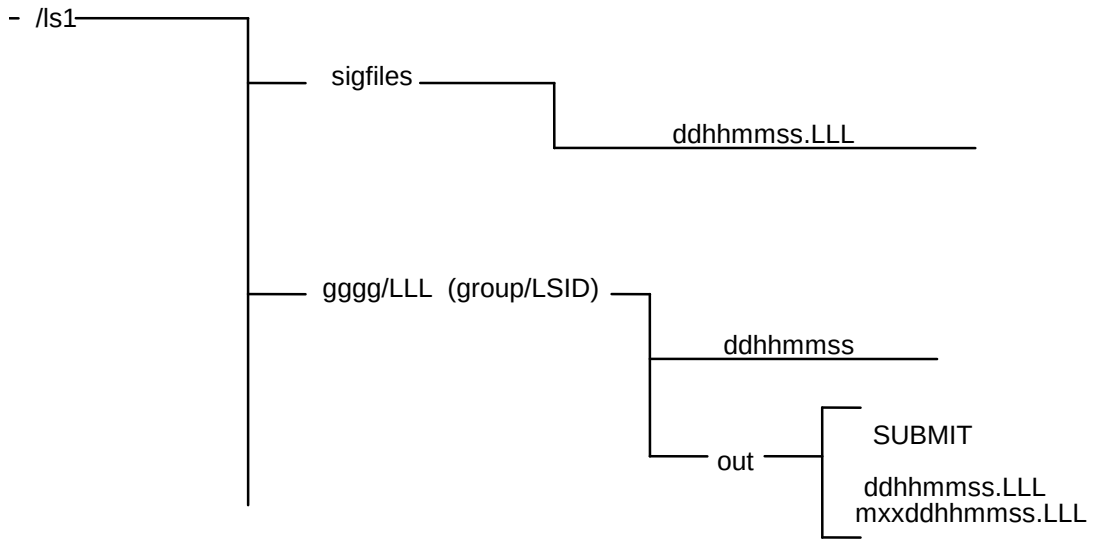
/ls1/def3/abc

This directory will be used to receive the NIST text and image data from the live scan device.

Signal files will be sent to indicate that a submission is ready for processing (See “Submitting Text and Images”). There will be one directory in each FTP partition to receive these signal files. This directory will be called **sigfiles**. The sigfile directory will be used by all devices assigned to that partition.

For example, using the mount point ls1 relevant directories would be:

/ls1/def3/abc	NIST text and image directory assigned to live scan device abc group def3.
/ls1/def3/123	NIST text and image directory assigned to live scan device 123 in group def3.
/ls1/rst7/jkl	NIST text and image directory assigned to live scan device jkl in group rst7.
/ls1/sigfiles	directory where all live scan devices assigned to partition ls1 will write signal files.



3.6 Submitting Text and Images

As part of the submission process, the live scan will check the out directories for the presence of a file named SUBMIT. The presence of this file indicates the live scan may submit NIST records to NFC. The absence of this file indicates that live scan may not submit NIST records. If live scan submits NIST records without the **SUBMIT** file present, the submissions will be ignored by NFC.

When the **SUBMIT** file is detected, the live scan device will copy the text and image set to the NFC in the FTP submission partition. The text and image set will be concatenated into a single file. The file name of the text and image set must be in the format of **ddhhmmss** to distinguish it from previously submitted records. After transmission of text and images is complete, the live scan device will copy a signal file to the partition's **sigfiles** directory.

Once NFC has received a transaction it will write an acknowledgement to the *out* file indicting the record has been received. Live scan will check the *out* file at a constant interval for an acknowledgment that the transaction has been received by NFC. If the acknowledgment does not appear in the *out* file after a maximum amount of time, the live scan will begin the

submission process again with the **SUBMIT** check and the generation of a new **ddhhmmss** file. It will be the responsibility of NFC to process and clean up any of these "orphaned" *sigfiles* and submission files. The default values will be one minute between checks and ten minutes total. All text and image data will be submitted in **NIST** format.

3.6.1 Text and Image File Name Set

At the time of submission, the device will create within its assigned device directory a NIST file using a name composed of the date and time of the submission. The format will be:

ddhhmmss

where

dd is the current day of the month,
hh is the hour based on the 24-hour clock,
mm is the minutes and
ss is the seconds.

3.6.2 Signal File Format

When transmission of the text and image set is complete, the device will create a signal file in the ***/*sigfiles** directory containing one character of data using a name composed of the time stamp of the submission and the live scan device id. The name of the signal file will be in the following format:

ddhhmmss.LLL

where

ddhhmmss is the name of the submission file and

LLL is the live scan device identifier.

3.6.3 Message Formats

Submission messages will be placed in the live scan "out" directory to be retrieved by the live scan using FTP as described in 3.6.3.2. All other messages will be sent to live scan devices by POP3 mail message.

3.6.3.1 POP 3 Mail Formats

All NFC to live scan mail messages will contain a header record composed of the following:

TO, FROM, SUBJECT, DATE/TIME

and a message record. The message record will contain identifying data items and possible "attachment" records. At the present time GBI has identified the following message record formats for POP 3 mail.

- **REJECT** (mrj)
- **IDENTIFICATION** (mid)
- **FBI IDENTIFICATION** (mfi)
- **FBI NAME SEARCH** **(**mfn)

Provided below are the POP 3 record layouts for both the header and message record formats:

- ***HEADER RECORD FORMAT***

TO:

FROM: tnetsystem@TNET02.GBITNET.local

SUBJECT: mrj, mid, mfi or mfn

DATE/TIME: YYYY/MM/DD HH:MM:SS

- ***REJECT MESSAGE FORMAT***

  TYPE: mrj

  LSTCN: Live scan TCN number

  GBITCN: TCN assigned by TNET subsystem

  DATE/TIME: YYYY/MM/DD HH:MM:SS

  NAME:

  RCODE: Return code numeric

  RLITERAL: Translation

  NOTE: Instructions from AFIS

- ***GBI IDENTIFICATION RESPONSE FORMAT***

  TYPE: mid

  LSTCN Live scan TCN number

  GBITCN: TCN assigned by TNET subsystem

  DATE/TIME: YYYY/MM/DD HH:MM:SS

  NAME:

  SID: State Identification number assigned by GBI

  OTN:

  OCA:

  IDENT: Record on File
  No Prior Criminal History information is available for this request.

- ***FBI IDENTIFICATION RESPONSE FORMAT***

  TYPE: mfi – FBI Identification Response *or* DHS Identification Response

  LS TCN: Live Scan TCN number

  GBI TCN:

  DATE/TIME: YYYY/MM/DD HH:MM:SS

  OCA: Originating Agency Case number

  FBI NUMBER: Federal Identification number assigned by FBI

  SID: State Identification number assigned by GBI

  NAME: Name identified from FBI master record

  FBI IDENT: Y or N

NOTE: *When an Applicant (APP) transaction is rejected from the FBI twice a pre-populated form will be sent back to the submitting agency via live scan. The agency staff will print out the form and manually submit to the FBI for a name search to be conducted.*

Therefore, a new FBI Reject message has been created to provide the agency the name search form. (See below)

- ***FBI NAME SEARCH RESPONSE FORMAT***

  TYPE: mfn

  LS TCN: Live Scan TCN number

  GBI TCN:

  DATE/TIME: YYYY/MM/DD HH:MM:SS

  NAME: Sent at time of request

  FBI Name Search form below:

FBI CJIS NAME SEARCH REQUEST FORM

Please complete the form below to request a FBI name check. Please be advised that an individual's fingerprints must be rejected twice for image quality prior to requesting a FBI name check.

ORI of State/Federal/Regulatory Agency: _____
Your Agency's Point of Contact (POC) for the Response: _____
Phone Number of POC: _____
FAX Number of POC: _____
Address of Requesting Agency: _____
_____
_____
Please FAX _____ or mail _____ my response to this request.

SUBJECT OF NAME CHECK

Transaction Control Number (TCN) of Subject's Fingerprint Submission: _____
Transaction Control Number (TCN) of Subject's Fingerprint Submission: _____
Name: _____ Alias: _____
Date of Birth: _____ Place of Birth: _____
Sex: _____ Race: _____ Height: _____ Weight: _____ Eyes: _____ Hair: _____
Social Security Number: _____ Miscellaneous Number: _____
State Identification Number: _____ OCA: _____

** Please note that highlighted fields are required for name check searches. **

Be sure to include the TCN from both rejected transactions.

FBI CJIS Division
ATTN: Name Check Request
1000 Custer Hollow Road
Clarksburg, WV 26306
FAX 304-625-5102

3.6.3.2 FTP Submission Record Formats

Provided below are the record layouts for the FTP record formats. The data elements may be in any order with the exception of the _ _ END_ _ line, which must be last. The device may send additional information in the sigfile besides SIGF:. Any additional information sent is not used by AFIS but will be echoed back with the acknowledgement and *mac* messages. Any additional information must appear before_ _END_ _ . Live scan will not honor any *out* file that does not have the_ _END_ _ marker present.

SIGNAL FILE

SIGF: ddhhmmss.LLL

_ _END_ _

Where

SIGF is the signal file name

_ _END_ _ is the end of file marker

ACKNOWLEDGMENT FILE

SIGF: ddhhmmss.LLL

TNETTCN:

ARV: ddhhmmss

SAN: nnnnnnnnnn

_ _END_ _

Where

SIGF is the signal file name

TNETTCN:

ARV is the arrival time (ddhhmmss)

SAN	is a unique NFC assigned acknowledgment number.
_ _END_ _	is the end of file marker

3.6.3.3 FTP Message Formats

When NFC completes processing of a NIST record or has a notification for the live scan device(s), a message file named **mxxddhhmmss.LLL** will be written into the *out* directory detailing the results. **mxxddhhmmss.LLL** refers to the following:

m	general file description **m** indicates a message file
xx	specific file description **ac** indicates a acknowledgment message **ad** indicates an administrative message
ddhhmmss	date and time message file was written to the *out* directory by NFC
LLL	live scan ID

There are currently two valid file types:

ACKNOWLEDGEMENT	(ac)	macddhhmmss.LLL
ADMINISTRATIVE	(ad)	maddhhmmss.LLL

The live scan device will find these messages in the *out* directory in the form of mxxddhhmmss.LLL.
The content of the message file will be identical to the initial *out* file (minus the END marker) with the following data elements added: RC, REG, TCN, MSG,_ _END_._ The data elements, except for the MSG line, may be in any order with the exception of the _ _END_ _ line which must be last. Live scan will not honor the message file unless the _ _END_ _ marker is present. The live scan device will delete each POP3 message and FTP file from the server after reading. **(See Appendices X, Y & Z for Message Codes)**

mac

SIGF: ddhhmmss.LLL

TNETTCN:

ARV: is the arrival time ddhhmmss

SAN: unique NFC assigned number

RC: code(s) from reject table

REG: time quick edit checks performed

NCN: internal order number

_ _**END**_ _ end-of-file marker

mad

RC: code from administrative table

MSG: description of administrative code

_ _**END**_ _ end-of-file marker

3.6.3.4 FLOW CONTROL

Flow control message files are intended to control the live scan NIST submission data flow. These messages will be delivered in the out directory detailing the condition in the form **mxxddhhmmss.LLL**. Currently valid file descriptions will be '**mad**' which indicates an administrative notification from NFC to a specific live scan or to all live scan devices. This '**mad**' message has a higher priority in processing than the '**mrj**' or '**mid**'. When the out SUBMIT file status is modified, a flow control message detailing the status change will be written detailing the reason for the SUBMIT change. The format of the flow control files will be: RC, MSG,_ _END_._ Live scan will ignore the flow control messages if the _ _END_ _ marker is not present. Live scan will delete the messages after reading.

The reactions of the live scan devices for each type of flow control message are defined in the following table:

NFC Message	NFC Situation	Live Scan Will	Return to Normal Message Expected	Live Scan Will Then
'mad' : A50 or A20 out/SUBMIT file removed.	NFC queue is full. No more NIST submissions can be received.	Stop Transmissions	'mad' : A00 or out/SUBMIT file added.	Resume normal transmissions
'mad' : A10	NFC queue is approaching full.	Slow down transmissions. Live scan will increase its out file check interval.	'mad': A00	Resume normal transmission rate
'mad': A90 out/SUBMIT file removed	NFC is shutting down	Stop transmissions	**'**mad': A00 or out/SUBMIT file added	Resume normal transmissions

3.7 Directory Schematic

The general structure of the FTP partition in diagram form appears below.

ls1	partition start point
sigfiles	directory for signal files from all devices assigned to this partition
nc2a	directory for group nc2a (individually connected livescan devices)

478	directory for live scan device 478
ddhhmmss	text and images for one submission
ddhhmmss	text and images for one submission
def7	directory for group def7 (livescan store and forward concentrator)
abc	directory for live scan device abc
ddhhmmss	text and images for one submission
ddhhmmss	text and images for one submission
123	directory for live scan device 123
ddhhmmss	text and images for one submission
ddhhmmss	text and images for one submission

3.8 File Definitions

Listed below are the various definitions of files that will interact with the live scan device. The order listed is the order encountered.

3.8.1 LS Configuration File

The LS Configuration File is a control file that contains data items that the live scan device needs to complete the connection to the NFC. This file will contain the name of the partition a live scan device will write its submissions to. Also contained will be maximum timer values for the purpose of checking for administrative messages from the NFC. The LS configuration file will contain only a single line with the data fields separated by commas and terminated with a new line character. There will be one file for each livescan group.

File name	-	/(lscommon)/envfiles/(livescan group id)
Contents	-	Sigfiles Partition, NIST Data Partition, Minimum Timer(minutes), Maximum Timer (minutes)↵
Sample file	-	/ls1/sigfiles, /ls1/gggg,1,10↵

3.8.2 Validation Revision Control File

The Validation Revision Control File contains the version number and implementation date of each validation table in the **valtabs** directory. As validation tables are to be updated, the date at which the file was replaced in the /(common partition)/valtabs directory will be entered into this file. The control file will be called **revcon.dta**. It will contain a header record consisting of the implementation date and time of the table set (always a past date). The following lines will contain one line for each validation table. Each line will start with a table version number consisting of the year (yyyy), date (Julian), and time (hhmm) of implementation (always a past date) and the name of the table beginning in column twelve (12). Each live scan device will be responsible for ensuring that it is using the latest version of each table.

File name	-	/(lscommon)/valtabs/revcon.dta
Contents	-	Implement Date Time(yyyyjjjhhmm) ↵ Date Time(yyyyjjjhhmm) table name↵
Sample file	-	19943321201↵ 19942551201 agency.txt↵ 19933310001 atyp.txt↵ 19941821201 booking.txt↵

3.8.3 New Submission Signal File to NFC

When transmission to the NFC of the text and image set is complete, the device will create a signal file containing one character of data using a name composed of the time stamp of the submission and the live scan device id. The name of the signal file will be in the following format:

ddhhmmss.LLL

Where

ddhhmmss is the name of the submission file

LLL is the live scan device identifier.

The actual contents of this signal file will be ignored. Only the name is important.

File name - /(partition)/sigfiles/(timestamp.livescan id)
Contents - one character
Sample Name - /ls1/sigfiles/29134327.478
Sample File - ↵

3.8.4 Re-Submission of Error Transactions

When the transmission of the text and image set is complete and errors have been detected an **" mrj"** message is returned to the submitting live scan device. The following procedures are to be performed:

- Correct the error(s)
- Use the same TCN number
- Create a new sigfile
- Resubmit transaction to NFC

3.8.5 Live Scan TCN Format

Listed below is the format for the live scan TCN number. This number consists of the following:

Live scan ID = 3 character field
Last number of the current year = 1 character field
Unique generated live scan number = 6 character field

Sample format:

0121000123

012 = LS ID
1 = last number of current year
000123 = unique generated live scan number

4.0 FUNCTIONAL SPECIFICATIONS

The following sections are designed to clarify basic requirements of the Live Scan function. An exhaustive listing of detailed requirements and functions is not provided and is beyond the scope of this section.

4.1 ELECTRONIC SUBMISSION - BOOKING PROCESS LOCAL AGENCY

1.0 Operator Logon

1.0.1 Enter operator id

1.0.2 Enter password

1.0.3 Logon correct?
= **Yes** GOTO 1.1
= **No** GOTO 1.0

1.1 Check NFC common partition for LS Configuration file
Check NFC common partition for Valtabs directory

1.1.1 Live scan revcon number = NFC revcon.dta file?
= **Yes** GOTO 1.2
= **No** Live scan checks NFC valtab tables
If NFC valtabs does not equal live scan valtabs
Download valtabs

1.1.2 Last table in valtab directory?
= **Yes** GOTO 1.2
= **No** GOTO 1.1.1

1.2 Operator enters arrest and demographic data at live scan, booking or case management system.

1.3 Data edits are performed on entered data.

1.3.1 Data edits correct?
= **Yes** GOTO 1.4
= **No** GOTO 1.2

1.4 Data sent to **(LIVE SCAN FINGERPRINT QUEUE)**

1.5 Select card type (criminal,applicant)

1.6 Select ORI/OAC number

1.7 Select subject's name from list or enter search parameters.

1.8 Demographic data screen appears with subject's

information.

1.8.1 Operator verifies data matches with subject.

1.8.2 Data OK?
= **Yes** GOTO 1.9
= **No** GOTO 1.7

1.9 Fingerprint screen appears

1.9.1 Roll finger

1.9.2 Fingerprints acceptable?
= **Yes** GOTO 1.9.3
= **No** GOTO 1.9.1

1.9.3 Last finger?
= **Yes** GOTO 1.10
= **No** GOTO 1.9.1

1.10 Check charges for GBI criterion offenses

1.10.1 GBI submission?
= **Yes** Print card for local agency
GOTO 1.11
= **No** Print card for local agency
END booking process

1.11 Demographic and arrest data reformatted into type 1 and type 2 records

1.12 Fingerprint data formatted into type 4 record using WSQ compression algorithm.

1.13 Live scan checks NFC *out* directory for SUBMIT file.

1.13.1 SUBMIT file present?
= **Yes** GOTO 1.14
= **NO** GOTO 1.13

1.14 Live scan sends record to gggg/LLL group id

1.15 Live scan writes to signal files.

1.16 Live scan checks *out* file

1.16.1 *Out* file present?
= **Yes** live scan deletes *out* file record
= **No** live scan increments check count

1.16.2 Check count = 10?
= **Yes** GOTO 1.13
= **No** GOTO 1.16

4.2 MESSAGE HANDLING

2.1 Operator reviews message

2.2 Print screen?
= **Yes** Message information sent to print server.
GOTO 2.3
= **No** GOTO 2.3

2.3 Operator clears message

2.4 Message type = Reject?
= **Yes** Select subject from list or enter search parameter
GOTO 2.5
= **No** **End**

2.5 Fingerprint error?
= **Yes** Operator re-rolls requested fingerprints
= **No** GOTO 2.6

2.6 Demographic error?
= **Yes** Operator corrects entry at live scan.
GOTO 2.7
= **No** GOTO 2.7

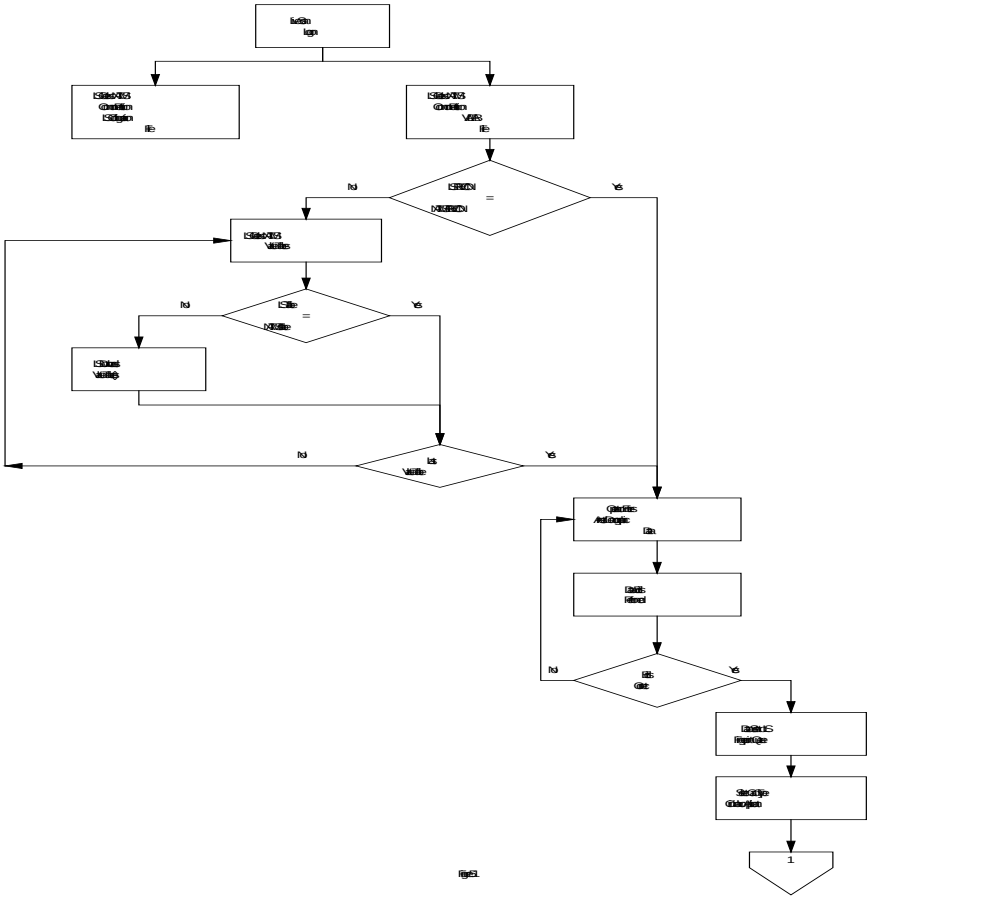
2.7 NIST error?
= **Yes** resend transaction
GOTO 2.8
= **No** GOTO 2.8

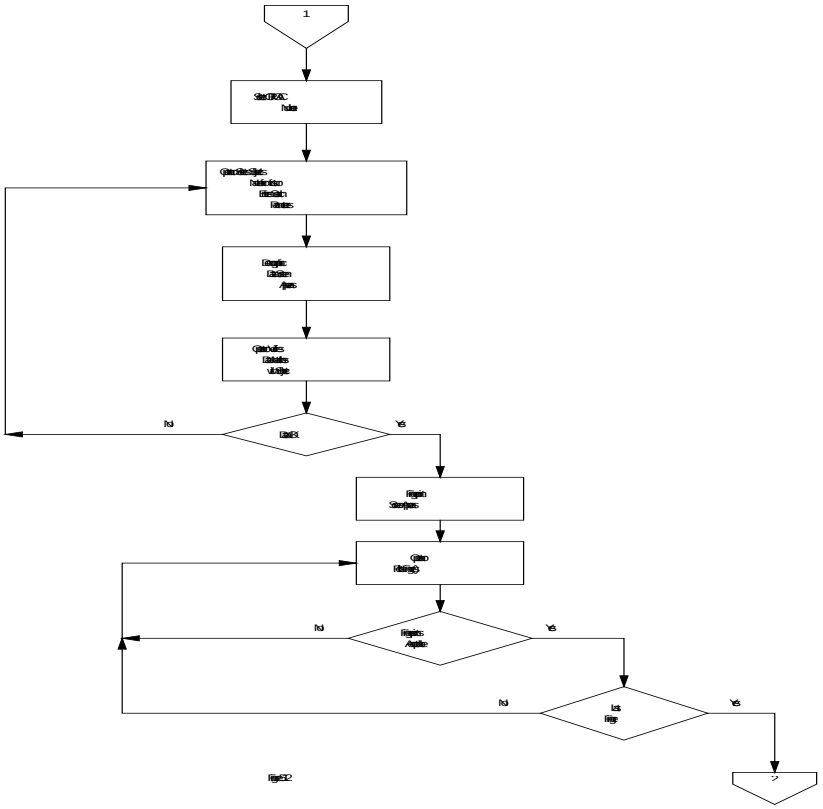
2.8 Demographic, arrest and fingerprint data formatted into Type 1, Type 2 and Type 4 records.

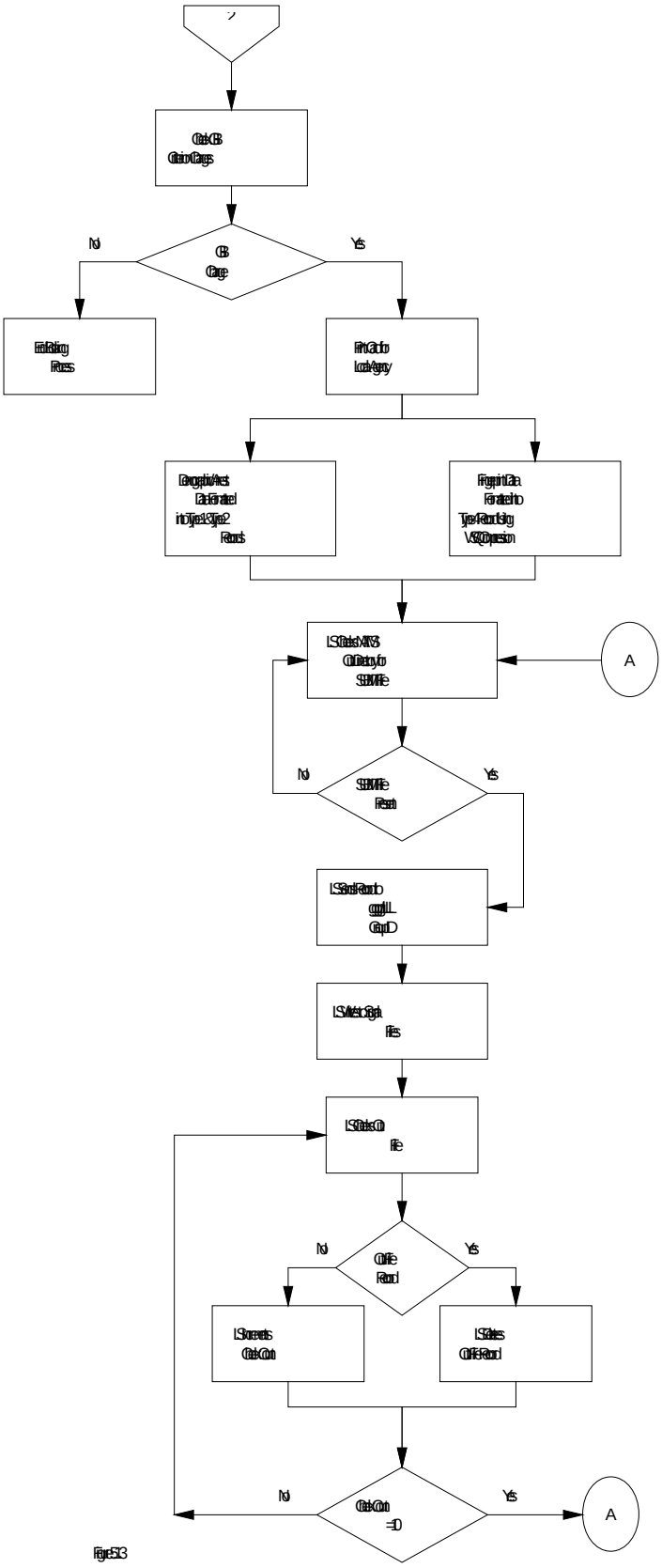
2.9 Type 1, Type 2 and Type 4 records sent to agency's NFC submission partition for device.

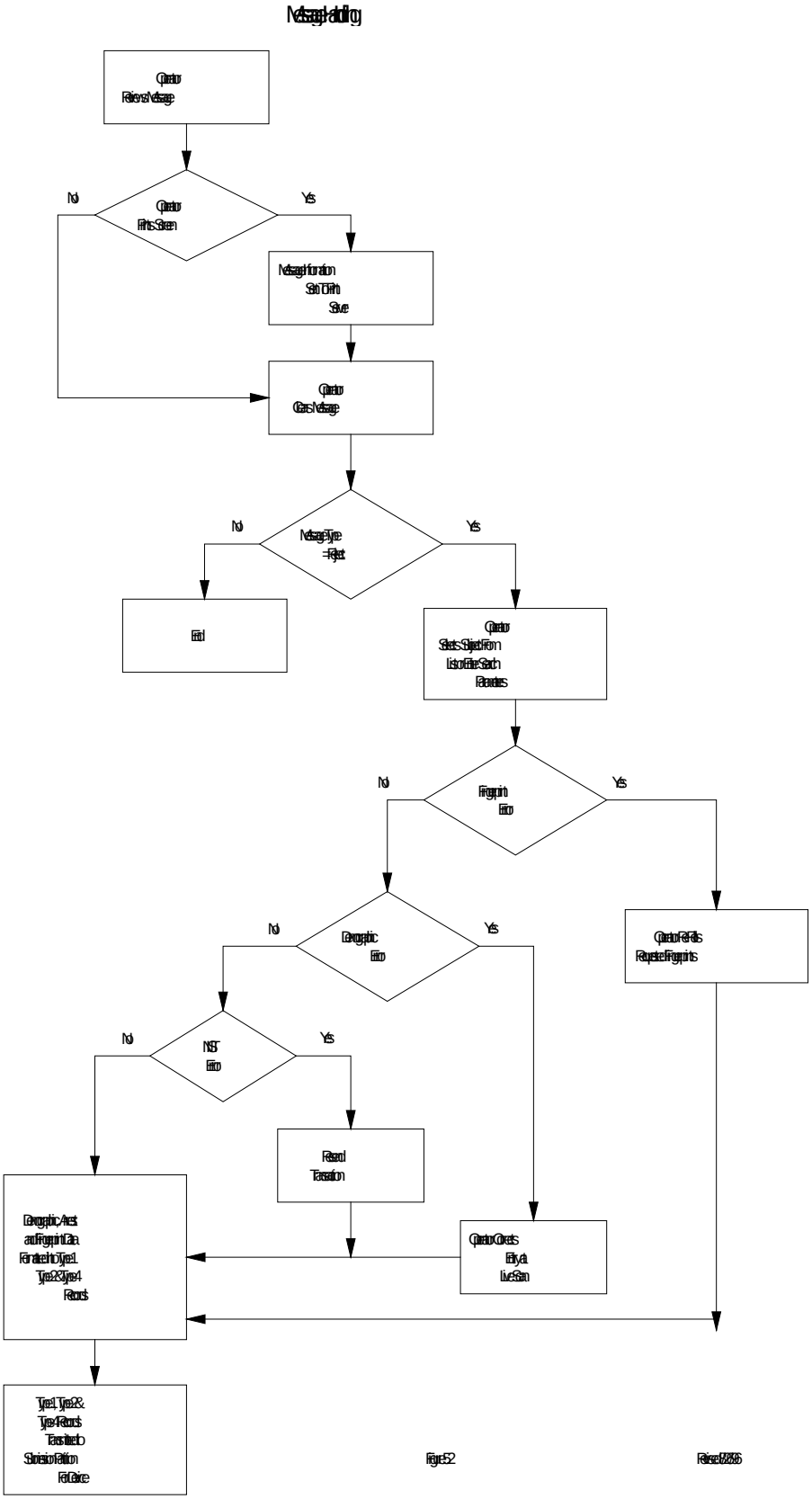
5.0 LIVE SCAN WORKFLOW

This section represents the Live Scan system workflow.






No
Yes
A
No
Yes
No
Yes
No
Yes
A



6.0 NETWORK INTERFACE SPECIFICATION

6.1 INTRODUCTION

Law enforcement agencies throughout the state of Georgia will soon be able to take advantage of Georgia's upgraded Automated Fingerprint Identification System (AFIS) by installing new live scan devices or upgrading current live scan systems.

Benefits from the new live scan device include better quality fingerprints for tenprint and latent searching, faster processing and response for booking of offenders and improved identification capabilities throughout the state. Installation of the enhanced live scan devices will coincide with the upgrade of the State of Georgia's AFIS.

Current live scan devices are not equipped to support the format and electronic transmission of fingerprint images, demographic data or arrest data as defined in the National Standard for Fingerprint Image Transmission.

The updated live scan device will utilize the Georgia Technology Authority (GTA) Network and/or via the Internet for communications between the local law enforcement agency and the GBI's NIST File Collector (NFC). The NFC is the component of the AFIS that stores, processes and routes fingerprint image data, criminal history update information and search results.

The Network Interface Specification uses widely available Internet protocols. Most of the protocols mentioned in this document are used in open systems. The FTP protocol is designed to be portable across different hardware platforms, operating systems, network architectures and allows for passive transfers via a firewall or proxy. The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol. The Internet Protocol (IP) provides for transmitting blocks of data called data grams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses.

The Internet protocol also provides for fragmentation and reassembly of long datagrams. The Post Office Protocol - Version 3 (POP3) is intended to permit a workstation to dynamically access a maildrop on a server host. POP3 protocol allows a workstation to retrieve mail that the server is holding for it.

The wide spread availability of software and hardware supporting the above protocols should ease the Live Scan vendor's and local agencies' burden in establishing a connection to the Georgia AFIS.

6.2 Types of Protocol

- FTP
- TCP
- IP
- POP3

6.3 LAN Connection

IEEE 802 LANs
- 802.2 Ethernet (Common To All)
- 802.3 (CSMA)

6.4 Network Cabling

- 10 BASE 2
- 10 BASE T

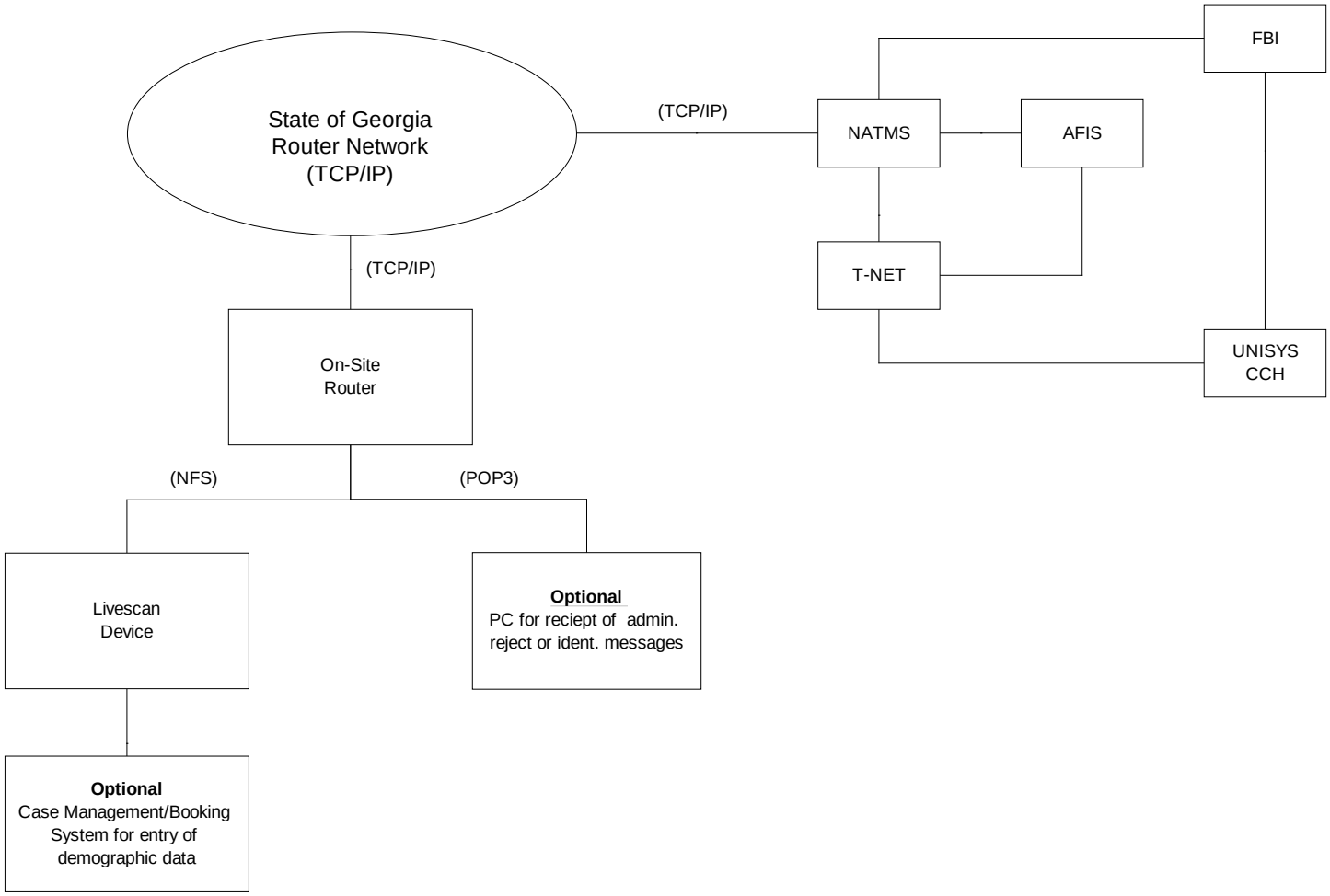
6.5 Transmission

- 56KB (minimum)

6.6 Routers
- 6611 IBM
- 2210 IBM

6.7 Network Interface Workflow

This section represents the Network Interface workflow.



Network Specifications Interface Flowchart

Figure 6.1

APPENDIX D

Please refer to EBTS Type 1 and Type 2 Record layouts for the maximum number of BYTES including character separators and field number for each.

APPENDIX E

APPENDIX F

APPENDIX G

APPENDIX H

APPENDIX I

APPENDIX J

APPENDIX K

APPENDIX L

APPENDIX M

APPENDIX N

APPENDIX O

APPENDIX P

APPENDIX Q

APPENDIX R

APPENDIX S

APPENDIX T

APPENDIX U

APPENDIX V

TRANSLATION TABLE FOR TOT TYPE 1 TRANSACTIONS

CAR	Criminal Ten-Print Submission (Answer Required)
CNA	Criminal Ten-Print Submission (No Answer Required)
JUV	Juvenile
APP	Applicant Submission
SOT	Search Only
COR	Corrections
JCOR	Juvenile Corrections

APPENDIX W

TRANSLATION TABLE FOR TOT TYPE 1 RESPONSES

SRE	Submission Results - Electronic
ERRT	Transaction Error

APPENDIX X

ADMINISTRATIVE MESSAGE CODE TABLE

Type	Code
mad	A000: Resume transmission
	A010: Reaching input limit
	A020: Stop transmission
	A050: NFC queue is full
	A090: NFC shutting down

APPENDIX Y

Offender Tracking Number (OTN) and State Identification number (SID) Format

OTN is an numeric 11 character field with the 11th character being a check character. The 11th character is the remainder after dividing the first 10 characters by 7.

Sample format:
46385835 = 4638583 divided by 7 leaves a remainder of 5 (the last character).

SID is an alphanumeric 8 character field. SID numbers less than 1075000 must be numeric right justified, zero filled. All SID numbers greater than 1074999 require a check character may be alphabetic. If the 8th character is alphabetic, a check character must be determined as follows:

Multiply position	1	by	2	giving	A
	2	by	7	giving	B
	3	by	6	giving	C
	4	by	5	giving	D
	5	by	4	giving	E
	6	by	3	giving	F
	7	by	2	giving	G

To determine the check character add 39 + A + B + C + D + E + F + G = SUM.
Divide the SUM by 11 giving a remainder.
The remainder corresponds to the following check characters:

Remainder:	0	1	2	3	4	5	6	7	8	9	10
Character:	A	E	H	J	K	L	M	P	T	W	X

Example: SID / 2090187P

2 * 2 = 4
0 * 7 = 0
9 * 6 = 54
0 * 5 = 0
1 * 4 = 4
8 * 3 = 24
7 * 2 = 14
100 + 39 = 139/11= 12 remainder 7 = P

APPENDIX Z

ACKNOWLEDGEMENT MESSAGE CODE TABLE

Type	Code
mac	0000 Positive 0001 Unreadable/not accepted (list may be expanded)

APPENDIX HH

APPENDIX II

APPENDIX JJ

APPENDIX KK

TYPE 10 FACIAL and TYPE 15 PALM PRINT IMAGE SPECIFICATIONS

Please refer to;

Type 10 Facial and Type 15 Palm Print Record Layout; NIST Special Publication 500-271; ANSI/NIST – ITL 1-2007, American National Standard for Information Systems, Data Format for the Interchange of Fingerprint Facial and Other Biometric Information Part 1; National Institute of Standards and Technology

Criminal Justice Information Services (CJIS) Electronic Biometric Transmission Specification (EBTS) IAFIS-DOC-01078-9.0 (November 2009)