This refers to NGI copying data from its repositories to removable media.

Department of Justice

Federal Bureau of Investigation

NEXT GENERATION IDENTIFICATION

(NGI)

SYSTEM REQUIREMENTS DOCUMENT

VERSION 4.4

Ocotober 1, 2010

CJIS Document Number - NGI-DOC-01185-4.4

Prepared By:

332 P95

Federal Bureau of Investigation
Criminal Justice Information Services Division
1000 Custer Hollow Road
Clarksburg, WV 26306

This Page Intentionally Left Blank

CHANGE HISTORY SECTION

Version/ Revision	Revision Date	Description of Change	QA Approved	Date
1	11/3/2006	Release for internal FBI review of legacy requirements.		
1.0b	11/9/2006	Baseline for IntelliDyne SRD DCN of legacy requirements.		
1.0d	12/20/2006	Updated to incorporate NGI Initiative Functional Requirement Documents (FRD).		
2	2/9/2007	Updated to incorporate NGI FRDs, Biometric Interoperability Program Office FRD Version 2.0, and International Terrorist File FRD.		
2.1	3/2/2007	Updated to incorporate SRD Version 2.0 formal comments.		
4	5/4/2007	Incorporated SRR changes (Version 3.0) with Biometric Interoperability Program Office FRD Version 3.1.		
4.1	2/13/2008	Updated to incorporate: NPPR 6a - Requirements changes based on Due Diligence preparation and IV&V comments NNPR 6b – IAFIS Build 8.2 SPCRS 26510z and 27815. NPPR6d – Updates to NGI resulting from IAFIS SRD Updates for IAFIS Sys Spec Revision.		
4.2	7/7/2008	Updated to incorporate: NPPR 38 – "Update NGI SRD with consistent verb usage" NPPR 41 – "Update NGI SRD with findings from the RTIE team's use case creation" NPPR 42 – "Additonal requirements for Verification Service in NGI SRD"		

		NPPR 43 – "NGI SRD – Add new QuickWin requirements for Build 9.0 Expanded ULF Serach Phase 1" NPPR 45 – " NGI SRD – Add new QuickWin requirements for additional biometrics storage" NPPR 50 – "Update NGI SRD with "As Is" iDSM requirements." NPPR 56 – "Update NGI SRD to change all "IAFIS shall" statements to "NGI shall" NPPR 57 – "Update NGI SRD with "tenprint" and "palmprint" NPPR 66 – "Update "IAFIS" to "NGI" in the NGI SRD supporting Text"		
4.3		NPPR 86c – "NGI QuickWin - Receive and Store 1000ppi Tenprint Transactions" NPPR 86d – "Verb Appendix F" NPPR 86g – "NGI SRD Rqmt Updates/Changes per SCN (NGI-SCN-INC10001)" NPPR 86h – "NGI SRD Text Updates/Changes per SCN (NGI-SCN-INC10001)" NPPR 86j – "Update Bibliography Appendix C" NPPR 86k – "Workload Tables Updates" NPPR 86m – "Map Legacy Rqmts to NGI SRD" NPPR 86v – "Change 3 security requirements from Functional (SFR) to Non-Functional (SNFR) based on Security Clarification reqmt review" NPPR 86w – "New iDSM NGI SRD subsections need to follow standardized naming conventions" NPPR 86ab – "Update SRD PalmPrint and Supplemental Fingerprint and Palmprint Workload Assumptions regarding biometric updates"		

		NPPR 86ae – "NBRP Revised Workload Estimates"		
4.4		NPPR 101c – "NGI SFR1586 & SFR461 Text" Correction" NPPR 101e – "Remove palmprint to palmprint search services from SRD 4.4 baseline - Text Updates/Deletes/Changes" NPPR 101f – "Remove palmprint to palmprint search services from SRD 4.4 baseline - Requirement Updates/Deletes/Changes" NPPR 101g – "Interoperability ICA Final with Signatures to be added to Interoperability Joint CIL - Requirement/Updates/Deletes/Changes" NPPR 101i – "Modification to the NGI SRD for Fingerprint Image Replacement request - Text Updates/Deletes/Changes" NPPR 101j – "Modification to the NGI SRD for Fingerprint Image Replacement request - Requirement Updates/Deletes/Changes" NPPR 101k – "CPI Message Processing Functionality - Requirement Updates/Deletes/Changes" NPPR 101l – "CPI Message Processing Functionality - Text Updates/Deletes/Changes" NPPR 101m- "New Business Requirements - Notifications to U.S. Immigration and Customs Enforcement (ICE) Law Enforcement Support Center (LESC) Requirement Updates/Deletes/Changes" NPPR 101n – "New Business Requirements - Notifications to U.S. Immigration and Customs Enforcement (ICE) Law Enforcement Support Center (LESC) Text/Deletes/Changes"		

		NPPR101o – "[LMCO PR 1044] IDFP RISC Response Time requirement not attainable, Requirement needs to be modified (IDFP 049 in MT SOW)" NPPR101p – "Add IAFIS External Subject Search new capability to NGI requirements - Text Updates/Deletes/Changes" NPPR101q – "Add IAFIS External Subject Search new capability to NGI requirements - Requirement Updates/Deletes/Changes" NPPR101u – "Change Title of LFIS and LFFS to use Friction Ridge instead of Fingerprint" NPPR101v – "Add cascaded searches and advise for the Supplementals in the Identification Threads" NPPR101w – "Remove palmprint composite requirements related to the storage of palmprint composite images SRD" NPPR101x – "Remove Palmprint and Supplemental Fingerprint and Palmprint Decisions from SRD 4.4 Baseline - Text Updates 4.4 baseline" NPPR101y –"Remove Palmprint and Supplemental Fingerprint and Palmprint Decisions from SRD 4.4 Baseline - Requirement Updates" NPPR101z –"Delete the Biometric Delete Notification Requirements – SRD" NPPR101ab –"Add cascaded searches to the Verification Service thread" NPPR101ac –" Update to SRD Workload Tables"NPPR101ad –" Interoperability 10 Second Search of the CMF" NPPR101ae –" Interoperability 10 Second Search of the CMF - Text Updates/Deletes/Changes" NPPR101af – "TCN to FNU Conversion for Interoperability"		

		NPPR101ag – "Update/delete all requirements related to returning a composite for either palmprints or supplemental fingerprints and palmprints. NGI will return the most recent as the default." NPPR101ai – "Add EIHR requirements to the NGI SRD – review IAFIS SRD Functional Requirement FR667" NPPR101aj –"Updates to the NGI SRD as a result of the Latent Fingerprint / Palmprint Trade Study" NPPR101ak –"Remove cascaded searching of the ULF from the Latent threads"		

This Page Left Intentionally Blank.

TABLE OF CONTENTS

LIST OF TABLES

This Page Left Intentionally Blank.

1 INTRODUCTION

The FBI has a family of automated systems that support the capability to provide identification, verification, information, investigation, notification, and data management services to criminal justice and authorized non-criminal justice users. The Criminal Justice Information Services (CJIS) Division System of Services (SoS), located in Clarksburg, West Virginia, includes the National Crime Information Center (NCIC), the National Instant Criminal Background Check System (NICS), and the Integrated Automated Fingerprint Identification System (IAFIS). Together, these systems form an integrated approach to providing customer information and services that support the detection and reduction of domestic and international terrorist, and criminal related activities.

The NCIC system maintains a national index to document theft reports, warrants, and other criminal justice information submitted by law enforcement agencies from across the country. It provides law enforcement with access to criminal justice data pertaining to crimes and criminals of national interest.

The NICS system is a national system that provides authorized users with information about persons who may be prohibited by federal or state laws from owning or receiving a firearm. NICS ensures national security and public safety by providing the timely determination of a person's eligibility to possess firearms or explosives in accordance with federal law.

The IAFIS provides an up-to-date, integrated system to respond to the needs of the local, state, tribal, federal, and international criminal and authorized non-criminal justice agencies. It houses the largest collection of digital representations of fingerprint images, features from the digital fingerprint images, and associated criminal history information in the world. Collectively, this data comprises the biometrics, content, format, and units of measurement for the electronic exchange of information that may be used for the fingerprint identification of a subject. The current IAFIS, implemented in July 1999, allows the standard electronic submission of fingerprint identification data to the FBI.

The IAFIS provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses 24 hours a day, 365 days a year, in support of thousands of law enforcement organizations and background checks for hundreds of civil agencies. The system, which contains more than 51 million criminal subjects, provides an "open-set" identification of submitted fingerprints, which are checked against all known criminals in relevant portions of the database, normally within two hours of an electronic criminal request and within 24 hours of an electronic civil fingerprint submission. Each day, approximately 7,000 new records are added to the database.

The mission of government in today's global society demands more robust identification solutions that can be deployed on an increasingly large scale. Systems such as the IAFIS are crucial for national security and homeland security in addition to supporting law enforcement agencies. The defense and intelligence communities require automated methods capable of rapidly determining an individual's true identity, as well as previously used identities and past activities. Fusion and distribution of MultiModal biometrics and other contextual information can augment human interaction when a confrontation

occurs with an unknown individual in a hostile or controlled setting. Depth of knowledge and real-time access to these data sets make biometrics a significant force multiplier and precision weapon in U.S. national security operations. The defense and intelligence communities recognize the need to enable matching and searching capabilities for multiple biometric modalities. The use of multiple biometrics requires increases in capacity and throughput while maintaining data integrity and improvements in recognition algorithms.

Homeland security and law enforcement communities require technologies to secure the U.S. borders and to identify criminals in the civilian law enforcement environment. At the same time, any solution must also seek to maintain international relations, ensure smooth passage of legitimate visitors and commerce, and provide confidence in the identity and credentials of those given local or national trust.

The FBI continues to improve existing technology in order to provide the most reliable and accurate information possible. To remain responsive to law enforcement and other customer needs, and given the advances in fingerprint identification technology, it is essential that enhancements be made to the IAFIS.

The Next Generation Identification (NGI) Program introduces new capabilities to reduce terrorist and criminal activities by improving and expanding biometric services to its users, provides the infrastructure to support interoperability with authorized external agencies for external searches, and provides additional repositories for external searches.

The NGI Program incorporates into IAFIS the six core initiatives listed below:

- Advanced Fingerprint Identification Technology (AFIT)
- Quality Check Automation (QCA) Phase III
- Interstate Photo System (IPS) Enhancements
- Disposition Reporting Improvements (DRI)
- Enhanced IAFIS Repository (EIR)
- National Palmprint System (NPPS)

These six core initiatives in addition to the legacy IAFIS functionality will comprise the NGI System. Based on the long term vision of DOJ/FBI to make NGI fully interoperable with other biometric systems, the Biometric Interoperability Program incorporates enhancements to enable interoperability with the Department of Homeland Security (DHS).

Within DHS, the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program supports key immigration and border management processes across agencies. These processes include creating new capabilities to biometrically verify the identities and monitor border crossings of foreign visitors and immigrants. The Automated Biometric Identification System (IDENT) system, operated by US-VISIT, is the core technical component of this biometric capability.

Interoperability is being managed as two projects and deployed in three phases. The projects are Shared Services, which is fully described within this document, and Shared Data, which encompasses the first phase of interoperability. Phase one of deployment is the interim Data Sharing Model (iDSM), which was deployed on September 3, 2006 and provides a short-term interoperability solution with a reciprocal exchange of biometric data subsets between IDENT and IAFIS. Phase two is the Initial Operating

Capability (IOC), which provides incremental enhancements for both projects. The third phase is the Full Operating Capability (FOC), which will deploy after IOC is completed (tentatively projected for FY 2010) and represents the final information sharing enhancements necessary to support interoperability.

Full information sharing between these two systems (and among other relevant systems) will offer a multitude of benefits to DHS, DOJ, and other stakeholder agencies. DHS access to criminal history files would facilitate improved decisions regarding an individual's admissibility, eligibility of immigration benefits, and deportability from the United States. Expanded DOJ access to DHS data will enhance the ability to develop comprehensive histories and threat profiles of individuals and to share immigration information with stakeholders. Access to systems will be governed by applicable laws and policy. Additionally, improved interoperability will enhance the mutual effort to identify and apprehend high-risk terrorist and wanted individuals.

Additionally, the CJIS Global Initiatives Unit (GIU) provided the vision for new NGI capabilities to support an International Terrorist File Shared Services and Data Exchange initiative that supports identification searches with multi-tiered responses.

1.1 Purpose of Document

This document, the NGI System Requirements Document (SRD), defines the user, functional, and operational requirements for the system identified as the Integrated Automated Fingerprint Identification System. These requirements will provide the core NGI User Services to the communities served by the FBI.

The requirements contained within this document are intended to be free from design considerations unless there are compelling reasons to constrain the design. Also included are workload and performance requirements for the overall system through the year 2012.

1.2 Background

The CJIS IAFIS, one of the largest fingerprint identification systems in the world, has been instrumental in meeting the fingerprint identification needs of the law enforcement and non-criminal justice communities. Since IAFIS FOC in July 1999, it has provided automated Tenprint and latent identification and criminal history data for both civil and criminal needs. Continuous improvements and upgrades since then have provided unprecedented increases in system performance, search reliability, throughput and response times.

The tragic events of September 11, 2001 transformed the direction of the FBI and the law enforcement community, and highlighted the need for reliable and rapid identification of individuals and the capability to provide and share criminal information across agencies. The adoption of Homeland Security legislation and other national security legislation has spawned the implementation of additional IAFIS services to improve homeland and border security, enhance transportation safety and security, and increase information sharing.

1.3 System Objectives

NGI objectives are as follows:

- *Provide accurate and timely services to user agencies*: The FBI provides vital services to support law enforcement agencies and other users nationwide. To accomplish this mission, the FBI's automated systems must supply critical information in a timely manner.
- *Support a paperless environment*: Transactions received from and sent to other organizations, as well as internal FBI transactions, will be electronic to the maximum extent feasible. Since not all external organizations will be fully automated, some paper will continue to be received. Incoming fingerprint cards and documents received in paper form will be converted to digital image form and processed electronically upon receipt.
- *Enable the FBI to process a significant growing workload without increasing staff*: The pressures on the federal budget dictate the use of high performance automation and work re-engineering to cope with increasing workloads.
- *Increase the number of crimes solved by providing enhanced identification and investigative services*: The improvement of both the Tenprint and latent capabilities will assist law enforcement agencies in solving more crimes.
- *Provide options for NGI participation to international, federal, state, tribal, and local agencies*: Each option will provide users with access to a different predefined level of NGI technical capability, so that each agency can choose the option best suited to its needs. Agencies may continue to mail Tenprint cards and documents to the FBI for processing, or take full advantage of electronic data transmission and access a greater number of NGI capabilities.

1.4 Organization of Document

Following this introduction, Section 2 describes the core NGI user service requirements, Section 3 describes the functional requirements, and Section 4 contains a description of workload, performance, security, and other non-functional requirements. A bibliography is provided at the end of the document.

2 USER SERVICE REQUIREMENTS FOR NGI

The FBI provides user services to: (1) authorized customers located at law enforcement and criminal justice agencies, (2) others that have an authorized non-criminal justice purpose, and (3) FBI staff members who are identified as Authorized FBI Service Providers.

There are six core NGI services to be provided to these users. The NGI user requirements identified below have been listed by these six categories.

2.1 Identification Services

The Identification Service provides a positive identification or non-identification of an individual based on a one-to-many biometric search. This includes Tenprint Fingerprint Identification Searches, Latent Identification Searches, Repository for Individuals of Special Concern (RISC) Rapid Searches, ITF Identification Searches, and Disposition Fingerprint Identification Searches. NGI may return a reject response if the submission fails to satisfy processing criteria.

Fingerprint Identification user requirements are defined as follows:

NGI shall support Tenprint Fingerprint Identification Search requests.

Tenprint searches may be submitted in hardcopy, or electronically in accordance with the latest Electronic Biometric Transmission Standard (EBTS). NGI processing of these searches includes system and service provider functionality such as Automated Quality Check (AQC), Fingerprint Sequence Check (FSC), Automated Sequence Check (ASC), Fingerprint Image Comparison (FIC), Latent Fingerprint Image Comparison (LFIC), and error conflict resolution. Fingerprint submissions may be processed by internal Tenprint or Latent Service Providers who may choose to manually generate an identification, non-identification, or rejection response in reply to the request.

NGI shall support Tenprint Fingerprint Identification Searches against designated NGI repositories.

NGI shall support Tenprint Fingerprint Identification Searches against designated external repositories (e.g., IDENT).

NGI shall support a Tenprint Fingerprint Identification Search from an Authorized External System (e.g., IDENT) against designated NGI repositories.

NGI shall support photos as part of a Tenprint Fingerprint Identification Search response from an External System (e.g., IDENT), when requested.

NGI shall support Tenprint Fingerprint Identification Search requests against shared data records.

Tenprint Fingerprint Identification Search requests against shared data records contained within iDSM may only be submitted by Authorized Participating Shared Data Agencies.

Deleted.

NGI shall support prioritized Tenprint Fingerprint Identification Searches.

NGI shall support AQC for Tenprint Fingerprint Identification Searches.

NGI shall enroll fingerprints into designated repositories as part of Tenprint Fingerprint Identification Searches.

Deleted.

NGI shall enroll an Identity as part of a retained Tenprint Fingerprint Identification Search.

NGI shall enroll photos as part of a Tenprint Fingerprint Identification Search.

NGI shall enroll palmprints as part of a Tenprint Fingerprint Identification Search.

NGI shall enroll iris data as part of a Tenprint Fingerprint Identification Search.

NGI shall enroll a Rap Back Subscription as part of a Tenprint Fingerprint Identification Search.

NGI shall enroll Identity Theft Victims as part of a Tenprint Fingerprint Identification Search.

NGI shall enroll supplemental fingerprint and palmprint information as part of a Tenprint Fingerprint Identification Search.

NGI shall support the linking of NGI and External System (e.g., IDENT) records as part of a search.

Linking of NGI and External System records will occur when NGI or the External System enrolls a new identity or receives higher quality fingerprints for an unlinked record.

Deleted.

Deleted.

Deleted.

NGI shall support Identity maintenance as part of a Tenprint Fingerprint Identification Search.

NGI shall provide an appropriate response to a Tenprint Fingerprint Identification Search request.

A response may include Identity History (i.e., criminal, civil) relevant to the identified subject. NGI may provide an electronic or printed response, as requested by the submitter of the request.

NGI shall provide wanted person information with the Tenprint Fingerprint Identification Search response.

NGI shall provide flash information with the Tenprint Fingerprint Identification Search response.

NGI shall provide sex offender registry information with the Tenprint Fingerprint Identification Search response.

NGI shall provide Identity Theft information with the Tenprint Fingerprint Identification Search response.

NGI shall provide a photo with the Tenprint Fingerprint Identification Search response, when requested.

Deleted.

NGI shall support a Hot Check Name Search of the NCIC persons' files for Tenprint Fingerprint Identification Searches.

As part of a Hot Check Name Search, NCIC will compare the submitted Tenprint fingerprint search request biographic data to the NCIC Wanted Person File and the terrorists records contained within the NCIC Violent Gang and Terrorist Organization File (VGTOF). NCIC may provide notifications of hits to the NCIC record owner(s).

NGI shall support electronic disposition submissions using fingerprints.

NGI will allow authorized Contributors to submit disposition requests with fingerprints to identify the associated subject.

NGI shall support Latent Fingerprint Identification Search requests.

Latent Fingerprint Identification Search requests will be submitted electronically in accordance with the latest EBTS.

NGI shall support Latent Fingerprint Identification Searches against designated repositories.

NGI shall provide an appropriate response to a Latent Fingerprint Identification Search request.

Latent Fingerprint Identification Searches will be processed by FBI Latent Service Providers who will provide identification, non-identification, inconclusive, or rejection response in reply to the request.

NGI shall support RISC Rapid Searches.

The RISC Rapid Search functionality provides the capability to perform an identification search against a limited population with a significantly reduced response time.

NGI shall support International Terrorist Identification Searches.

NGI shall support enrollment into the ITF.

2.2 Verification Services

The Verification Service provides a confirmation of an Identity based on a one-to-one comparison.

NGI shall verify the Identity of an individual using fingerprints.

NGI shall verify the Identity of an individual using fingerprints provided by an External System (e.g., IDENT).

2.3 Information Services

The Information Service supports user requests for biographic and/or biometric information for a specific individual.

NGI shall support the retrieval of fingerprint and supplemental fingerprint and palmprint information associated with an Identity.

NGI shall support the retrieval of Identity History information.

NGI shall support the retrieval of a photo on an Identity History request.

NGI shall provide external system link identifiers as part of Identity History responses.

Deleted.

Deleted.

Deleted.

Interstate Identification Index (III) participating states will submit all arrest fingerprints to the FBI for processing. The FBI will maintain a copy of the criminal history for III states, although the state may have a more complete history. For the purpose of criminal Tenprint Fingerprint Identification Search responses, the FBI will use its copy of a III state's criminal history.

When external criminal history requests (QR messages) are done for criminal or national security purposes, the FBI will notify all III states holding portions of the requested record. The III states will be responsible for disseminating their criminal histories to the requestor.

NGI shall support the retrieval of NFF Participant State Criminal Records on requests for criminal justice purposes.

National Fingerprint File (NFF) participating states will submit only the first arrest for an individual to the FBI. NGI will create a "stub" arrest that indicates that all criminal history from the NFF state is maintained at the state level. Subsequent arrests are not submitted to the FBI, but an electronic Criminal Print Ident (CPI) message is sent to inform the FBI when an individual is re-arrested.

Deleted.

NGI shall support the retrieval of photo information.

NGI shall support the retrieval of photo information from an External System (e.g., IDENT).

NGI shall provide photo images to External Systems.

NGI shall support the retrieval of palmprint information.

NGI shall support the retrieval of iris information.

Deleted.

NGI shall support the retrieval of unsolved latent audit trail information.

NGI shall support Other Information requests.

NGI shall support the retrieval of Rap Back Subscription Status.

NGI shall support the retrieval of a Rap Back Identity History Summary.

2.4 Investigation Services

The Investigation Service provides a list of candidates based on a one-to-many biometric and/or biographic search. The result set may include an ordered listing of candidates and corresponding information to facilitate the investigative decision process.

NGI shall support enrollment of an Identity as part of an Investigative Search.

Identity enrollment as part of an Investigative Search will only occur when the contributor indicates that a biometric should be retained in an unsolved biometric file.

NGI shall provide external system link identifiers as part of an Investigative Search response.

NGI shall support Subject Search requests based on biographic information.

The search request may be submitted via NCIC, NICS or NGI workstations, or Machine Readable Data (MRD).

NGI shall provide a candidate list in response to a Subject Search request.

The response may contain additional biographical data for each subject, or pointers to other systems that may contain additional data.

NGI shall support Ad Hoc Subject Search requests of Identity History repositories.

Deleted.

NGI shall support Latent Investigation Searches against designated NGI repository(ies).

NGI shall support Latent Investigation Searches of an external biometric repository.

NGI shall support Latent Investigation Searches from External Systems (e.g., IDENT).

NGI shall support Latent Investigation Searches filtered by NCIC fingerprint classifications.

NGI shall support Latent Print Image Investigation Searches.

NGI shall support Latent Print Feature Investigation Searches.

NGI shall support Unsolved Latent Searches.

Deleted.

NGI shall support Latent Penetration Searches against NGI repositories.

NGI shall support Latent Search Status and Modification requests.

NGI shall support Latent Repository Statistics Query requests.

NGI shall support Comparison Print Image Submission requests.

Deleted MCP.

NGI shall support Evaluation Latent Fingerprint Submission for investigation.

NGI shall support Fingerprint Image Search requests against NGI fingerprint repositories.

NGI shall provide a candidate list in response to a Fingerprint Image Search requests.

NGI shall support Fingerprint Feature Search requests against NGI fingerprint repositories.

NGI shall provide a candidate list in response to a Fingerprint Feature Search request.

NGI shall support Tenprint Fingerprint Rap Sheet Search requests of NGI repositories.

NGI shall provide a candidate list and corresponding Identity History Summaries in response to a Tenprint Fingerprint Rap Sheet Search request.

NGI shall support Text-Based Facial Photo Searches.

In addition to Text-Based Facial Photo searching, NGI will also support Text-Based Scars, Marks, and Tattoos (SMT) Photo searching.

NGI shall support Text-Based SMT Photo Searches.

NGI shall support Facial Recognition Searches.

Deleted.

NGI shall support Iris Searches.

2.5 Notification Services

The Notification Service provides event notification to users for their data contained within any of the NGI repositories [e.g., Criminal and Civil Files, Special Population Cognizant (SPC) Files, Unsolved

Iris File (UIF), and Unsolved Photo File (UPF)]. With this service, a data owner will receive an unsolicited notification from the system based on event criteria (triggers). In addition, events that trigger a notification on Immigration Violator File (IVF) records will be provided to the Law Enforcement Support Center (LESC).

NGI shall provide notification of record activity on persons who are of special interest.

Special Interest Flags will include Flashes, Wanted Persons, Registered Sexual Offenders, and other persons of special interest.

NGI shall provide Authorized Contributors with notifications of external system activity on a linked record flagged as being of special interest.

NGI shall provide notification of file maintenance activities to criminal record owners.

NGI shall provide notifications of positive identifications against shared data records to the shared data owner (e.g., IDENT).

NGI shall provide an External System (e.g., IDENT) with notifications of activity on a linked record.

NGI shall send notifications to wanting agencies as the result of fingerprint verification activity.

NGI shall send IVF notifications to the LESC.

NGI shall provide a Rap Back Notification Service.

NGI shall provide the owner of an unsolved latent fingerprint with notification of potential fingerprint matches.

NGI shall provide the owner of an SPC File with notification of potential fingerprint matches.

NGI shall provide the owner of an unsolved latent fingerprint with notification of fingerprint decisions.

NGI shall provide the owner of an SPC File fingerprint with notification of fingerprint decisions.

NGI shall provide the owner of an unsolved latent with notification of latent decisions.

NGI shall provide the owner of an SPC File with notification of latent decisions.

NGI shall provide the owner of an unsolved Latent with notification of deletions due to ULF maximum capacity.

NGI shall provide the owner of an unsolved photo with notification of potential facial photo matches as a result of a cascaded search.

NGI shall provide the owner of an SPC File with notification of potential facial photo matches as a result of a cascaded search.

NGI shall provide the owner of an unsolved photo with notification of positive facial photo decisions.

NGI shall provide the owner of an SPC File photo with notification of a positive facial photo decision

NGI shall provide the owner of an unsolved latent with notification of potential palmprint matches as a result of a cascaded search.

NGI shall provide the owner of an SPC File with notification of potential palmprint matches as a result of a cascaded search.

Deleted.

Deleted.

NGI shall provide the owner of an unsolved latent with notification of potential supplemental fingerprint and palmprint matches as a result of a cascaded search.

NGI shall provide the owner of an SPC File with notification of potential supplemental fingerprint and palmprint matches as a result of a cascaded search.

Deleted.

Deleted.

NGI shall provide the owner of unsolved iris data with notification of potential iris matches as a result of a cascaded search.

NGI shall provide the owner of an SPC File with notification of potential iris matches as a result of a cascaded search.

NGI shall provide the owner of an unsolved iris with notification of iris decisions.

NGI shall provide the owner of an SPC File with notification of iris decisions.

NGI shall send notification to RISC record owner(s) as the result of a positive identification.

Deleted.

NGI shall send Foreign or Unknown Place of Birth notifications to the LESC.

NGI shall send IDENT Hit notifications to the LESC.

2.6 Data Management Services

The Data Management Service supports data management by providing authorized users the capability to add, delete, or modify biographic and/or Identity History data.

NGI shall support the maintenance of fingerprints.

NGI shall support the maintenance of supplemental fingerprint and palmprint information.

NGI shall support link maintenance between NGI and external repositories.

NGI shall support the maintenance of shared data records.

NGI shall support direct enrollment of fingerprints into an SPC File.

NGI shall support the direct enrollment of latent information into an SPC File.

NGI shall support fingerprint decisions for ULF records.

NGI shall support latent decisions.

NGI shall forward a latent decision on an external system's candidate to that External System.

NGI will accept and process latent decisions from authorized contributors and latent examiners resulting from an investigative search that returned latent candidates.

NGI shall support file maintenance of latent files.

NGI will have capabilities to modify and delete data within the SPC Files and ULF.

NGI shall support file maintenance of SPC Files.

NGI shall support file maintenance of contributor information.

Deleted.

NGI will support the processing of information related to dispositions, expungements, consolidations, death notices, and want and flash notifications. NGI also supports the maintenance of specific biographic and criminal record data.

NGI shall support file maintenance requests for the synchronization of NCIC and NGI Wanted Person and Sexual Offender Registry information.

NGI shall support the maintenance of authorized statutes.

NGI will provide the capability to perform statute maintenance for the list of known state statutes used by AQC.

NGI shall support Unsolved Latent Add Confirm submissions.

NGI shall support the maintenance of the Computerized Records Sent File.

NGI shall support electronic disposition submissions without fingerprints.

NGI shall support electronic disposition maintenance requests.

NGI shall provide a conflict resolution capability in support of disposition processing.

NGI shall support the maintenance of Identity History information.

NGI shall support restoration of Identity History information.

The following requirements are related to the direct enrollment and maintenance of biometrics. Direct biometric enrollment may be done with fingerprints for validation, or without fingerprints when a Memorandum of Understanding (MOU) is in place with the contributor.

NGI shall support direct enrollment of photos.

NGI shall support bulk enrollment of photos.

NGI shall support the maintenance of photos.

NGI shall support direct enrollment of supplemental fingerprint and palmprint information.

NGI shall support bulk enrollment of supplemental fingerprint and palmprint information.

NGI shall support direct enrollment of palmprints.

NGI shall support bulk enrollment of palmprints.

NGI shall support the maintenance of palmprints.

NGI shall support direct enrollment of iris data.

NGI shall support bulk enrollment of iris data.

NGI shall support the maintenance of iris data.

NGI shall support direct enrollment into Rap Back.

NGI shall support the maintenance of Rap Back Subscriptions.

NGI shall support Rap Back Subscription Renewal.

NGI shall support ITF record maintenance requests.

NGI shall support the maintenance of Special Interest records.

NGI shall support Death Notice submissions.

NGI shall support Flash Submissions.

NGI shall support the maintenance of IVF information.

NGI shall support NFF State CPI Notifications.

3 FUNCTIONAL REQUIREMENTS

This section identifies the functional requirements derived from the user requirements described in the previous section. Pertinent workload, performance, availability, security, and other requirements that must be considered in conjunction with these functional requirements are identified in Section 4. References made to EBTS Types of Transactions (TOTs) indicate that the transaction is submitted by contributors external to CJIS. Likewise, references made to System Types of Transactions (STOTs) indicate that the transaction is submitted by an Authorized FBI Service Provider internal to CJIS.

3.1 Identification Services Functional Requirements

The following section contains the functional requirements supporting Identification user services.

3.1.1 Tenprint Fingerprint Identification Services

The Tenprint Fingerprint Identification Services will provide the capability to match fingerprint information from criminal and civil Tenprint submissions to fingerprint information contained within the NGI repositories. This service results in an identification decision (i.e., positive identification, non-identification). If the submission does not meet minimum processing criteria (e.g., quality), the submission will be returned with a reason for rejection. Tenprint Fingerprint Identification Search requests submitted by participating shared data agencies will generate a search of the Shared Data independent of the NGI search.

3.1.1.1 Tenprint Fingerprint Identification Inputs

NGI shall accept a Tenprint Fingerprint Identification Search request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall accept a Tenprint Fingerprint Identification Search request from an Authorized External System (e.g., IDENT) in accordance with the latest EBTS version.

The EBTS TOTs that support the Tenprint Fingerprint Identification Search are: AMN, CAR, CNA, CPDR, CPNU, DEK, DEU, DOCE, EMUF, FANC, FAUF, FIDO, FNDR, MAP, MPR, NFAP, NFUF, NFUE and NNDR. The following TOTs are considered Humanitarian Tenprint Identification searches: AMN, DEU, and MPR.

NGI also supports additional TOTs that are not defined, but are compliant with the EBTS. These TOTs are limited to use by the Card Scanning Service to support hardcopy submission of Tenprint Fingerprint Identification searches: CARC, CNAC, FUFC, MAPC, NFDP, and NFFC. The CSS TOTs are validated in the same manner as their corresponding EBTS TOTs which are: CAR, CNA, FAUF, MAP, NFAP, and NFUF, respectively.

NGI shall allow an Authorized FBI Service Provider to submit a Tenprint Fingerprint Identification Search request.

The NGI STOTs that support the Tenprint Fingerprint Identification Search are: LCAR, IAMN, ICAR, ICNA, IDEK, IDEU, IFANC, IFAUF, FOID, IMAP, IMPR, and INFUF. The following STOTs are considered Humanitarian Tenprint Identification searches: IAMN, IDEU, and IMPR.

NGI shall accept flat fingerprint data as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept rolled fingerprint data as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept an external system link identifier and biographic data from an External System (e.g., IDENT) as part of a Tenprint Fingerprint Identification Search request.

NGI shall require a retention status indicator as part of a Tenprint Fingerprint Identification Search request.

NGI shall require a designation of the repository(ies) into which biometric data should be enrolled as part of a Tenprint Fingerprint Identification Search request.

The TOT/STOT may be used to determine designated repository.

NGI shall accept a designation of the NGI repository(ies) against which fingerprint data should be searched as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept a designation of the external repository(ies) (e.g., IDENT) against which fingerprint data should be searched as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept an indicator on a Tenprint Fingerprint Identification Search that specifies which dissemination tier to apply to a RISC enrolled Identity.

NGI shall accept an indicator on a retained Tenprint Identification Search request that specifies whether or not a RISC enrolled tier-1 or tier-2 Identity should be marked for hit notifications to the RISC record owner.

NGI provides a multi-tier dissemination structure that is defined as follows: tier 1 – Share All; tier 2 – Point of Contact Only; tier 3 – Silent Hit.

NGI shall accept a designation of transaction priority by which the Tenprint Fingerprint Identification Search request should be performed.

NGI shall accept supplemental fingerprint and palmprint information as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept photo input from an Authorized Contributor as part of a Tenprint Fingerprint Identification Search request.

NGI shall allow photo input from an Authorized FBI Service Provider as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept a multi-level SMT photo descriptor field as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept an indicator on a Tenprint Fingerprint Identification Search request that specifies if a photo should be included with the fingerprint search response.

The following requirement will support an Authorized Contributor request to search the LESC using an Immigration Alien Query (IAQ) as part of an identification search of the IDENT System. Responses to NGI will be provided as an Immigration Alien Response (IAR).

NGI shall accept an indicator on a Tenprint Fingerprint Identification Search request of the IDENT system that an IAQ be requested of the LESC.

NGI shall accept as part of a Tenprint Fingerprint Identification Search from an External System (e.g., IDENT) an indication of whether or not NGI should establish a link when the search results in a positive identification.

NGI shall accept palmprint images from an Authorized Contributor as part of a Tenprint Fingerprint Identification Search request.

NGI shall allow palmprint images from an Authorized FBI Service Provider as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept iris data input from an Authorized Contributor as part of a Tenprint Fingerprint Identification Search request.

NGI shall allow iris data input from an Authorized FBI Service Provider as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept a Rap Back Enrollment from an Authorized Contributor as part of a Tenprint Fingerprint Identification Search request.

NGI shall allow a Rap Back Enrollment from an Authorized FBI Service Provider as part of a Tenprint Fingerprint Identification Search request.

NGI shall require a designation of which event type(s) (e.g., civil, criminal, external system) will trigger Rap Back notifications for the associated Identity when Rap Back Enrollment is indicated as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept a Rap Back subscription expiration date for the associated Identity, as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept a designation of the Authorized Contributor(s) that should receive Rap Back Notifications for the associated Identity, as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept a UCN(s) as part of a Tenprint Fingerprint Identification Search request.

NGI will optionally accept one or more quoted Universal Control Numbers (UCN) when a contributor has made an identification at the state level.

NGI shall accept an Identity History Summary indicator as part of a Tenprint Fingerprint Identification Search request.

The Identity History Summary indicator will be used to determine if an Identity History Summary should be included as part of a Tenprint Fingerprint Identification response for a positive identification decision.

NGI shall allow an Authorized FBI Service Provider to input fingerprint images to initiate a Tenprint Fingerprint Identification Search request.

The NGI workstation will support multiple input methods for biometric images (scanning, CD-ROM, and other removable media). These methods will support the standards for output stated in ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, Data Format for the Interchange of Fingerprint Information" and with the EBTS.

NGI shall accept an Identity Theft Victim File Enrollment indicator as part of a Tenprint Fingerprint Identification Search request.

3.1.1.2 Tenprint Fingerprint Identification Processing

NGI shall initiate a Tenprint Fingerprint Identification Search against the Shared Data as a result of a Tenprint Fingerprint Identification Search request from an Authorized Contributor participating in Shared Data.

When an incoming Tenprint Fingerprint Identification Search request or CPI Notification is from an Authorized Shared Data Agency, NGI will not only search against the required repository but will also independently search and compare against the Shared Data.

NGI shall perform AQC of textual data (i.e., reason fingerprinted, arrest data) contained in a Tenprint Fingerprint Identification Search request against the AQC business rules.

NGI has the capability to make a pass or fail decision through a rule-based AQC process. Tenprint Fingerprint Identification Search requests that do not pass the automated process are forwarded to an Authorized FBI Service Provider for manual review. NGI will provide two options to validate the Reason Fingerprinted (RFP) field for Non-Federal User Fee applicant submissions. Option A will validate the RFP against a list of authorized statutes. Option B will validate the RFP against a list of standardized terms.

NGI shall reject a Tenprint Fingerprint Identification Search request when textual information is invalid based on AQC business rules.

NGI shall require an Authorized FBI Service Provider to perform Manual Quality Check on a Tenprint Fingerprint Identification Search request when AQC business rules determine manual review is necessary.

NGI shall allow an Authorized FBI Service Provider to reject a Tenprint Fingerprint Identification Search request when it is determined to be invalid as part of Manual Quality Check.

NGI shall perform ASC of the individual fingerprint impressions to the plain fingerprint impressions contained in a Tenprint Fingerprint Identification Search request to determine if the individual fingerprint impressions are correctly sequenced.

NGI shall reject a Tenprint Fingerprint Identification Search request as part of ASC when fingerprint data fails to meet processing criteria in accordance with ASC business rules.

NGI shall require an Authorized FBI Service Provider to perform manual FSC on a Tenprint Fingerprint Identification Search request when ASC determines that manual review is necessary.

NGI shall allow an Authorized FBI Service Provider to reject a Tenprint Fingerprint Identification Search request as part of manual FSC when fingerprint data fails to meet processing criteria.

Processing criteria is based on the Authorized FBI Service Providers' FSC Standard Operating Manual (SOM).

NGI shall extract fingerprint features from the fingerprint images provided in the Tenprint Fingerprint Identification Search request.

NGI shall perform an image quality check on a Tenprint Fingerprint Identification Search request based on image quality standards.

NGI shall reject a Tenprint Fingerprint Identification Search request when the fingerprint images fail to satisfy minimum fingerprint image quality standards.

NGI shall mark the Tenprint Fingerprint Identification Search request as SBDA when the submitted fingerprint data fails to satisfy fingerprint image quality for retention.

The Search But Don't Add (SBDA) indicator allows tenprint fingerprint data of a defined quality to be used in a search of the NGI repositories, but not allow the images and features to be added to the NGI repository(ies). Humanitarian prints will be added despite the SBDA indicator being set. If the search request results in a non-identification decision, NGI will respond with a quality reject message.

NGI shall perform a fingerprint search of the default repository when the repository is not specified in the Tenprint Fingerprint Identification Search request.

NGI shall perform a search of default internal repositories before sending a Tenprint Fingerprint Identification Search request to an External System.

The default NGI repositories will be searched first to determine if there is a link to the External System (e.g., IDENT). If a link exists, a search request will not be sent to the External System. Information will be retrieved from the system directly using the external system's link identifier.

NGI shall perform a rolled fingerprint search of the repositories designated in a Tenprint Fingerprint Identification Search request.

NGI shall perform a flat fingerprint search of the repositories designated in a Tenprint Fingerprint Identification Search request.

NGI shall perform all Tenprint Fingerprint Identification Search requests against composite fingerprints.

NGI shall prioritize a Tenprint Fingerprint Identification Search request using established and specified priority criteria.

NGI shall perform a rolled fingerprint search against the RISC for all Tenprint Fingerprint Identification Search requests.

NGI shall perform a flat fingerprint search against the RISC for all Tenprint Fingerprint Identification Search requests.

Fingerprint Search results of the RISC repository will be included in the Tenprint Fingerprint Identification Search response.

When an incoming submission references at least one UCN, a fingerprint comparison of each quoted UCN is made prior to a technical search and/or name search.

NGI shall perform a Subject Search of the designated NGI repository for candidates based on biographic data provided for all Tenprint Fingerprint Identification Search requests.

NGI shall perform III/Verify as part of a Tenprint Fingerprint Identification Search request for each quoted UCN and each Subject Search candidate.

NGI shall compare the fingerprint features extracted from the fingerprint images provided in the Tenprint Fingerprint Identification Search request against the fingerprint features of each candidate provided to III/Verify.

NGI shall calculate a match score for each candidate resulting from a Tenprint Identification Search request.

NGI will determine a match score for each quoted UCN, Subject Search candidate, or Feature Search candidate.

NGI shall require an Authorized FBI Service Provider to perform a manual special processing review when one or more candidates are marked with a special processing indicator (e.g., SPF) as part of a Tenprint Fingerprint Identification Search request.

NGI shall eliminate each candidate that has a match score below the minimum threshold for III/Verify as part of a Tenprint Fingerprint Identification Search request.

NGI shall perform a fingerprint feature search for all Tenprint Fingerprint Identification Searches.

NGI shall perform a subject search of the civil repository using biographic data provided as part of a Humanitarian Tenprint Fingerprint Identification Search request.

NGI shall perform a feature search of the civil repository using the fingerprint features extracted from the fingerprint images provided in the Humanitarian Tenprint Fingerprint Identification Search request.

NGI shall perform a feature search of the Shared Data records as part of a Tenprint Fingerprint Identification Search request submitted by an Authorized Contributor participating in Shared Data.

NGI shall calculate a match score for each candidate resulting from a feature search of the Shared Data.

NGI shall determine a positive identification decision for each candidate that has a match score above the high confidence threshold as part of a Tenprint Fingerprint Identification Search request.

Identification decisions may require manual FIC, depending on the match score. If the match score is above the high confidence threshold ("Lights Out"), then no manual FIC is required. If the match score is below the high confidence threshold and above the low confidence threshold, then one manual FIC is required. If the match score is below the low confidence threshold, then two manual FICs are required.

NGI shall require an Authorized FBI Service Provider to perform a manual FIC for each candidate from a Tenprint Fingerprint Identification Search request that is below the high confidence threshold.

NGI shall require a second Authorized FBI Service Provider to perform a manual FIC to confirm a positive identification for each candidate from a Tenprint Fingerprint Identification Search request that is below the low confidence threshold.

The second manual FIC will be performed independent of the first FIC decision. The decision made by the first service provider will not be made known to the second service provider.

NGI shall reject any search request of the Shared Data that has been determined "Unable to Process" by three independent manual FIC service providers.

NGI shall allow an Authorized FBI Service Provider to reject a Tenprint Fingerprint Identification Search request as a result of the manual FIC.

NGI shall require an Authorized FBI Service Provider to perform a Post Process Review check on all positive identifications resulting from a Tenprint Fingerprint Identification Search of the Shared Data.

NGI shall retrieve the corresponding subject's Identity History information when requested and a positive identification decision results from a Tenprint Fingerprint Identification Search request.

NGI shall retrieve Identity History information from III/NFF State systems, when a positive identification decision is made to an Identity that contains an NFF indicator as part of a Tenprint Fingerprint Identification Search request.

For the purpose of criminal Fingerprint Identification Search responses, the FBI will solicit the III/NFF State for their portion of the criminal history. The response from the III/NFF State Participant will be merged or appended to the FBI's response and returned to the submitter of the Fingerprint Identification Search. These queries will be sent to states over the NCIC network. The responses will be sent to NGI over Nlets, assembled by NGI, and returned to the requester.

NGI shall create a unique Identity as a result of a retained Tenprint Fingerprint Identification Search request that results in a non-identification decision.

NGI shall enroll Identity information for the newly created Identity into the appropriate NGI repository as a result of a retained Tenprint Fingerprint Identification Search request that results in a non-identification decision.

NGI shall enroll the fingerprint data in the designated repository(ies) based on file maintenance rules as part of a retained Tenprint Fingerprint Identification Search request.

NGI shall provide the capability to uniquely identify fingerprint data enrolled as a result of a Tenprint Fingerprint Identification Search request.

NGI shall assign the multi-tier dissemination level indicated in a retained Tenprint Fingerprint Identification Search request designated for the RISC repository.

NGI shall assign the default multi-tier dissemination level, when the multi-tier dissemination level is not indicated in a retained Tenprint Fingerprint Identification Search request designated for the RISC repository.

NGI shall enroll the photos in the designated repository based on file maintenance rules as part of a Tenprint Fingerprint Identification Search request.

NGI shall provide the capability to uniquely identify photos enrolled as a result of a Tenprint Fingerprint Identification Search request.

NGI shall perform a validation to ensure that submitted palmprint images match the submitted fingerprints, when the distal segments of the palmprint images are included in the Tenprint Fingerprint Identification Search request.

Palmprints will not be enrolled if the validation of the Palmprints to the submitted fingerprints fails.

NGI shall enroll the palmprints in the designated repository based on file maintenance rules as part of a Tenprint Fingerprint Identification Search request.

NGI shall provide the capability to uniquely identify palmprints enrolled as a result of a Tenprint Fingerprint Identification Search request.

NGI shall enroll the iris data in the designated repository based on file maintenance rules as part of a Tenprint Fingerprint Identification Search request.

NGI shall provide the capability to uniquely identify iris data enrolled as a result of a Tenprint Fingerprint Identification Search request.

NGI shall perform a validation to ensure that submitted supplemental fingerprint and palmprint images match the submitted fingerprints, when the distal segments of the supplemental fingerprint and palmprint images are included in the Tenprint Fingerprint Identification Search request.

Supplemental fingerprint and palmprint images will not be enrolled if the validation of the supplemental fingerprint and palmprint images to the submitted fingerprints fails.

NGI shall enroll supplemental fingerprint and palmprint information into the designated repository(ies) based on file maintenance rules as part of a retained Tenprint Fingerprint Identification Search request.

NGI shall provide the capability to uniquely identify supplemental fingerprint and palmprint data enrolled as a result of a Tenprint Fingerprint Identification Search request.

NGI shall enroll an Identity into Rap Back, when indicated, as part of a retained Tenprint Fingerprint Identification Search request.

NGI shall assign a default Rap Back subscription expiration date when an expiration date is not specified as part of the Tenprint Fingerprint Identification Search request.

NGI shall assign the default Rap Back subscription expiration date when the expiration date specified, as part of the Tenprint Fingerprint Identification Search request, exceeds the maximum allowable Rap Back subscription period.

NGI shall reject the Tenprint Fingerprint Identification Search request when the search is marked as SBDA and results in a non-identification decision.

NGI shall reject a Rap Back enrollment when the associated Tenprint Fingerprint Identification Search request is rejected.

NGI shall reject a photo enrollment when the associated Tenprint Fingerprint Identification Search request is rejected.

NGI shall reject a palmprint enrollment when the associated Tenprint Fingerprint Identification Search request is rejected.

NGI shall reject an iris enrollment when the associated Tenprint Fingerprint Identification Search request is rejected.

NGI shall reject the supplemental fingerprint and palmprint information enrollment when the associated Tenprint Fingerprint Identification Search request is rejected.

NGI shall maintain an Identity based on file maintenance rules as a result of a Tenprint Fingerprint Identification Search request with a positive identification decision.

NGI shall update Identity History information with the link information contained in a Tenprint Fingerprint Identification Search request from an External System (e.g., IDENT), when indicated.

NGI shall update fingerprint information based on file maintenance rules as a result of a Tenprint Fingerprint Identification Search request with a positive identification decision.

NGI shall create a copy of the Tenprint Fingerprint Identification Search request for the NGI Certification File based on file maintenance rules.

NGI shall update the Identity History with an Identity Theft Victim indicator when provided as part of a Tenprint Fingerprint Identification Search request.

NGI shall send an External Tenprint Fingerprint Identification Search request to an External System (e.g., IDENT) when the designated repository is external and no record link exists to that External System.

NGI shall send an External Tenprint Fingerprint Identification Search request when a retained Tenprint Fingerprint Identification Search request results in a non-identification decision (i.e., new NGI enrollment) based on External System Search rules.

NGI shall send an External Tenprint Fingerprint Identification Search request to an External System, when the external system is not IDENT, in accordance with the latest EBTS version as part of a Tenprint Fingerprint Identification Search request.

The EBTS TOT that supports an External Tenprint Fingerprint Identification Search request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall send an External Tenprint Fingerprint Identification Search request to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement as part of a Tenprint Fingerprint Identification Search request.

NGI shall send an External Tenprint Fingerprint Identification Search request, when fingerprint image quality exceeds the quality improvement threshold and a link to the External System does not exist, as part of a Tenprint Fingerprint Identification Search request based on External System Search rules.

NGI shall indicate as part of an External Tenprint Fingerprint Identification Search request against an external repository whether or not the External System should establish a link when the external system search results in a positive identification, as part of a Tenprint Fingerprint Identification Search request.

NGI shall include biographic data in an External Tenprint Fingerprint Identification Search request, as part of a Tenprint Fingerprint Identification Search request. NGI shall include a unique transaction control number (TCN) in an External Tenprint Fingerprint Identification Search request, as part of a Tenprint Fingerprint Identification Search request.

NGI shall record the correlation between the identified UCN and the unique transaction control number (TCN) included in an External Tenprint Fingerprint Identification Search request when a Tenprint Fingerprint Identification Search request results in a positive identification.

NGI shall record the correlation between the UCN assigned to the newly enrolled identity and the unique transaction control number (TCN) included in an External Tenprint Fingerprint Identification Search request when a Tenprint Fingerprint Identification Search request results in a non-identification decision.

NGI shall send an External Information request to an External System (e.g., IDENT) when the designated repository is external and a record link exists to that External System as part of a Tenprint Fingerprint Identification Search request.

NGI shall send an External Information request in accordance with the latest EBTS version, when the external system is not IDENT.

The EBTS TOT that supports an External Information request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

An External Information request will be used to retrieve external record information when a Tenprint Fingerprint Identification Search request of NGI results in a positive identification against a record containing a linked identifier to an External System.

NGI shall send an External Information request to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement.

NGI shall include the UCN and the external system link identifier in an External Information request.

NGI shall accept a response from an External System as a result of an External Tenprint Fingerprint Identification Search request of external repositories in accordance with the latest EBTS version when the external system is not IDENT, as part of a Tenprint Fingerprint Identification Search request.

The EBTS TOT that supports an External Tenprint Fingerprint Identification Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a response from an IDENT as a result of an External Tenprint Fingerprint Identification Search request of external repositories in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement, as part of a Tenprint Fingerprint Identification Search request.

NGI shall accept a response from an External System as a result of an External Information request in accordance with the latest EBTS version when the external system is not IDENT.

The EBTS TOT that supports an External Information response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a response from IDENT as a result of an External Information request in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement.

NGI shall accept an external system link identifier and biographic data from an External System (e.g., IDENT) in a response to an External Tenprint Fingerprint Identification Search request.

NGI shall accept a unique transaction control number (TCN) from an External System (e.g., IDENT) in a response to an External Tenprint Fingerprint Identification Search request as part of a Tenprint Fingerprint Identification Search request.

NGI shall determine the UCN using the unique transaction control number (TCN) returned in an External Tenprint Fingerprint Identification Search response, and the previously recorded UCN/TCN correlation when an External Tenprint Fingerprint Identification Search results in a positive identification as part of a Tenprint Fingerprint Identification Search request.

NGI shall send a TCN/UCN correlation message to an External System (e.g., IDENT), providing the Identified UCN when an External Tenprint Fingerprint Identification Search results in a positive identification as part of a Tenprint Fingerprint Identification Search request.

NGI shall send a TCN/UCN correlation message to an External System in accordance with the latest EBTS version when the external system is not IDENT as part of a Tenprint Fingerprint Identification Search request.

NGI shall send a TCN/UCN correlation message to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement as part of a Tenprint Fingerprint Identification Search request.

NGI shall update an Identity with the information contained in an External Tenprint Fingerprint Identification Search response from an External System (e.g., IDENT).

NGI shall accept a photo(s) as part of an External Tenprint Fingerprint Identification Search response.

NGI shall accept a photo(s) as part of an External Information response.

NGI shall send an IAQ to the LESC as part of a Tenprint Identification Search request when an IDENT record exists, the LESC information has been requested, and the Daily IAQ Search Limit has not been reached.

NGI shall send an IAQ to LESC, when the daily configured limit is not exceeded, for any positive identification resulting from a Tenprint Fingerprint Identification Search of the Shared Data.

NGI shall send an IAQ to LESC in accordance with the Nlets User and Technical Guide.

NGI shall accept an IAR from the LESC in accordance with the Nlets User and Technical Guide.

NGI shall accept an IAR from LESC that contains biographic information for a positive identification resulting from a Tenprint Fingerprint Identification Search of the shared data records.

The biographic data will consist of DOB, Gender, the IDENT unique identifier (EID), the A-number, FNU, and Subject Name.

NGI shall perform a cascaded fingerprint search of the ULF, in accordance with cascaded search business rules, as a result of Tenprint Fingerprint Identification Search requests.

NGI shall send an External Unsolved Latent Search request when a retained Tenprint Fingerprint Identification Search request results in a non-identification decision (i.e., new NGI enrollment) based on External System Search rules.

NGI shall send an External Unsolved Latent Search request when fingerprint image quality exceeds the quality improvement threshold as part of a Tenprint Fingerprint Identification Search request based on External System Search rules.

NGI shall send an External Unsolved Latent Search request in accordance with the latest version of the EBTS.

The EBTS TOT that supports an External Unsolved Latent Search request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI will not receive a response to this unsolved latent search of an External System.

NGI shall perform a cascaded fingerprint search of the marked SPC Files, in accordance with cascaded search business rules, as a result of Tenprint Fingerprint Identification Search requests.

NGI shall perform a cascaded facial recognition search of the UPF when the photo submitted with a Tenprint Fingerprint Identification Search request meets the minimum quality standard for facial recognition in accordance with cascaded search business rules.

NGI shall perform a cascaded facial recognition search of marked SPC Files when the photo submitted with a Tenprint Fingerprint Identification Search request meets the minimum quality standard for facial recognition in accordance with cascaded search business rules.

NGI shall perform a cascaded palmprint search of the ULF when the palmprint submitted with a Tenprint Fingerprint Identification Search request meets the minimum quality standard for palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded palmprint search of the marked SPC Files, if the palmprint submitted with a Tenprint Fingerprint Identification Search request meets the minimum quality standard for palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded supplemental fingerprint and palmprint search of the ULF when the supplemental fingerprint and palmprint submitted with a Tenprint Fingerprint Identification Search request meets the minimum quality standard for supplemental fingerprint and palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded supplemental fingerprint and palmprint search of the marked SPC Files, if the supplemental fingerprint and palmprint submitted with a

Tenprint Fingerprint Identification Search request meets the minimum quality standard for supplemental fingerprint and palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded search of the UIF when the iris data submitted with a Tenprint Fingerprint Identification Search request meets the minimum quality standard for iris searches in accordance with cascaded search business rules.

NGI shall perform a cascaded search of marked SPC File(s) when the iris data submitted with a Tenprint Fingerprint Identification Search request meets the minimum quality standard for iris searches in accordance with cascaded search business rules.

NGI shall send a Hot Check Name Search request to NCIC for all Tenprint Fingerprint Identification Search requests.

NGI shall determine the response distribution method (i.e., electronic or hardcopy) for a Tenprint Fingerprint Identification Search response.

3.1.1.3 Tenprint Fingerprint Identification Outputs

NGI shall provide an Authorized Contributor with an identification decision as part of a Tenprint Fingerprint Identification Search response.

An identification decision will be either a positive identification or a non-identification. If the contributor is identified as not being capable of receiving electronic response, a hardcopy response will be generated and sent to the contributor. Otherwise, an electronic EBTS compliant response will be sent.

NGI shall provide the Identity History Summary for a positive identification candidate in the Tenprint Fingerprint Identification Search response, when requested.

NGI shall provide an Identity History Summary in response to a Tenprint Fingerprint Identification Search request of the RISC repository that results in an identification against a tier-1 RISC record.

NGI shall provide contact information in response to a Tenprint Fingerprint Identification Search request of the RISC repository that results in an identification against a tier-2 RISC record.

NGI shall provide a non-identification response in response to a Tenprint Fingerprint Identification Search request of the RISC repository that results in an identification against a tier-3 RISC record.

NGI shall optionally include, on a Tenprint Fingerprint Identification Search response, the most recently taken frontal facial photo for the identified subject.

NGI shall optionally include, on a Tenprint Fingerprint Identification Search response, the most recently taken facial photo for the identified subject, when no frontal facial photo is available.

NGI shall optionally include, on a Tenprint Fingerprint Identification Search response, the external system photo for the identified subject.

NGI shall provide a reject response, as appropriate, for a Tenprint Fingerprint Identification Search request.

NGI shall provide Authorized Contributors with an electronic response to a Tenprint Fingerprint Identification Search request in accordance with the latest EBTS version.

NGI shall provide a Tenprint Fingerprint Identification Search response to an External System in accordance with the latest version of the EBTS.

The EBTS TOT that supports a Tenprint Fingerprint Identification Search response is SRE.

NGI shall provide the appropriate Tenprint Fingerprint Identification Search response to an Authorized FBI Service Provider.

NGI shall provide a hardcopy response to a Tenprint Fingerprint Identification Search request, as appropriate.

NGI shall provide an initial partial response when a Tenprint Fingerprint Identification Search request results in a positive identification to a manual record.

NGI shall combine the NGI Tenprint Fingerprint Identification Search request results with the response(s) from external system(s) (e.g., IDENT) into a single Tenprint Fingerprint Identification Search response, when all search results are available within the response time threshold required to create a combined response.

NGI shall combine the NGI Tenprint Fingerprint Identification Search request results with the Identity History information retrieved from III/NFF State systems, when all III/NFF Identity History information is available within the response time threshold required to create a combined response.

NGI shall provide partial Tenprint Fingerprint Identification Search request results as part of a Tenprint Fingerprint Identification Search response when External System(s) do not meet the response time threshold required to create a combined response.

A partial response will include information to indicate that the external system designated to search did not respond to the search within the NGI response time. The status of the external system may be included if provided.

NGI shall provide partial Tenprint Fingerprint Identification Search request results as part of a Tenprint Fingerprint Identification Search response when III/NFF State systems do not meet the response time threshold required to create a combined response.

A partial response will include information to indicate that the III/NFF State system did not provide Identity History information within the NGI response time.

NGI shall forward External System Tenprint Fingerprint Identification Search request results independently from an NGI Tenprint Fingerprint Identification Search response

when the External System does not meet the response time threshold required to create a combined response.

For IDENT linked records, the combined Tenprint Fingerprint Identification Search response will not include the supplemental data obtained from the LESC.

NGI shall indicate the source repository (e.g., IDENT) of all external repository information returned in a Tenprint Fingerprint Identification Search response.

NGI shall forward the LESC IAR responses to an Authorized Contributor independent of the Tenprint Fingerprint Identification Search responses.

The IAR responses forwarded to Authorized Contributors include those contributors participating in Shared Data.

NGI shall forward the LESC IAR responses to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports notification of the LESC IAR responses will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the LESC IAR responses to an Authorized FBI Service Provider independent of the Tenprint Fingerprint Identification Search responses.

NGI shall advise the Authorized Contributor when a photo is enrolled as a result of a Tenprint Fingerprint Identification Search request, but fails to meet minimum quality standards for facial recognition.

NGI shall advise the Authorized FBI Service Provider when a photo is enrolled as a result of a Tenprint Fingerprint Identification Search request, but fails to meet minimum quality standards for facial recognition.

NGI shall advise the Authorized Contributor when a palmprint is enrolled as a result of a Tenprint Fingerprint Identification Search request, but fails to meet minimum quality standards for palmprint searching.

NGI shall advise the Authorized FBI Service Provider when a palmprint is enrolled as a result of a Tenprint Fingerprint Identification Search request, but fails to meet minimum quality standards for palmprint searching.

NGI shall advise the Authorized Contributor when a palmprint is not enrolled due to a failed validation of fingerprints to palmprints when processing a Tenprint Fingerprint Identification Search request.

NGI shall advise the Authorized FBI Service Provider when a palmprint is not enrolled due to a failed validation of fingerprints to palmprints when processing a Tenprint Fingerprint Identification Search request.

NGI shall advise the Authorized Contributor when a supplemental fingerprint and palmprint is enrolled as a result of a Tenprint Fingerprint Identification Search request, but fails to meet minimum quality standards for supplemental fingerprint and palmprint searching.

NGI shall advise the Authorized FBI Service Provider when a supplemental fingerprint and palmprint is enrolled as a result of a Tenprint Fingerprint Identification Search request, but fails to meet minimum quality standards for supplemental fingerprint and palmprint searching.

NGI shall advise the Authorized Contributor when a supplemental fingerprint and palmprint is not enrolled due to a failed validation of fingerprints to supplemental fingerprint and palmprints when processing a Tenprint Fingerprint Identification Search request.

NGI shall advise the Authorized FBI Service Provider when a supplemental fingerprint and palmprint is not enrolled due to a failed validation of fingerprints to supplemental fingerprint and palmprints when processing a Tenprint Fingerprint Identification Search request.

NGI shall advise the Authorized Contributor when iris data is enrolled as a result of a Tenprint Fingerprint Identification Search request, but fails to meet minimum quality standards for iris searches.

NGI shall advise the Authorized FBI Service Provider when iris data is enrolled as a result of a Tenprint Fingerprint Identification Search request, but fails to meet minimum quality standards for iris searches.

NGI shall advise the Authorized Contributor of the Rap Back Enrollment status as part of a Tenprint Fingerprint Identification Search response.

NGI shall advise the Authorized FBI Service Provider of the Rap Back Enrollment status as part of a Tenprint Fingerprint Identification Search response.

3.1.2 Latent Fingerprint Identification Services

The Latent Fingerprint Identification Services will provide the capability to match fingerprint data from Latent Fingerprint Identification Search requests to fingerprint data contained within the NGI fingerprint repositories. Latent Fingerprint Identification Search requests can only be submitted by FBI Field Offices or Authorized FBI Service Providers. Following receipt of the submission by NGI, these transactions will be manually processed by an Authorized FBI Service Provider (Latent Examiner). This service results in an identification decision (i.e., positive identification, non-identification or inconclusive). If the submission does not meet minimum processing criteria (e.g., quality), the submission will be returned with reason for rejection.

The following functional requirements relate to a fingerprint identification search for latent purposes using ten or less fingerprints resulting in an identification decision.

3.1.2.1 Latent Fingerprint Identification Inputs

NGI shall accept fingerprint data from an Authorized Contributor as part of a Latent Fingerprint Identification Search request in accordance with the latest EBTS version.

The EBTS TOT that supports a Latent Fingerprint Identification Search request is LFS.

NGI shall allow an Authorized FBI Service Provider to submit a Latent Fingerprint Identification Search request.

The NGI STOT that supports Latent Fingerprint Identification Search is ILFS.

NGI shall allow an Authorized FBI Service Provider to input fingerprint images to initiate a Latent Fingerprint Identification Search request.

The NGI workstation will support multiple input methods for biometric images (scanning, CD-ROM, and other removable media). These methods will support the standards for output stated in ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, Data Format for the Interchange of Fingerprint Information" and with the EBTS.

NGI shall accept a designation of the internal repository(ies) against which fingerprint data should be searched as part of a Latent Fingerprint Identification Search request.

NGI shall accept an indicator for enrollment into the ULF as part of the Latent Fingerprint Identification Search request.

NGI shall accept a fingerprint position(s) indicator when a single fingerprint is submitted in a Latent Fingerprint Identification Search request.

An Authorized FBI Service Provider can indicate which finger position to search against in the NGI repository. If the Latent Fingerprint Identification Search request contains a single fingerprint image, the Authorized FBI Service Provider can indicate multiple finger positions to be searched. If no finger position is indicated, then all finger positions will be searched.

NGI shall require a finger position indicator for each fingerprint when multiple fingerprints are submitted as part of a Latent Fingerprint Identification Search request.

On a multiple finger submission, NGI will accept only one position for each finger submitted within the request. Each indicator must be unique and may not be the same as any other finger position indicator.

NGI shall accept specified pattern classification(s) for each finger to be used as a filter for a Latent Fingerprint Identification Search request.

NGI shall accept an Identity History Summary indicator as part of a Latent Fingerprint Identification Search request.

3.1.2.2 Latent Fingerprint Identification Processing

NGI shall allow an Authorized FBI Service Provider to manually extract fingerprint features from the fingerprint images provided in the Latent Fingerprint Identification Search request.

NGI shall allow an Authorized FBI Service Provider to initiate automated fingerprint feature extraction to process a Latent Fingerprint Identification Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

NGI shall require an Authorized FBI Service Provider to extract (i.e., automated or manual) fingerprint features prior to processing a Latent Fingerprint Identification Search request.

NGI shall search using the finger position(s) and fingerprint features extracted from the fingerprint images provided in the Latent Fingerprint Identification Search request.

NGI shall search all finger positions for a Latent Fingerprint Identification Search request containing a single fingerprint when no finger position is indicated.

NGI shall perform a fingerprint feature search for all Latent Fingerprint Identification Search requests.

NGI shall perform a fingerprint search of the default repository, when the repository is not specified in the Latent Fingerprint Identification Search request.

NGI shall perform a rolled fingerprint search of the repository(ies) designated in the Latent Fingerprint Identification Search request.

NGI shall perform a flat fingerprint search of the repository(ies) designated in the Latent Fingerprint Identification Search request.

Latent Fingerprint Identification Search requests will be searched against both flat and rolled NGI fingerprint records.

NGI shall perform the Latent Fingerprint Identification Search requests against all individual event fingerprint features (non-composite), including plain impressions.

NGI shall perform a fingerprint search against the RISC for all Latent Fingerprint Identification Search requests.

NGI shall calculate a match score for each candidate resulting from a Latent Fingerprint Identification Search Request.

Deleted.

NGI shall perform a cascaded fingerprint search of the marked SPC Files as a result of all Latent Fingerprint Identification Search requests in accordance with cascaded search business rules.

NGI shall require an Authorized FBI Service Provider to perform a manual special processing review when one or more candidates are marked with a special processing indicator (e.g., SPF) as part of a Latent Fingerprint Identification Search request.

NGI shall allow an Authorized FBI Service Provider to perform a manual LFIC for each candidate for a Latent Fingerprint Identification Search request.

NGI shall allow an Authorized FBI Service Provider to reject a Latent Fingerprint Identification Search request.

NGI shall enroll Identity information into the ULF when indicated as part of a Latent Fingerprint Identification Search request that results in a non-identification decision.

NGI shall reject a Latent Fingerprint Identification Search request when the fingerprint images fail to satisfy minimum image quality standards.

NGI shall determine the response distribution method (i.e., electronic or hardcopy) for a Latent Fingerprint Identification Search response.

3.1.2.3 Latent Fingerprint Identification Outputs

NGI shall provide an Authorized Contributor with an identification decision, when applicable, as part of a Latent Fingerprint Identification Search response.

An identification decision will be a positive identification, non-identification, or inconclusive decision.

NGI shall provide the Identity History Summary for a positive identification in the Latent Fingerprint Identification Search response when requested.

NGI shall provide a reject response, as appropriate, for a Latent Fingerprint Identification Search request.

NGI shall provide a response to a Latent Fingerprint Identification Search request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports a Latent Fingerprint Identification Search response is LSR.

NGI shall provide the appropriate Latent Fingerprint Identification Search response to an Authorized FBI Service Provider.

NGI shall provide a hardcopy response to a Latent Fingerprint Identification Search request, as appropriate.

3.1.3 Rapid Fingerprint Identification Services

The RISC Rapid Search functionality provides the capability to perform an identification search against a limited population with a significantly reduced response time in comparison to Tenprint Fingerprint Identification Search response times. These Rapid Fingerprint Identification Searches are directed against the RISC, which is anticipated to contain records for Wanted Persons, Known or Suspected Terrorists, and other persons of special interest. This rapid search functionality also includes cascading

searches of the ULF and marked SPC Files after a Rapid Search response has been provided to the Authorized Contributor.

3.1.3.1 Rapid Fingerprint Identification Inputs

NGI shall accept a RISC Rapid Search request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports RISC Rapid Search request is RPIS.

NGI shall accept a RISC Rapid Search request from an Authorized Contributor in accordance with the latest III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC Message Key (MKE) for a RISC Rapid Search request will be developed in accordance with the NGI Message Definition Database (MDD).

These RISC Rapid Searches may be submitted via the NCIC communications network.

NGI shall accept ten or fewer flat fingerprints as part of a RISC Rapid Search request.

NGI shall accept ten or fewer rolled fingerprints as part of a RISC Rapid Search request.

NGI shall accept an indicator on a RISC Rapid Search request that specifies if the most recent frontal facial photo should be included as part of the RISC Rapid Search response if available.

NGI shall accept an indicator on a RISC Rapid Search request that specifies if an Identity History Summary should be returned as part of the RISC Rapid Search response.

3.1.3.2 Rapid Fingerprint Identification Processing

NGI shall extract fingerprint features from the fingerprint images provided in the RISC Rapid Search request.

NGI shall perform an automated fingerprint image quality check on a RISC Rapid Search request based on image quality standards.

NGI shall reject a RISC Rapid Search request when the fingerprint images fail to satisfy minimum fingerprint image quality standards.

NGI shall perform a rolled fingerprint search of the RISC repository as part of a RISC Rapid Search request.

NGI shall perform a flat fingerprint search of the RISC repository as part of a RISC Rapid Search request.

RISC Rapid Search requests will be searched against both flat and rolled NGI fingerprint records.

NGI shall perform all RISC Rapid Search requests against composite fingerprints.

NGI shall perform a fingerprint feature search of the RISC repository for all RISC Rapid Search requests.

NGI shall calculate a match score for each candidate resulting from a RISC Rapid Search request.

NGI shall determine a positive identification decision for each candidate that has a match score above the high confidence threshold as part of a RISC Rapid Search request.

NGI shall perform a cascaded fingerprint search of the ULF, in accordance with cascaded search business rules, if the fingerprints submitted with the RISC Rapid Search request meet the minimum quality standards in accordance with cascaded search business rules.

NGI shall perform a cascaded fingerprint search of the marked SPC Files designated for cascaded searches, in accordance with cascaded search business rules, if the fingerprints submitted with the RISC Rapid Search request meet the minimum quality standards in accordance with cascaded search business rules.

3.1.3.3 Rapid Fingerprint Identification Outputs

NGI shall provide a response to a RISC Rapid Search request based on multi-tiered dissemination rules.

NGI shall provide a "Red Light" indicator as part of a RISC Rapid Search response for a positive identification resulting from a RISC Rapid Search request.

NGI shall provide a "Green Light" indicator as part of a RISC Rapid Search response, when the match scores for all candidate(s) resulting from a RISC Rapid Search request are below the low confidence threshold.

NGI shall provide a "Green Light" indicator as part of a RISC Rapid Search response, when no candidates result from a RISC Rapid Search request.

NGI shall provide a "Yellow Light" indicator as part of a RISC Rapid Search response, when a candidate(s) resulting from a RISC Rapid Search request is found whose match score is above the low confidence threshold and below the high confidence threshold.

See Appendix E RISC Candidate Evaluation for a table clarifying the distinction between green, red and yellow indicators.

NGI shall optionally include, on a RISC Rapid Search response, an Identity History Summary.

NGI will not retrieve Identity History information from III/NFF States for Identity History Summaries that are included in RISC Rapid Search Responses. The Identity History Summaries will indicate that additional Identity History information is available from III/NFF States.

NGI shall provide a RISC record type indicator (e.g., Wanted Person, KST) for each candidate returned as part of a RISC Rapid Search response.

NGI shall optionally include, on a RISC Rapid Search response, the most recently taken frontal facial photo.

NGI shall optionally include, on a RISC Rapid Search response, the most recently taken facial photo when no frontal facial photo is available.

NGI shall provide a reject response for a RISC Rapid Search request when the associated fingerprints fail to satisfy minimum fingerprint image quality standards.

NGI shall provide a response to a RISC Rapid Search request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports a RISC Rapid Search response is RPISR.

NGI shall provide a response to a RISC Rapid Search request received via NCIC in accordance with the latest III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE for a RISC Rapid Search response will be developed in accordance with the NGI Message Definition Database (MDD).

3.1.4 International Terrorist Identification Services

The International Terrorist Identification Searches will be performed against the RISC Repository.

3.1.4.1 International Terrorist Identification Inputs

NGI shall accept an International Terrorist Identification Search request from an Authorized Domestic Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports an International Terrorist Identification Search request from an Authorized Domestic Contributor will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept an International Terrorist Identification Search request from an Authorized International Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports an International Terrorist Identification Search request from an Authorized International Contributor will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept an International Terrorist Identification Search request from an Authorized International Contributor in accordance with the latest ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

The ANSI/NIST-ITL TOT that supports an International Terrorist Identification Search will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit an International Terrorist Identification Search request.

The NGI STOT that supports an International Terrorist Identification Search will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to input fingerprint images to initiate an International Terrorist Identification Search request.

The NGI workstation will support multiple input methods for biometric images (scanning, CD-ROM, and other removable media). These methods will support the standards for output stated in ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, Data Format for the Interchange of Fingerprint Information" and with the EBTS.

NGI shall accept ten or fewer flat fingerprints as part of an International Terrorist Identification Search request.

NGI shall accept ten or fewer rolled fingerprints as part of an International Terrorist Identification Search request.

NGI shall accept palmprints as part of an International Terrorist Identification Search request.

NGI shall accept photos as part of an International Terrorist Identification Search request.

NGI shall accept iris data as part of an International Terrorist Identification Search request.

NGI shall accept supplemental fingerprint and palmprint information as part of an International Terrorist Identification Search request.

NGI shall accept an indicator on an International Terrorist Identification Search request that specifies if the most recent facial photo should be included as part of the response.

NGI shall accept an indicator on an International Terrorist Identification Search request that specifies whether or not the Identity should be enrolled into the ITF subset of the RISC repository.

NGI shall require an indicator on a retained International Terrorist Identification Search request that specifies which dissemination tier to apply to the enrolled Identity.

NGI shall accept an indicator on a retained International Terrorist Identification Search request that specifies whether or not an enrolled tier-1 or tier-2 Identity should be marked for hit notifications to the ITF record owner.

Multiple agencies can mark the same NGI Identity within the RISC repository with dissemination levels unique for their agency. Each agency will be able to set a dissemination tier level and indicate whether they will be notified upon a positive identification. NGI provides a multi-tier dissemination structure that is defined as follows: tier 1 – Share All; tier 2 – Point of Contact Only; tier 3 – Silent Hit.

3.1.4.2 International Terrorist Identification Processing

NGI shall perform ASC of the individual fingerprint impressions to the plain fingerprint impressions contained in an International Terrorist Identification Search request to determine if the individual fingerprint impressions are correctly sequenced.

NGI shall reject an International Terrorist Identification Search request as part of ASC when fingerprint data fails to meet processing criteria in accordance with ASC business rules.

NGI shall require an Authorized FBI Service Provider to perform manual FSC on an International Terrorist Identification Search request when ASC determines that manual review is necessary.

NGI shall allow an Authorized FBI Service Provider to reject an International Terrorist Identification Search request as part of manual FSC when fingerprint data fails to meet processing criteria.

Processing criteria is based on the Authorized FBI Service Providers' FSC Standard Operating Manual (SOM).

NGI shall extract fingerprint features from the fingerprint images provided in an International Terrorist Identification Search request.

NGI shall perform an automated image quality check on an International Terrorist Identification Search request based on image quality standards.

NGI shall reject an International Terrorist Identification Search request when the associated fingerprints do not meet minimum fingerprint image quality standards.

The reject will provide contact information to the Contributor indicating that they may submit a Tenprint card to the FBI for manual processing.

NGI shall perform an International Terrorist Identification Search request against composite fingerprints.

NGI shall perform a rolled fingerprint search of the RISC repository as part of an International Terrorist Identification Search request.

NGI shall perform a flat fingerprint search of the RISC repository as part of an International Terrorist Identification Search request.

International Terrorist Identification Search requests will be searched against both flat and rolled NGI fingerprint records.

NGI shall perform a fingerprint feature search for all International Terrorist Identification Search requests.

NGI shall calculate a match score for each candidate resulting from an International Terrorist Identification Search request.

NGI shall determine a positive identification decision for each candidate that has a match score above the high confidence threshold as part of an International Terrorist Identification Search request.

NGI shall require an Authorized FBI Service Provider to perform a manual FIC for each candidate with a match score that is below the high confidence threshold as part of an International Terrorist Identification Search request.

NGI shall allow an Authorized FBI Service Provider to reject an International Terrorist Identification Search request as a result of the manual FIC.

NGI shall require a second Authorized FBI Service Provider to perform a manual FIC to confirm a positive identification for each candidate with a match score that is below the low confidence threshold as part of an International Terrorist Identification Search request.

The second manual FIC will be performed independent of the first FIC decision. The decision made by the first service provider will not be made known to the second service provider.

NGI shall retrieve the corresponding subject's Identity history information when a tier-1 candidate results in a positive identification decision as part of an International Terrorist Identification Search request.

NGI shall retrieve Identity history information from III/NFF State systems, when a tier-1 candidate results in a positive Identification decision and the Identity contains an NFF Indicator, as part of an International Terrorist Identification Search request.

NGI will solicit the III/NFF State for its portion of the criminal history. The response from the III/NFF State Participant will be merged or appended to the NGI response and returned to the submitter of the search. These queries will be sent to states over the NCIC network. The responses will be sent to NGI over Nlets, assembled by NGI, and returned to the requester.

NGI shall forward an International Terrorist Identification Search request to an ITF participating International organization in accordance with the latest EBTS version.

The EBTS TOT that supports an International Terrorist Identification Search request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall forward an International Terrorist Identification Search request to an ITF participating International organization in accordance with the latest ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

The ANSI/NIST-ITL TOT that supports an International Terrorist Identification Search request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept an International Terrorist Identification Search response from an International organization in accordance with the latest EBTS version.

The EBTS TOT that supports an International Terrorist Identification Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept an International Terrorist Identification Search response from an International organization in accordance with the latest ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

The ANSI/NIST-ITL TOT that supports an International Terrorist Identification Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall enroll an Identity into the ITF subset of the RISC repository as part of a retained International Terrorist Identification Search request that results in a non-identification decision.

NGI shall update Identity history information based on file maintenance rules as a result of an International Terrorist Identification Search request with a positive identification decision.

NGI shall update fingerprint information based on file maintenance rules as a result of an International Terrorist Identification Search request with a positive identification decision.

NGI shall update a fingerprint composite as part of a retained International Terrorist Identification Search request, when the quality of the submitted fingerprints is better.

NGI shall assign the multi-tier dissemination level specified in the International Terrorist Identification Search request to the Identity when enrolling fingerprint data into the RISC repository.

NGI shall enroll palmprints in the ITF subset of the RISC repository based on file maintenance rules as part of an International Terrorist Identification Search request.

NGI shall enroll photos in the ITF subset of the RISC repository based on file maintenance rules as part of an International Terrorist Identification Search request.

NGI shall enroll iris data in the ITF subset of the RISC repository based on file maintenance rules as part of an International Terrorist Identification Search request.

NGI shall enroll supplemental fingerprint and palmprint information in the ITF subset of the RISC repository based on file maintenance rules as part of an International Terrorist Identification Search request.

NGI shall reject palmprint enrollment when the associated International Terrorist Identification Search request is rejected.

NGI shall reject photo enrollment when the associated International Terrorist Identification Search request is rejected.

NGI shall reject iris data enrollment when the associated International Terrorist Identification Search request is rejected.

NGI shall reject supplemental fingerprint and palmprint information enrollment when the associated International Terrorist Identification Search request is rejected.

NGI shall create a copy of the International Terrorist Identification Search request for the NGI Certification File based on file maintenance rules.

NGI shall perform a cascaded fingerprint search of the ULF, in accordance with cascaded search business rules, when the fingerprints submitted with an International Terrorist Identification Search request meet the minimum quality standards.

NGI shall perform a cascaded fingerprint search of marked SPC Files, in accordance with cascaded search business rules, when the fingerprints submitted with an International Terrorist Identification Search request meet the minimum quality standards.

NGI shall determine the response distribution method (i.e., electronic or hardcopy) for an International Terrorist Identification Search response.

NGI shall perform a cascaded facial recognition search of the UPF, in accordance with cascaded search business rules, when the photo submitted with a International Terrorist Identification Search request meets the minimum quality standard for facial recognition.

NGI shall perform a cascaded facial recognition search of marked SPC Files, in accordance with cascaded search business rules, when the photo submitted with an International Terrorist Identification Search request meets the minimum quality standard for facial recognition.

NGI shall perform a cascaded palmprint search of the ULF, in accordance with cascaded search business rules, when the palmprint submitted with an International Terrorist Identification Search request meets the minimum quality standard for palmprints.

NGI shall perform a cascaded palmprint search of the marked SPC Files, in accordance with cascaded search business rules, if the palmprint submitted with an International Terrorist Identification Search request meets the minimum quality standard for palmprints.

NGI shall perform a cascaded supplemental fingerprint and palmprint search of the ULF, in accordance with cascaded search business rules, when the supplemental fingerprint and palmprint submitted with an International Terrorist Identification Search request meets the minimum quality standard for supplemental fingerprint and palmprints.

NGI shall perform a cascaded supplemental fingerprint and palmprint search of the marked SPC Files, in accordance with cascaded search business rules, if the supplemental fingerprint and palmprint submitted with an International Terrorist Identification Search request meets the minimum quality standard for supplemental fingerprint and palmprints.

NGI shall perform a cascaded search of the UIF, in accordance with cascaded search business rules, when the iris data submitted with an International Terrorist Identification Search request meets the minimum quality standard for iris searches.

NGI shall perform a cascaded search of marked SPC File(s), in accordance with cascaded search business rules, when the iris data submitted with an International Terrorist Identification Search request meets the minimum quality standard for iris searches.

3.1.4.3 International Terrorist Identification Outputs

NGI shall provide an Authorized Domestic Contributor with an identification decision as part of an International Terrorist Identification Search response.

NGI shall provide an Authorized International Contributor with an identification decision as part of an International Terrorist Identification Search response.

An identification decision will be either a positive identification or a non-identification.

NGI shall provide a response to an International Terrorist Identification Search request, when appropriate, in accordance with the latest EBTS version.

The EBTS TOT that supports an International Terrorist Identification Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide a response to an International Terrorist Identification Search request, when appropriate, in accordance with the latest ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

The ANSI/NIST-ITL TOT that supports an International Terrorist Identification Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate International Terrorist Identification Search response to an Authorized FBI Service Provider.

NGI shall provide a response to an International Terrorist Identification Search request based on multi-tiered dissemination rules.

NGI shall provide the NGI portion of an International Terrorist Identification Search response upon completion of the NGI search.

NGI shall provide an Identity History Summary in response to an International Terrorist Identification Search request that results in a positive identification to a tier-1 Identity.

NGI shall provide contact information in response to an International Terrorist Identification Search request that results in a positive identification to a tier-2 Identity.

NGI shall provide a non-identification response to an International Terrorist Identification Search request that results in a positive identification to a tier-3 Identity.

NGI shall optionally include, on a tier-1 International Terrorist Identification Search response, the most recently taken frontal facial photo.

NGI shall optionally include, on a tier-1 International Terrorist Identification Search response, the most recently taken facial photo when no frontal facial photo is available.

NGI shall combine the NGI International Terrorist Identification Search request results with the Identity History information retrieved from III/NFF State systems, when all III/NFF Identity History information is available within the response time threshold required to create a combined response.

NGI shall provide partial International Terrorist Identification Search request results as part of an International Terrorist Identification Search response when III/NFF State systems do not meet the response time threshold required to create a combined response.

A partial response will include information to indicate that the III/NFF State system did not provide Identity History information within the NGI response time.

NGI shall forward International Terrorist Identification Search responses from International organizations back to the original requestor independent from the NGI response.

NGI shall provide a reject response, as appropriate, for an International Terrorist Identification Search request.

NGI shall advise the Record Owner when the palmprint data is enrolled as a result of an International Terrorist Identification Search, but fails to meet minimum quality standards for searches.

NGI shall advise the Record Owner when a photo is enrolled as a result of an International Terrorist Identification Search, but fails to meet minimum quality standards for searches.

NGI shall advise the Record Owner when iris data is enrolled as a result of an International Terrorist Identification Search, but fails to meet minimum quality standards for searches.

NGI shall advise the Record Owner when the supplemental fingerprint and palmprint information is enrolled as a result of an International Terrorist Identification Search, but fails to meet minimum quality standards for searches.

3.1.5 Disposition Fingerprint Submissions

The Disposition Fingerprint Submission Service will allow an Authorized Contributor to submit a disposition request with fingerprints. The fingerprints will be used to identify the subject in NGI that is associated with the disposition information. If no subject can be identified using the fingerprints, a new Identity will be created for the disposition information.

3.1.5.1 Disposition Fingerprint Submission Inputs

NGI shall accept Disposition Fingerprint Search requests from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports Disposition Fingerprint Search requests is FDSP.

NGI shall accept rolled fingerprint images as part of the Disposition Fingerprint Search request.

NGI shall accept flat fingerprint images as part of the Disposition Fingerprint Search request.

NGI shall require the designated repository to be criminal as part of a Disposition Fingerprint Search request.

NGI shall accept a designation of transaction priority by which the Disposition Fingerprint Search request should be performed.

NGI shall accept supplemental fingerprint and palmprint information as part of a Disposition Fingerprint Search request.

NGI shall accept photo input from an Authorized Contributor as part of a Disposition Fingerprint Search request.

NGI shall accept a multi-level SMT photo descriptor field as part of a Disposition Fingerprint Search request.

NGI shall accept an indicator on a Disposition Fingerprint Search request that specifies if a photo should be included with the fingerprint search response.

NGI shall accept palmprint images from an Authorized Contributor as part of a Disposition Fingerprint Search request.

NGI shall accept iris data input from an Authorized Contributor as part of a Disposition Fingerprint Search request.

NGI shall accept a UCN as part of a Disposition Fingerprint Search request.

NGI will optionally accept one or more quoted UCNs when a contributor has made an identification at the state level.

NGI shall accept an Identity History Summary indicator as part of a Disposition Fingerprint Search request.

The Identity History Summary indicator will be used to determine if an Identity History Summary should be included as part of a Disposition Fingerprint Search response for a positive identification decision.

3.1.5.2 Disposition Fingerprint Submission Processing

NGI shall perform AQC of textual data contained in a Disposition Fingerprint Search request against the AQC business rules.

NGI has the capability to make a pass or fail decision through a rule-based AQC process. Disposition Submission requests that are rejected from Manual Quality Check are forwarded to conflict resolution.

NGI shall require an Authorized FBI Service Provider to perform Manual Quality Check on a Disposition Fingerprint Search request when AQC business rules determine manual review is necessary.

NGI shall reject a Disposition Fingerprint Search request when textual information is invalid based on AQC business rules.

NGI shall provide Conflict Resolution for a Disposition Fingerprint Search request when AQC business rules determine manual review is necessary.

NGI shall perform ASC of the individual fingerprint impressions to the plain fingerprint impressions contained in a Disposition Fingerprint Search request to determine if the individual fingerprint impressions are correctly sequenced.

NGI shall reject a Disposition Fingerprint Search request as part of ASC when fingerprint data fails to meet processing criteria in accordance with ASC business rules.

NGI shall require an Authorized FBI Service Provider to perform manual FSC on a Disposition Fingerprint Search request when ASC determines that manual review is necessary.

NGI shall allow an Authorized FBI Service Provider to reject a Disposition Fingerprint Search request as part of manual FSC when fingerprint data fails to meet processing criteria.

Processing criteria is based on the Authorized FBI Service Providers' FSC SOM.

NGI shall provide Conflict Resolution for a Disposition Fingerprint Search request that is rejected from manual FSC.

NGI shall extract fingerprint features from the fingerprint images provided in a Disposition Fingerprint Search request.

NGI shall perform an image quality check on a Disposition Fingerprint Search request based on image quality standards.

NGI shall reject a Disposition Fingerprint Search request when the fingerprint images fail to satisfy minimum fingerprint image quality standards.

NGI shall provide Conflict Resolution for a Disposition Fingerprint Search request that is rejected as a result of fingerprint images that fail to satisfy minimum fingerprint image quality standards.

NGI shall mark the Disposition Fingerprint Search request as SBDA when the submitted fingerprint data fails to satisfy fingerprint image quality for retention.

The SBDA indicator allows tenprint fingerprint data of a defined quality to be used in a search of the NGI repositories, but not allow the images and features to be added to the NGI repository(ies).

NGI shall provide Conflict Resolution for a Disposition Fingerprint Search request when the search is marked as SBDA and results in a non-identification decision.

Deleted.

NGI shall perform all Disposition Fingerprint Search requests against composite fingerprints.

NGI shall prioritize a Disposition Fingerprint Search request using established and specified priority criteria.

NGI shall perform a rolled fingerprint search against the RISC for all Disposition Fingerprint Search requests.

NGI shall perform a flat fingerprint search against the RISC for all Disposition Fingerprint Search requests.

Fingerprint Search results of the RISC repository will be included in the Disposition Fingerprint Search response.

When an incoming submission references at least one UCN, a fingerprint comparison of each quoted UCN is made prior to a biometric search and/or name search.

Disposition Fingerprint Search requests will be searched against both flat and rolled NGI fingerprint records.

NGI shall perform a Subject Search of the designated NGI repository for candidates based on biographic data provided for all Disposition Fingerprint Search requests.

NGI shall perform III/Verify as part of a Disposition Fingerprint Search request for each quoted UCN and each Subject Search candidate.

NGI shall compare the fingerprint features extracted from the fingerprint images provided in the Disposition Fingerprint Search request against the fingerprint features of each candidate provided to III/Verify.

NGI shall calculate a match score for each candidate resulting from a Disposition Fingerprint Search request.

NGI will determine a match score for each quoted UCN, Subject Search candidate or Feature Search candidate.

NGI shall require an Authorized FBI Service Provider to perform a manual special processing review when one or more candidates are marked with a special processing indicator (e.g., SPF) as part of a Disposition Fingerprint Search request.

NGI shall eliminate each candidate that has a match score below the minimum threshold for III/Verify as part of a Disposition Fingerprint Search request.

NGI shall perform a fingerprint feature search for all Disposition Fingerprint Search requests.

NGI shall determine a positive identification decision for each candidate that has a match score above the high confidence threshold as part of a Disposition Fingerprint Search request.

Identification decisions may require manual FIC, depending on the match score. If the match score is above the high confidence threshold ("Lights Out"), then no manual FIC is required. If the match score is below the high confidence threshold, and above the low confidence threshold, then one manual FIC is required. If the match score is below the low confidence threshold, then two manual FICs are required.

NGI shall require an Authorized FBI Service Provider to perform a manual FIC for each candidate with a match score that is below the high confidence threshold as part of a Disposition Fingerprint Search request.

NGI shall require a second Authorized FBI Service Provider to perform a manual FIC to confirm a positive identification for each candidate with a match score that is below the low confidence threshold as part of a Disposition Fingerprint Search request.

The second manual FIC will be performed independent of the first FIC decision. The decision made by the first service provider will not be made known to the second service provider.

NGI shall allow an Authorized FBI Service Provider to reject a Disposition Fingerprint Search request as a result of the manual FIC.

NGI shall provide Conflict Resolution for a Disposition Fingerprint Search request that is rejected as a result of the manual FIC.

NGI shall retrieve the corresponding subject's Identity History information when requested and a positive identification decision results from a Disposition Fingerprint Search request.

NGI shall retrieve Identity History information from III/NFF State systems when a positive identification decision is made to an Identity that contains an NFF indicator as part of a Disposition Fingerprint Search request.

The FBI will solicit the III/NFF State for their portion of the criminal history. The response from the III/NFF State Participant will be merged or appended to the FBI's response and returned to the submitter of the search. These queries will be sent to states over the NCIC network. The responses will be sent to NGI over Nlets, assembled by NGI, and returned to the requester.

NGI shall perform a fingerprint search of the criminal repository to determine the Identity associated with the Disposition Fingerprint Search request.

NGI shall create a new Identity with a default arrest cycle and submitted disposition data when the Disposition Fingerprint Search request results in a non identification decision.

NGI shall enroll Identity information for the newly created Identity into the appropriate NGI repository as a result of a retained Disposition Fingerprint Search request that results in a non-identification decision.

NGI shall enroll the fingerprint data in the designated repository(ies) based on file maintenance rules as part of a retained Disposition Fingerprint Search request.

NGI shall provide the capability to uniquely identify fingerprint data enrolled as a result of a Disposition Fingerprint Search request.

NGI shall perform a validation to ensure that submitted palmprint images match the submitted fingerprints, when the distal segments of the palmprint images are included in the Disposition Fingerprint Search request.

NGI shall enroll the photos in the designated repository based on file maintenance rules as part of a Disposition Fingerprint Search request.

NGI shall provide the capability to uniquely identify photos enrolled as a result of Disposition Fingerprint Search request.

NGI shall enroll the palmprints in the designated repository based on file maintenance rules as part of a Disposition Fingerprint Search request.

NGI shall provide the capability to uniquely identify palmprints enrolled as a result of a Disposition Fingerprint Search request.

NGI shall enroll the iris data in the designated repository based on file maintenance rules as part of a Disposition Fingerprint Search request.

NGI shall provide the capability to uniquely identify iris data enrolled as a result of a Disposition Fingerprint Search request.

NGI shall enroll supplemental fingerprint and palmprint information into the designated repository based on file maintenance rules as part of a Disposition Fingerprint Search request.

NGI shall perform a validation to ensure that submitted supplemental fingerprint and palmprint images match the submitted fingerprints, when the distal segments of the supplemental fingerprint and palmprint images are included in the Disposition Fingerprint Search request.

NGI shall provide the capability to uniquely identify supplemental fingerprint and palmprint data enrolled as a result of a Disposition Fingerprint Search request.

NGI shall reject a photo enrollment when the associated Disposition Fingerprint Search request is rejected.

NGI shall reject a palmprint enrollment when the associated Disposition Fingerprint Search request is rejected.

NGI shall reject an iris enrollment when the associated Disposition Fingerprint Search request is rejected.

NGI shall reject the supplemental fingerprint and palmprint information enrollment when the associated Disposition Fingerprint Search request is rejected.

NGI shall maintain an Identity based on file maintenance rules as a result of a Disposition Fingerprint Search request with a positive identification decision.

NGI shall update the identified subject with disposition data from a Disposition Fingerprint Search request when a unique arrest cycle exists on the identified subject that matches the submitted Date of Arrest (DOA) and Originating Agency Identifier (ORI), and a disposition for that DOA does not already exist.

NGI shall require an Authorized FBI Service Provider to perform conflict resolution for a Disposition Fingerprint Search request when submitted disposition data cannot be automatically applied to an Identity.

NGI shall update fingerprint information based on file maintenance rules as a result of a Disposition Fingerprint Search request with a positive identification decision.

NGI shall create a copy of the Disposition Fingerprint Search request for the NGI Certification File based on file maintenance rules.

NGI shall send an External Tenprint Fingerprint Identification Search request when a retained Disposition Fingerprint Search request results in a non-identification decision (i.e., new NGI enrollment) based on External System Search rules.

NGI shall send an External Tenprint Fingerprint Identification Search request to an External System, when the external system is not IDENT, in accordance with the latest EBTS version as part of a Disposition Fingerprint Search request.

The EBTS TOT that supports an External Tenprint Fingerprint Identification Search request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall send an External Tenprint Fingerprint Identification Search request to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement as part of a Disposition Fingerprint Search request.

NGI shall send an External Tenprint Fingerprint Identification Search request, based on External System Search rules, when fingerprint image quality exceeds the quality improvement threshold and a link to the External System does not exist, as part of a Disposition Fingerprint Search request.

NGI shall indicate in an External Tenprint Fingerprint Identification Search request against an external repository whether or not the External System should establish a link when the external system search results in a positive identification, as part of a Disposition Fingerprint Search request.

NGI shall include biographic data in an External Tenprint Fingerprint Identification Search request, as part of a Disposition Fingerprint Search request.

NGI shall include a unique transaction control number (TCN) in an External Tenprint Fingerprint Identification Search request, as part of a Disposition Fingerprint Search request.

NGI shall record the correlation between the identified UCN and the unique transaction control number (TCN) included in an External Tenprint Fingerprint Identification Search request when a Disposition Fingerprint Search request results in a positive identification.

NGI shall record the correlation between the UCN assigned to the newly enrolled identity and the unique transaction control number (TCN) included in an External Tenprint Fingerprint Identification Search request when a Disposition Fingerprint Search request results in a non-identification decision.

NGI shall accept a response from an External System, when the external system is not IDENT, as a result of an External Tenprint Fingerprint Identification Search request of external repositories in accordance with the latest EBTS version, as part of a Disposition Fingerprint Search request.

The EBTS TOT that supports an External Tenprint Fingerprint Identification Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a unique transaction control number (TCN) from an External System (e.g., IDENT) in a response to an External Tenprint Fingerprint Identification Search request as part of a Disposition Fingerprint Search request.

NGI shall determine the UCN using the unique transaction control number (TCN) returned in an External Tenprint Fingerprint Identification Search response, and the previously recorded UCN/TCN correlation when an External Tenprint Fingerprint Identification Search results in a positive identification as part of a Disposition Fingerprint Search request.

NGI shall send a TCN/UCN correlation message to an External System (e.g., IDENT), providing the Identified UCN when an External Tenprint Fingerprint Identification Search results in a positive identification as part of a Disposition Fingerprint Search request.

NGI shall send a TCN/UCN correlation message to an External System in accordance with the latest EBTS version when the external system is not IDENT as part of a Disposition Fingerprint Search request.

NGI shall send a TCN/UCN correlation message to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement as part of a Disposition Fingerprint Search request.

NGI shall accept a response from an External IDENT as a result of an External Tenprint Fingerprint Identification Search request of external repositories in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement, as part of a Disposition Fingerprint Search request.

NGI shall update an Identity with the information contained in an External Tenprint Fingerprint Identification Search response from an External System (e.g., IDENT) as a result of a Disposition Fingerprint Search request.

NGI shall send an External Unsolved Latent Search request when a retained Disposition Fingerprint Search request results in a non-identification decision (i.e., new NGI enrollment) based on External System Search rules.

NGI shall send an External Unsolved Latent Search request when fingerprint image quality exceeds the quality improvement threshold as part of a Disposition Fingerprint Search request based on External System Search rules.

NGI shall perform a cascaded fingerprint search of the ULF, in accordance with cascaded search business rules, as a result of Disposition Fingerprint Search requests.

NGI shall perform a cascaded fingerprint search of the marked SPC Files, in accordance with cascaded search business rules, as a result of Disposition Fingerprint Search requests.

NGI shall perform a cascaded facial recognition search of the UPF when the photo submitted with a Disposition Fingerprint Search request meets the minimum quality standard for facial recognition in accordance with cascaded search business rules.

NGI shall perform a cascaded facial recognition search of marked SPC Files when the photo submitted with a Disposition Fingerprint Search request meets the minimum quality standard for facial recognition in accordance with cascaded search business rules.

NGI shall perform a cascaded palmprint search of the ULF when the palmprint submitted with a Disposition Fingerprint Search request meets the minimum quality standard for palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded palmprint search of the marked SPC Files designated for cascaded searches, if the palmprint submitted with a Disposition Fingerprint Search request meets the minimum quality standard for palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded supplemental fingerprint and palmprint search of the ULF when the supplemental fingerprint and palmprint submitted with a Disposition Fingerprint Search request meets the minimum quality standard for supplemental fingerprint and palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded supplemental fingerprint and palmprint search of the marked SPC Files designated for cascaded searches, if the supplemental fingerprint and palmprint submitted with a Disposition Fingerprint Search request meets the minimum quality standard for supplemental fingerprint and palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded search of the UIF when the iris data submitted with a Disposition Fingerprint Search request meets the minimum quality standard for iris searches in accordance with cascaded search business rules.

NGI shall perform a cascaded search of marked SPC File(s) when the iris data submitted with a Disposition Fingerprint Search request meets the minimum quality standard for iris searches in accordance with cascaded search business rules.

NGI shall send a Hot Check Name Search request to NCIC for all Disposition Fingerprint Search requests.

NGI shall determine the response distribution method (i.e., electronic or hardcopy) for a Disposition Fingerprint Search response.

3.1.5.3 Disposition Fingerprint Submission Outputs

NGI shall provide a response to a Disposition Fingerprint Search request in accordance with the latest EBTS version.

The EBTS TOT that supports a Disposition Fingerprint Search response is DSPR.

NGI shall provide the Identity History Summary for a positive identification candidate in the Disposition Fingerprint Search response, when requested.

NGI shall optionally include, on a Disposition Fingerprint Search response, the most recently taken frontal facial photo for the identified subject.

NGI shall optionally include, on a Disposition Fingerprint Search response, the most recently taken facial photo for the identified subject, when no frontal facial photo is available.

NGI shall combine the NGI Disposition Fingerprint Search request results with the Identity History information retrieved from III/NFF State systems, when all III/NFF Identity History information is available within the response time threshold required to create a combined response.

NGI shall provide partial Disposition Fingerprint Search request results as part of a Disposition Fingerprint Search response when III/NFF State systems do not meet the response time threshold required to create a combined response.

A partial response will include information to indicate that the III/NFF State system did not provide Identity History information within the NGI response time.

NGI shall provide a reject response, as appropriate, for a Disposition Fingerprint Search response.

NGI shall provide Authorized Contributors with an electronic response to a Disposition Fingerprint Search request in accordance with the latest EBTS version.

NGI shall provide a hardcopy response to a Disposition Fingerprint Search request, as appropriate.

NGI shall provide an initial partial response when a Disposition Fingerprint Search request results in a positive identification to a manual record.

NGI shall advise the Authorized Contributor when a photo is enrolled as a result of a Disposition Fingerprint Search request, but fails to meet minimum quality standards for facial recognition.

NGI shall advise the Authorized Contributor when a palmprint is enrolled as a result of a Disposition Fingerprint Search request, but fails to meet minimum quality standards for palmprint searching.

NGI shall advise the Authorized Contributor when a supplemental fingerprint and palmprint is enrolled as a result of a Disposition Fingerprint Search request, but fails to meet minimum quality standards for supplemental fingerprint and palmprint searching.

NGI shall advise the Authorized Contributor when a supplemental fingerprint and palmprint is not enrolled due to a failed validation of fingerprints to supplemental fingerprint and palmprints when processing a Disposition Fingerprint Search request.

NGI shall advise the Authorized Contributor when a palmprint is not enrolled due to a failed validation of fingerprints to palmprints when processing a Disposition Fingerprint Search request.

NGI shall advise the Authorized Contributor when iris data is enrolled as a result of a Disposition Fingerprint Search request, but fails to meet minimum quality standards for iris searches.

3.1.6 Rapid Tenprint Fingerprint Identifcation Services

The Rapid Tenprint Fingerprint Identification Service provides the capability to perform an identification type search with a significantly reduced response time in comparison to Tenprint Fingerprint Identification Search response times. These rapid responses will not include identity history information, photos or any other additional information. Only the criminal repository will be searched and no file maintenance activities will take place.

3.1.6.1 Rapid Tenprint Fingerprint Identifcation Inputs

NGI shall accept a Rapid Tenprint Fingerprint Identification Search request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall accept a Rapid Tenprint Fingerprint Identification Search request from an Authorized External System (e.g., IDENT) in accordance with the latest EBTS version.

The EBTS TOT that supports Rapid Tenprint Fingerprint Identification Search request is TBD. The RPIS TOT could be used with an NDR field indicator of "CMF".

NGI shall accept flat fingerprints as part of a Rapid Tenprint Fingerprint Identification Search request.

NGI shall require a designation of the NGI repository(ies) against which fingerprint data should be searched as part of a Rapid Tenprint Fingerprint Identification Search request.

3.1.6.2 Rapid Tenprint Fingerprint Identifcation Processing

NGI shall extract fingerprint features from the fingerprint images provided in the Rapid Tenprint Fingerprint Identification Search request.

NGI shall perform an automated fingerprint image quality check on a Rapid Tenprint Fingerprint Identification Search request based on image quality standards.

NGI shall reject a Rapid Tenprint Fingerprint Identification Search request when the fingerprint images fail to satisfy minimum fingerprint image quality standards.

NGI shall perform a flat fingerprint search of the repository(ies) designated in a Rapid Tenprint Fingerprint Identification Search request.

NGI shall perform all Rapid Tenprint Fingerprint Identification Search requests against composite fingerprints.

NGI shall search the designated repository(ies) using the extracted fingerprint features from the Rapid Tenprint Fingerprint Identification Search request.

NGI shall calculate a match score for each candidate resulting from a Rapid Tenprint Fingerprint Identification Search request.

3.1.6.3 Rapid Tenprint Fingerprint Identifcation Outputs

NGI shall provide a response to a Rapid Tenprint Fingerprint Identification Search request based on special processing indicator dissemination rules.

NGI shall provide a "Red Light" indicator as part of a Rapid Tenprint Fingerprint Identification Search response, when the match score for any candidate resulting from a Rapid Tenprint Fingerprint Identification Search request is above the high confidence threshold.

NGI shall provide a "Green Light" indicator as part of a Rapid Tenprint Fingerprint Identification Search response, when the match scores for all candidate(s) resulting from a Rapid Tenprint Fingerprint Identification Search request is equal to or below the high confidence threshold.

NGI shall provide a "Green Light" indicator as part of a Rapid Tenprint Fingerprint Identification Search response, when no candidates result from a Rapid Tenprint Fingerprint Identification Search request.

NGI shall provide a reject response for a Rapid Tenprint Fingerprint Identification Search request when the associated fingerprints fail to satisfy minimum fingerprint image quality standards.

NGI shall provide a response to a Rapid Tenprint Fingerprint Identification Search request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall provide a response to a Rapid Tenprint Fingerprint Identification Search request from an External System in accordance with the latest EBTS version.

The EBTS TOT that supports a Rapid Tenprint Fingerprint Identification Search response is TBD.

3.2 Verification Services Functional Requirements

This functionality provides services to users in support of biometric verification. It addresses Fingerprint Verification Searches that result in the confirmation of an individual's Identity based on a one-to-one comparison.

3.2.1 Fingerprint Verification Services

3.2.1.1 Fingerprint Verification Inputs

NGI shall accept a Fingerprint Verification request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall accept a Fingerprint Verification request from an Authorized External System (e.g., IDENT) in accordance with the latest EBTS version.

The EBTS TOT that supports Fingerprint Verification requests is FVR.

NGI shall accept a Fingerprint Verification request with ten or fewer rolled fingerprints.

NGI shall accept a Fingerprint Verification request with ten or fewer flat fingerprints.

NGI shall accept an indicator on a Fingerprint Verification request that specifies if an Identity History Summary should be included with the Fingerprint Verification response.

NGI shall require that a Fingerprint Verification request contains a UCN and fingerprint data.

3.2.1.2 Fingerprint Verification Processing

NGI shall perform AQC of textual data contained in a Fingerprint Verification request against the AQC business rules.

NGI shall reject a Fingerprint Verification request when textual information is invalid based on AQC business rules.

NGI shall require an Authorized FBI Service Provider to perform Manual Quality Check on a Fingerprint Verification request when AQC business rules determine manual review is necessary.

NGI shall allow an Authorized FBI Service Provider to reject a Fingerprint Verification request when it is determined to be invalid as part of Manual Quality Check.

NGI shall perform III/Verify as part of a Fingerprint Verification request for the UCN.

NGI shall extract fingerprint features from the fingerprint images provided in the Fingerprint Verification request.

NGI shall perform an image quality check on a Fingerprint Verification request based on image quality standards.NGI shall compare the fingerprint features extracted from the fingerprint images provided in the Fingerprint Verification request against the fingerprint features of the candidate provided to III/Verify.

NGI shall calculate a match score for the candidate resulting from a Fingerprint Verification request.

NGI shall determine a non-identification decision for a candidate that has a match score below the minimum threshold for III/Verify as part of a Fingerprint Verification request.

NGI shall determine a positive identification decision for a candidate that has a match score above the high confidence threshold as part of a Fingerprint Verification request.

NGI shall require an Authorized FBI Service Provider to perform a manual FIC when the candidate returned as part of the Fingerprint Verification request is below the high confidence threshold.

NGI shall require a second Authorized FBI Service Provider to perform a manual FIC to confirm a positive identification when the candidate returned as part of a Fingerprint Verification request is below the low confidence threshold.

The second manual FIC will be performed independent of the first FIC decision. The decision made by the first service provider will not be made known to the second service provider.

NGI shall allow an Authorized FBI Service Provider to reject a Fingerprint Verification request as a result of the manual FIC.

NGI shall retrieve the corresponding subject's Identity History information when requested and a positive identification decision results from a Fingerprint Verification request.

NGI shall reject a Fingerprint Verification request when a specified UCN does not exist.

NGI shall reject a Fingerprint Verification request when the submitted fingerprints fail to meet minimum quality standards.

NGI shall maintain an Identity based on file maintenance rules as a result of a Fingerprint Verification request with a positive identification decision.

NGI shall update fingerprint information based on file maintenance rules as a result of a Fingerprint Verification request with a positive identification decision.

NGI shall create a copy of the Fingerprint Verification request for the NGI Certification File based on file maintenance rules.

NGI shall perform a cascaded fingerprint search of the ULF, in accordance with cascaded search business rules, as a result of Fingerprint Verification requests.

NGI shall perform a cascaded fingerprint search of the marked SPC Files, in accordance with cascaded search business rules, as a result of Fingerprint Verification requests.

3.2.1.3 Fingerprint Verification Outputs

NGI shall provide a response to a Fingerprint Verification request in accordance with the latest EBTS version.

The EBTS TOT that supports a Fingerprint Verification response is SRE.

NGI shall provide an Identity History Summary in response to a Fingerprint Verification request resulting in a positive verification, when indicated.

NGI shall provide a positive verification response to a Fingerprint Verification request when submitted fingerprints and fingerprints associated with the specified UCN result in a positive identification.

NGI shall provide a negative verification response to a Fingerprint Verification request when submitted fingerprints and fingerprints associated with the specified UCN do not result in a positive identification.

NGI shall provide a reject response, as appropriate, for a Fingerprint Verification request.

NGI shall provide contact information in response to a Fingerprint Verification request resulting in a positive verification against a tier-2 RISC record.

NGI shall provide a negative verification response to a Fingerprint Verification request resulting in a positive verification against a tier-3 RISC record.

3.3 Information Services Functional Requirements

The following section contains the functional requirements supporting Information user services.

3.3.1 Fingerprint Image Retrieval Request

Fingerprint Image Retrieval requests allow Authorized Contributors to request fingerprint images for specific Identities and events. Authorized FBI Service Provider functionality for these requests is defined under the more general Fingerprint Information Retrieval request.

3.3.1.1 Fingerprint Image Retrieval Request Inputs

NGI shall accept a Fingerprint Image Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Fingerprint Image Retrieval requests is IRQ.

NGI shall require one or more UCNs up to a maximum number as part of a Fingerprint Image Retrieval request.

NGI shall accept an indicator on a Fingerprint Image Retrieval request that specifies if supplemental fingerprint and palmprint information should be provided in the response if available.

NGI shall accept fingerprint specific information as part of a Fingerprint Image Retrieval.

3.3.1.2 Fingerprint Image Retrieval Request Processing

NGI shall retrieve the composite fingerprint image for each specified UCN when fingerprint specific data is not provided as part of a Fingerprint Image Retrieval request.

NGI shall retrieve the fingerprint images associated with the fingerprint specific information provided in the Fingerprint Image Retrieval request.

NGI shall retrieve supplemental fingerprint and palm images associated with the fingerprint specific information, when indicated, as part of the Fingerprint Image Retrieval request.

NGI shall retrieve the most recent supplemental fingerprint and palm images for each specified UCN when fingerprint specific data is not provided as part of a Fingerprint Image Retrieval request.

NGI shall reject a Fingerprint Image Retrieval request when the specified UCN or specific fingerprint does not exist.

3.3.1.3 Fingerprint Image Retrieval Request Outputs

NGI shall provide a response to a Fingerprint Image Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports a Fingerprint Image Retrieval request is IRR, ISR.

3.3.2 Fingerprint Features Retrieval Request

Fingerprint Features Retrieval requests allow Authorized Contributors to request fingerprint features for specific fingerprints or the composite fingerprints for an Identity. Authorized FBI Service Provider functionality for these requests is defined under the more general Fingerprint Information Retrieval request.

3.3.2.1 Fingerprint Features Retrieval Request Inputs

NGI shall accept a Fingerprint Features Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Fingerprint Features Retrieval requests is IRQ.

NGI shall require one or more UCNs up to a maximum number as part of a Fingerprint Features Retrieval request.

NGI shall accept an indicator on a Fingerprint Features Retrieval request that specifies if supplemental fingerprint and palmprint information should be provided in the response, if available.

NGI shall accept fingerprint specific information as part of a Fingerprint Features Retrieval.

3.3.2.2 Fingerprint Features Retrieval Request Processing

NGI shall retrieve the composite fingerprint images and features for each specified UCN when fingerprint specific data is not provided as part of a Fingerprint Features Retrieval request.

NGI shall retrieve the fingerprint images associated with the fingerprint specific information provided in the Fingerprint Features Retrieval request.

NGI shall retrieve the fingerprint features associated with the fingerprint specific information provided in the Fingerprint Features Retrieval request.

NGI shall retrieve supplemental fingerprint and palm images, when indicated, as part of the Fingerprint Features Retrieval request.

NGI shall retrieve supplemental fingerprint and palm features, when indicated, as part of the Fingerprint Features Retrieval request.

NGI shall reject a Fingerprint Features Retrieval request when specified UCN or specific fingerprint does not exist.

3.3.2.3 Fingerprint Features Retrieval Request Outputs

NGI shall provide a response to a Fingerprint Features Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports a Fingerprint Features Retrieval response is IRR, ISR.

3.3.3 Fingerprint Audit Trail Retrieval Request

Fingerprint Audit Trail Retrieval requests allow Authorized Contributors to request the audit trail history for specific fingerprints. Authorized FBI Service Provider functionality for these requests is defined under the more general Fingerprint Information Retrieval request.

3.3.3.1 Fingerprint Audit Trail Retrieval Request Inputs

NGI shall accept a Fingerprint Audit Trail Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Fingerprint Audit Trail Retrieval requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a Fingerprint Audit Trail Retrieval request with a specified UCN and fingerprint specific information.

NGI shall accept an indicator on a Fingerprint Audit Trail Retrieval request that specifies if supplemental fingerprint and palmprint audit trail information should be provided in the response if available.

3.3.3.2 Fingerprint Audit Trail Retrieval Request Processing

NGI shall retrieve the fingerprint audit trail for the fingerprint specified in the Fingerprint Audit Trail Retrieval request.

NGI shall retrieve the audit trails for the supplemental fingerprints and palmprints when specified in the Fingerprint Audit Trail Retrieval request.

NGI shall reject a Fingerprint Audit Trail Retrieval request when a specified UCN or fingerprint does not exist.

NGI shall reject a Fingerprint Audit Trail Retrieval request when the Authorized Contributor is not the fingerprint owner.

3.3.3.3 Fingerprint Audit Trail Retrieval Request Outputs

NGI shall provide a response to a Fingerprint Audit Trail Retrieval request in accordance with the latest EBTS version.

NGI shall indicate on a Fingerprint Audit Trail Retrieval response whether the specified fingerprint was disseminated as part of the fingerprint composite.

The EBTS TOT that supports a Fingerprint Audit Trail Retrieval response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.3.4 Fingerprint Information Retrieval Request

The following functional requirements are specific to Fingerprint Information Retrieval requests unique to Authorized FBI Service Providers. The Authorized FBI Service Providers need additional functionality since they may need to access all fingerprints and all fingerprint information. A Fingerprint Information Retrieval request is a request for any or all fingerprint images, fingerprint features, or fingerprint audit trails.

3.3.4.1 Fingerprint Information Retrieval Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit Fingerprint Information Retrieval requests.

The NGI STOT that supports the Fingerprint Information Retrieval request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to retrieve any or all fingerprint information for a specified UCN as part of a Fingerprint Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to retrieve any or all supplemental fingerprint and palmprint information for a specified UCN as part of a Fingerprint Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to designate from which repository fingerprint information will be retrieved as part of a Fingerprint Information Retrieval request.

NGI shall accept a Fingerprint Information Retrieval request with a UCN and fingerprint specific information.

3.3.4.2 Fingerprint Information Retrieval Request Processing

NGI shall retrieve the fingerprint information associated with the fingerprint specific information provided in the Fingerprint Information Retrieval request.

NGI shall retrieve supplemental fingerprint and palm images associated with the fingerprint specific information, when indicated, as part of the Fingerprint Information Retrieval request.

NGI shall retrieve the fingerprint information for the UCN designated in the Fingerprint Information Retrieval request.

NGI shall retrieve the fingerprint information from the default NGI repository, when no repository or fingerprint is designated in the Fingerprint Information Retrieval request.

NGI shall reject a Fingerprint Information Retrieval request when specified UCN or specific fingerprint does not exist.

3.3.4.3 Fingerprint Information Retrieval Request Outputs

NGI shall allow an Authorized FBI Service Provider to view the information returned from the Fingerprint Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to print the information returned from the Fingerprint Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to save the Fingerprint Information Retrieval response onto removable media in a digital format.

3.3.5 Photo Image Retrieval Request

Photo Image Retrieval requests allow Authorized Contributors to request photo images for specific Identities and events. Authorized FBI Service Provider functionality for these requests is defined under the more general Photo Information Retrieval request.

3.3.5.1 Photo Image Retrieval Request Inputs

NGI shall accept a Photo Image Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall accept a Photo Image Retrieval request from an Authorized External System in accordance with the latest EBTS version.

The NGI Legacy EBTS TOT that supports the Photo Image Retrieval request is CPR.

The EBTS TOT that supports a Photo Image Retrieval request is IRQ.

NGI shall accept a Photo Image Retrieval request from an Authorized Contributor in accordance with the latest III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE Photo Image Retrieval request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall accept a Photo Image Retrieval request with a UCN or SID.

Deleted.

NGI shall accept a Photo Image Retrieval request with a UCN and photo specific information.

NGI shall allow the Authorized Contributor to specify which photo type (i.e., facial, SMT) to retrieve in a Photo Image Retrieval request.

NGI shall allow the Authorized Contributor to specify the number of photos to return in a Photo Image Retrieval request.

NGI shall provide the capability to designate the NGI repository from which photos should be retrieved as part of a Photo Image Retrieval request.

NGI shall provide the capability to designate an external repository(ies) (e.g., IDENT) from which photos should be retrieved as part of the Photo Image Retrieval request.

3.3.5.2 Photo Image Retrieval Request Processing

NGI shall retrieve photo(s) from the NGI repository designated in the Photo Image Retrieval request.

NGI shall retrieve up to the requested number of photos for the Identity, photo specific information, and photo type specified from the repository designated in the Photo Image Retrieval request.

NGI shall retrieve the photo image for the Identity and photo specific information specified in the Photo Image Retrieval request.

NGI shall retrieve the most recently taken photos for the Identity as a default, when no photo specific information is specified in the Photo Image Retrieval request.

NGI shall retrieve facial photos as a default, when no photo type is specified in the Photo Image Retrieval request.

NGI shall retrieve a single photo as a default, when the number of photos to retrieve is not specified in the Photo Image Retrieval request.

NGI shall retrieve from the default photo repository, when no repository is designated in the Photo Image Retrieval request.

NGI shall determine the external system's link identifier when an external repository is indicated as part of a Photo Image Retrieval request.

NGI shall include the external system's link identifier in an External Photo Image Retrieval request as part of a Photo Image Retrieval request.

NGI shall send an External Photo Image Retrieval request to the designated External System in accordance with the latest EBTS version when an external repository is specified in a Photo Image Retrieval request and the external system is not IDENT.

The EBTS TOT that supports an External System Photo Image Retrieval request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall send an External Photo Image Retrieval request to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement when IDENT is specified in a Photo Image Retrieval request.

NGI shall accept a response from an External Photo Image Retrieval request from an External System in accordance with the latest EBTS version when the external system is not IDENT.

The EBTS TOT that supports an External System Photo Image Retrieval response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a response from an External Photo Image Retrieval request from IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement.

NGI shall reject a Photo Image Retrieval request when a specified Identity or photo specific information does not exist.

NGI shall reject a Photo Image Retrieval request when a specified photo does not exist.

3.3.5.3 Photo Image Retrieval Request Outputs

NGI shall provide a response to a Photo Image Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports a Photo Image Retrieval request is IRR, ISR.

NGI shall provide a response to a Photo Image Retrieval request received via NCIC in accordance with the latest III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE Photo Image Retrieval response will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall provide zero or more photos as part of the Photo Image Retrieval response.

NGI shall indicate the source repository (e.g., criminal, civil, IDENT) of the photo image(s) returned in a Photo Image Retrieval response.

NGI shall combine the NGI Photo Image Retrieval results with the response(s) from external system(s) (e.g., IDENT) into a single Photo Image Retrieval response, when all search results are available.

When photos are requested from both an external repository and NGI, the requested number of photos will be retrieved by each system and all photos will be included in the combined response.

NGI shall provide partial Photo Image Retrieval results as part of a Photo Image Retrieval response when an External System does not meet the response time threshold required to create a combined response.

A partial response will include information to indicate that the external system designated to search did not respond to the search within the NGI response time. The status of the external system may be included if provided.

3.3.6 Photo Features Retrieval Request

Photo Features Retrieval requests allow Authorized Contributors to request photo features for specific photos. Authorized FBI Service Provider functionality for these requests is defined under the more general Photo Information Retrieval request.

3.3.6.1 Photo Features Retrieval Request Inputs

NGI shall accept a Photo Features Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Photo Features Retrieval requests is IRQ.

NGI shall accept a Photo Features Retrieval request with a UCN and photo specific information.

3.3.6.2 Photo Features Retrieval Request Processing

NGI shall retrieve the photo images for the specified Identity and photo included in the Photo Features Retrieval request.

NGI shall retrieve the photo features for the specified Identity and photo included in the Photo Features Retrieval request.

NGI shall reject a Photo Features Retrieval request when a specified UCN or photo does not exist.

3.3.6.3 Photo Features Retrieval Request Outputs

NGI shall provide a response to a Photo Features Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports a Photo Image Retrieval response is IRR, ISR.

3.3.7 Photo Audit Trail Retrieval Request

Photo Audit Trail Retrieval requests allow Authorized Contributors to request audit trail history for specific photos. Authorized FBI Service Provider functionality for these requests is defined under the more general Photo Information Retrieval request.

3.3.7.1 Photo Audit Trail Retrieval Request Inputs

NGI shall accept a Photo Audit Trail Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Photo Audit Trail Retrieval requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a Photo Audit Trail Retrieval request with a UCN and photo specific information.

3.3.7.2 Photo Audit Trail Retrieval Request Processing

NGI shall retrieve the photo audit trail for the specified Identity and photo in the Photo Audit Trail Retrieval request.

NGI shall reject a Photo Audit Trail Retrieval request when a specified UCN or photo does not exist.

NGI shall reject a Photo Audit Trail Retrieval request when the Authorized Contributor is not the photo owner.

3.3.7.3 Photo Audit Trail Retrieval Request Outputs

NGI shall provide a response to a Photo Audit Trail Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports a Photo Audit Trail Retrieval response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.3.8 Photo Information Retrieval Request

The following functional requirements are specific to Photo Information Retrieval requests unique to Authorized FBI Service Providers. The Authorized FBI Service Providers need additional functionality since they may need to access all photos and all photo information. A Photo Information Retrieval request is a request for any or all photo images, photo features, or photo audit trails.

3.3.8.1 Photo Information Retrieval Request Inputs

NGI shall allow an Authorized FBI Service Provider to retrieve any or all photo information for a specified UCN as part of a Photo Information Retrieval request.

The NGI STOT that supports the Photo Information Retrieval requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to retrieve any or all photo information for a specified UCN and photo specific information, as part of a Photo Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to designate from which NGI repository photo information will be retrieved, as part of a Photo Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to designate from which external repository(ies) (e.g., IDENT) photo information will be retrieved, as part of a Photo Information Retrieval request.

3.3.8.2 Photo Information Retrieval Request Processing

NGI shall retrieve the photo information for the UCN specified from the repository designated in the Photo Information Retrieval request.

NGI shall retrieve the photo information for the specified UCN and photo specific information designated in the Photo Information Retrieval request.

NGI shall retrieve from the default NGI repository, when no repository or photo is designated in the Photo Information Retrieval request.

NGI shall reject a Photo Information Retrieval request when a specified Identity or photo does not exist.

NGI shall determine the external system's link identifier based on the UCN contained in a Photo Information Retrieval request, when external repository indicated.

NGI shall include the external system's link identifier in an External Photo Image Retrieval request as part of a Photo Information Retrieval request.

NGI shall send an External Photo Image Retrieval request to the designated External System in accordance with the latest EBTS version when an external repository is specified in a Photo Information Retrieval request and the external system is not IDENT.

NGI shall send an External Photo Image Retrieval request to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement when IDENT is specified in a Photo Information Retrieval request.

3.3.8.3 Photo Information Retrieval Request Outputs

NGI shall allow an Authorized FBI Service Provider to view retrieved photo information as a result of a Photo Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to print retrieved photo information as a result of a Photo Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to save the Photo Information Retrieval response onto removable media in a digital format.

3.3.9 Palmprint Image Retrieval Request

Palmprint Image Retrieval requests allow Authorized Contributors to request palmprint images for specific Identities and events. Authorized FBI Service Provider functionality for these requests is defined under the more general Palmprint Information Retrieval request.

3.3.9.1 Palmprint Image Retrieval Request Inputs

NGI shall accept a Palmprint Image Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Palmprint Image Retrieval requests is IRQ.

NGI shall require one or more UCNs up to a maximum number as part of a Palmprint Image Retrieval request.

Deleted.

NGI shall accept a Palmprint Image Retrieval request with a UCN and palmprint specific information.

3.3.9.2 Palmprint Image Retrieval Processing

NGI shall retrieve the most recent palmprint for each specified UCN when palmprint specific information is not specified in the Palmprint Image Retrieval request.

Deleted.

NGI shall retrieve the palmprint images for the specified UCN and palmprint specific information in the Palmprint Image Retrieval request.

NGI shall reject a Palmprint Image Retrieval request when a specified UCN or palmprint specific information does not exist.

3.3.9.3 Palmprint Image Retrieval Outputs

NGI shall provide a response to a Palmprint Image Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports a Palmprint Image Retrieval response is IRR, ISR.

3.3.10 Palmprint Features Retrieval Request

Palmprint Features Retrieval requests allow Authorized Contributors to request palmprint features for specific palmprints. Authorized FBI Service Provider functionality for these requests is defined under the more general Palmprint Information Retrieval request.

3.3.10.1 Palmprint Features Retrieval Request Inputs

NGI shall accept a Palmprint Features Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Palmprint Features Retrieval requests is IRQ.

NGI shall require one or more UCNs up to a maximum number as part of a Palmprint Features Retrieval request.

NGI shall accept a Palmprint Features Retrieval request with palmprint specific information.

3.3.10.2 Palmprint Features Retrieval Request Processing

NGI shall retrieve the most recent palmprint images for the each specified UCN included in the Palmprint Features Retrieval request.

Deleted.

NGI shall retrieve the palmprint images for the specified UCN and palmprint in the Palmprint Features Retrieval request.

NGI shall retrieve the palmprint features for the specified UCN and palmprint in the Palmprint Features Retrieval request.

NGI shall reject a Palmprint Features Retrieval request when a specified UCN, palmprint, or palmprint features do not exist.

3.3.10.3 Palmprint Features Retrieval Request Outputs

NGI shall provide a response to a Palmprint Features Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports a Palmprint Features Retrieval response is IRR, ISR.

3.3.11 Palmprint Audit Trail Retrieval Request

Palmprint Audit Trail Retrieval requests allow Authorized Contributors to request audit trail history for specific palmprints. Authorized FBI Service Provider functionality for these requests is defined under the more general Palmprint Information Retrieval request.

3.3.11.1 Palmprint Audit Trail Request Inputs

NGI shall accept a Palmprint Audit Trail Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Palmprint Audit Trail Retrieval requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a Palmprint Audit Trail Retrieval request with a UCN and palmprint specific information.

3.3.11.2 Palmprint Audit Trail Request Processing

NGI shall retrieve the palmprint audit trail for the palmprint specified in the Palmprint Audit Trail Retrieval request.

NGI shall reject a Palmprint Audit Trail Retrieval request when a specified UCN or palmprint does not exist.

NGI shall reject a Palmprint Audit Trail Retrieval request when the Authorized Contributor is not the palmprint owner.

3.3.11.3 Palmprint Audit Trail Request Outputs

NGI shall provide a response to a Palmprint Audit Trail Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports a Palmprint Audit Trail Retrieval response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

Deleted.

3.3.12 Palmprint Information Retrieval Request

The following functional requirements are specific to Palmprint Information Retrieval requests unique to Authorized FBI Service Providers. The Authorized FBI Service Providers need additional functionality since they may need to access all palmprints and all palmprint information. A Palmprint Information Retrieval request is a request for any or all palmprint images, palmprint features, or palmprint audit trails.

3.3.12.1 Palmprint Information Retrieval Request Inputs

NGI shall allow an Authorized FBI Service Provider to retrieve all palmprint information for a specified UCN as part of a Palmprint Information Retrieval request.

The NGI STOT that supports the Palmprint Information Retrieval requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to retrieve any or all palmprint information for a specified UCN and palmprint specific information, as part of a Palmprint Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to designate from which repository palmprint information will be retrieved as part of a Palmprint Information Retrieval request

3.3.12.2 Palmprint Information Retrieval Request Processing

NGI shall retrieve the palmprint information for the UCN specified from the repository designated in the Palmprint Information Retrieval request.

NGI shall retrieve the palmprint information for the specified UCN and palmprint specific information designated in the Palmprint Information Retrieval request.

NGI shall retrieve the palmprint information from the default NGI repository, when no repository or palmprint is designated in the Palmprint Information Retrieval request.

NGI shall retrieve the palmprint information for the specified UCN and palmprint specific information designated in the Palmprint Information Retrieval request.

NGI shall reject a Palmprint Information Retrieval request when a specified UCN or specified palmprint does not exist.

3.3.12.3 Palmprint Information Retrieval Request Outputs

NGI shall allow an Authorized FBI Service Provider to view retrieved palmprint information as a result of a Palmprint Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to print retrieved palmprint information as a result of a Palmprint Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to save the Palmprint Information Retrieval response onto removable media in a digital format.

3.3.13 Iris Image Retrieval Request

Iris Image Retrieval requests allow Authorized Contributors to request iris images for specific Identities and events. Authorized FBI Service Provider functionality for these requests is defined under the more general Iris Information Retrieval request.

3.3.13.1 Iris Image Retrieval Request Inputs

NGI shall accept an Iris Image Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Iris Image Retrieval requests is IRQ.

NGI shall accept an Iris Image Retrieval request with a UCN.

Deleted.

NGI shall accept an Iris Image Retrieval request with a UCN and iris specific information.

NGI shall accept a specification of the number of iris images to return in an Iris Image Retrieval request.

NGI shall provide the capability to designate the repository from which iris images should be retrieved as part of an Iris Image Retrieval request.

3.3.13.2 Iris Image Retrieval Request Processing

Deleted.

NGI shall retrieve the iris image for the UCN and specified iris in the Iris Image Retrieval request.

NGI shall retrieve the most recently taken iris image(s) from the designated repository(ies) for the UCN as a default, when no event or iris specific information is specified in the Iris Image Retrieval request.

NGI shall retrieve the default number of iris images when the number of iris images to retrieve is not specified in the Iris Image Retrieval request.

NGI shall retrieve from the default iris repository, when no repository is designated in the Iris Image Retrieval request.

NGI shall reject an Iris Image Retrieval request when a specified UCN or event does not exist.

NGI shall reject an Iris Image Retrieval request when specified iris does not exist.

3.3.13.3 Iris Image Retrieval Request Outputs

NGI shall provide a response to an Iris Image Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports an Iris Image Retrieval response is IRR, ISR.

3.3.14 Iris Features Retrieval Request

Iris Features Retrieval requests allow Authorized Contributors to request iris features for specific irises. Authorized FBI Service Provider functionality for these requests is defined under the more general Iris Information Retrieval request.

3.3.14.1 Iris Features Retrieval Request Inputs

NGI shall accept an Iris Features Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Iris Features Retrieval requests is IRQ.

NGI shall accept an Iris Features Retrieval request with a UCN and iris specific information.

3.3.14.2 Iris Features Retrieval Request Processing

NGI shall retrieve iris images for the specified UCN and iris specific information included in the Iris Features Retrieval request.

NGI shall retrieve the iris features for the specified Identity and iris specific information included in the Iris Features Retrieval request.

NGI shall reject an Iris Features Retrieval request when a specified UCN or iris identifier does not exist.

NGI shall reject an Iris Features Retrieval request when specified features do not exist.

3.3.14.3 Iris Features Retrieval Request Outputs

NGI shall provide a response to an Iris Features Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports an Iris Features Retrieval response is IRR, ISR.

3.3.15 Iris Audit Trail Retrieval Request

Iris Audit Trail Retrieval requests allow Authorized Contributors to request audit trail history for specific irises. Authorized FBI Service Provider functionality for these requests is defined under the more general Iris Information Retrieval request.

3.3.15.1 Iris Audit Trail Request Inputs

NGI shall accept an Iris Audit Trail Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Iris Audit Trail Retrieval requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric

Information.

NGI shall accept an Iris Audit Trail Retrieval request with a UCN and iris specific information.

3.3.15.2 Iris Audit Trail Request Processing

NGI shall retrieve the iris audit trail for the iris specified in the Iris Audit Trail Retrieval request.

NGI shall reject an Iris Audit Trail Retrieval request when a specified UCN or iris specific information does not exist.

NGI shall reject an Iris Audit Trail Retrieval request when the Authorized Contributor is not the iris owner.

3.3.15.3 Iris Audit Trail Request Outputs

NGI shall provide a response to an Iris Audit Trail Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports an Iris Audit Trail Retrieval response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.3.16 Iris Information Retrieval Request

The following functional requirements are specific to Iris Information Retrieval requests unique to Authorized FBI Service Providers. The Authorized FBI Service Providers need additional functionality since they may need to access all iris images and all iris information. An Iris Information Retrieval request is a request for any or all iris images, iris features, or iris audit trails.

3.3.16.1 Iris Information Retrieval Request Inputs

NGI shall allow an Authorized FBI Service Provider to retrieve any or all iris information for a specified UCN as part of an Iris Information Retrieval request.

The NGI STOT that supports the Iris Information Retrieval requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to retrieve any or all iris information for a specified UCN and iris specific information, as part of an Iris Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to designate from which repository iris information will be retrieved, as part of an Iris Information Retrieval request.

3.3.16.2 Iris Information Retrieval Request Processing

NGI shall retrieve the iris information for the UCN specified from the repository designated in the Iris Information Retrieval request.

NGI shall retrieve the iris information for the specified UCN and iris specific information designated in the Iris Information Retrieval request.

NGI shall retrieve from the default NGI repository, when no repository or iris is designated in the Iris Information Retrieval request.

NGI shall reject an Iris Information Retrieval request when a specified UCN or iris does not exist.

3.3.16.3 Iris Information Retrieval Request Outputs

NGI shall allow an Authorized FBI Service Provider to view retrieved iris information as a result of an Iris Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to print retrieved iris information as a result of an Iris Information Retrieval request.

NGI shall allow an Authorized FBI Service Provider to save the Iris Information Retrieval response onto removable media in a digital format.

3.3.17 Unsolved Latent Audit Trail Retrieval Request

3.3.17.1 Unsolved Latent Audit Trail Request Inputs

NGI shall accept an Unsolved Latent Audit Trail Retrieval request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Unsolved Latent Audit Trail Retrieval requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit Unsolved Latent Audit Trail Retrieval requests.

The NGI STOT that supports the Unsolved Latent Audit Trail requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall accept an Unsolved Latent Audit Trail Retrieval request with a specified UCN.

3.3.17.2 Unsolved Latent Audit Trail Request Processing

NGI shall retrieve the audit trail for the UCN specified in the Unsolved Latent Audit Trail Retrieval request.

NGI shall reject an Unsolved Latent Audit Trail Retrieval request when a specified UCN does not exist.

NGI shall reject an Unsolved Latent Audit Trail Retrieval request when the Authorized Contributor is not the unsolved latent owner.

3.3.17.3 Unsolved Latent Audit Trail Request Outputs

NGI shall provide a response to an Unsolved Latent Audit Trail Retrieval request in accordance with the latest EBTS version.

The EBTS TOT that supports an Unsolved Latent Audit Trail Retrieval response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to view a retrieved audit trail as a result of an Unsolved Latent Audit Trail Retrieval request.

NGI shall allow an Authorized FBI Service Provider to print a retrieved audit trail as a result of an Unsolved Latent Audit Trail Retrieval request.

3.3.18 Identity History Request

3.3.18.1 Identity History Request Inputs

NGI shall accept Identity History request from Authorized Contributors in accordance with the III/NFF Operational and Technical Manual.

These requests arrive from the NCIC communications network.

NGI shall accept Identity History Requests in bulk via multiple methods (e.g., ftp, CD, DVD).

The NGI STOT that supports an NCIC MKE Identity History request is a Query Record (QR).

NGI shall allow an Authorized FBI Service Provider to submit Identity History request.

The NGI STOT that supports Identity History request is RRD.

NGI shall require an Identity History request with a UCN or State Identification Number (SID).

NGI shall accept an indicator on an Identity History request that specifies if a photo should be included with the Identity History response.

NGI shall provide the capability for an Authorized FBI Service Provider to request a Record Set Report as part of the Identity History Request.

NGI shall provide the capability for an Authorized FBI Service Provider to request a Receiving Agency Notification Report (RANR) as part of the Identity History Request.

3.3.18.2 Identity History Request Processing

NGI shall retrieve the Identity History information for the specified Identity as part of the Identity History request.

NGI shall retrieve the biographic compilation for the specified Identity as part of an Identity History request.

NGI shall retrieve the event information for the specified Identity as part of an Identity History request.

NGI shall send an Identity History Information request to a III/NFF State system, when appropriate, as a result of an Identity History request.

These queries will be sent to the states over the NCIC network, the responses will be sent via Nlets.

NGI shall send an Identity History Information request to a III/NFF State system in accordance with the III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE for an Identity History Information request is CHR.

NGI shall accept an Identity History Information response in accordance with the Nlets User and Technical Guide.

The NGI STOT that supports the Nlets Messaging for an Identity History Information response is SCR.

NGI shall combine NFF Identity History Information response(s) and NGI Identity History Information into a single Identity History response.

NGI shall optionally include, on an Identity History response, the most recently taken frontal facial photo for the specified Identity.

NGI shall optionally include, on an Identity History response, the most recently taken facial photo for the specified Identity, when no frontal facial photo is available.

NGI shall reject an Identity History request when the specified UCN or SID does not exist.

NGI shall determine the response distribution method (i.e., electronic or hardcopy) for an Identity History request.

3.3.18.3 Identity History Request Outputs

NGI shall provide the Identity History Summary for the specified Identity in an Identity History response.

NGI shall provide a collective response for Identity History Requests when submitted in bulk.

NGI shall provide a response to an Identity History request received via NCIC in accordance with the latest III/NFF Operational and Technical Manual.

NGI shall provide a hardcopy response to an Identity History request, as appropriate.

NGI shall allow an Authorized FBI Service Provider to view the Identity History response.

NGI shall allow an Authorized FBI Service Provider to print the Identity History response.

NGI shall provide the Record Set Report when requested for the specified Identity as part of the Identity History Request response.

NGI shall provide the RANR when requested for the specified Identity as part of the Identity History Request response.

3.3.19 Certification File Request

3.3.19.1 Certification File Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit a Certification File request.

The NGI STOT that supports the Certification File request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a UCN as part of a Certification File request.

NGI shall require a unique transaction identifier as part of a Certification File request.

The unique transaction identifier will allow NGI to retrieve the specific transaction certification file.

3.3.19.2 Certification File Request Processing

NGI shall retrieve the Certification File for the UCN and unique transaction identifier as part of the Certification File request.

NGI shall reject the Certification File request when the UCN or transaction identifier is invalid.

3.3.19.3 Certification File Request Outputs

NGI shall allow an Authorized FBI Service Provider to view the Certification File response.

NGI shall allow an Authorized FBI Service Provider to print the Certification File response.

3.3.20 Record Availability Inquiry

The Record Availability Inquiry (ZR) is used to determine, by providing a UCN or SID number, if a subject record is on file in the III.

3.3.20.1 Record Availability Inquiry Inputs

NGI shall accept Record Availability Inquiries Requests in accordance with the III/NFF Operations and Technical Manual.

The NGI STOT that supports a Record Availability Inquiry is ZR.

NGI shall accept a UCN as part of a Record Availability Inquiry Request.

NGI shall accept a SID as part of a Record Availability Inquiry Request.

These requests arrive from the NCIC communications network.

3.3.20.2 Record Availability Inquiry Processing

NGI shall determine if a subject exists in the Identity History File using the UCN or SID as part of a Record Availability Inquiry Request.

3.3.20.3 Record Availability Inquiry Outputs

NGI shall provide a response to a Record Availability Inquiry request received via NCIC in accordance with the III/NFF Operational and Technical Manual.

3.3.21 Record Status Inquiry

The Record Status Inquiry (ZRS) is used when a III participant wants to verify the status, single- or multi-state, of a subject record.

3.3.21.1 Record Status Inquiry Inputs

NGI shall accept Record Status Inquiry Requests in accordance with the III/NFF Operations and Technical Manual.

The NGI STOT that supports a Record Status Inquiry is ZRS.

NGI shall accept a UCN as part of a Record Status Inquiry Request.

NGI shall accept a SID as part of a Record Status Inquiry Request.

These requests arrive from the NCIC communications network.

3.3.21.2 Record Status Inquiry Processing

NGI shall determine the status of the subject in the Identity History File using the UCN number or SID as part of a Record Status Inquiry Request.

3.3.21.3 Record Status Inquiry Outputs

NGI shall provide a response to a Record Status Inquiry request received via NCIC in accordance with the III/NFF Operational and Technical Manual.

3.3.22 Administrative Inquiry

The Administrative Inquiry (ZI) is used by III participants when there is a need to determine: the presence of a SID or UCN pointer and the date established; single-, multi-state or wanted status; or dates of establishment and/or last update.

3.3.22.1 Record Administrative Inquiry Inputs

NGI shall accept Administrative Inquiries in accordance with the III/NFF Operations and Technical Manual.

The NGI STOT that supports an Administrative Inquiry is ZI.

NGI shall accept a UCN as part of an Administrative Inquiry Request.

NGI shall accept a SID as part of an Administrative Inquiry Request.

These requests arrive from the NCIC communications network.

3.3.22.2 Record Administrative Inquiry Processing

NGI shall retrieve biographic data and III pointer information as part of an Administrative Inquiry Request.

3.3.22.3 Record Administrative Inquiry Outputs

NGI shall provide a response to an Administrative Inquiry request received via NCIC in accordance with the III/NFF Operational and Technical Manual.

Rap Back Subscription List Request

3.3.23.1 Rap Back Subscription List Request Inputs

NGI shall accept a Rap Back Subscription List request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Rap Back Subscription List requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Rap Back Subscription List request.

The NGI STOT that supports the Rap Back Subscription List requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a Rap Back Subscriber identifier as part of a Rap Back Subscription List request.

NGI shall accept a Rap Back Recipient identifier(s) as part of a Rap Back Subscription List request.

3.3.23.2 Rap Back Subscription List Request Processing

NGI shall retrieve the Rap Back subscription list for the Rap Back Subscriber and Rap Back Recipient(s) specified in the Rap Back Subscription List request.

NGI shall reject the Rap Back Subscription List request when the Rap Back Subscriber identifier is invalid.

3.3.23.3 Rap Back Subscription List Request Outputs

NGI shall provide a response to an EBTS formatted Rap Back Subscription List request in accordance with the latest EBTS version.

The EBTS TOT that supports a Rap Back Subscription List response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to view the Rap Back Subscription List response.

NGI shall allow an Authorized FBI Service Provider to print the Rap Back Subscription List response.

3.3.24 Rap Back Identity History Summary Request

The following functional requirements relate to a Rap Back Subscriber retrieving an Identity History Summary after receipt of a Rap Back Activity Notification.

3.3.24.1 Rap Back Identity History Summary Request Inputs

NGI shall accept a Rap Back Identity History Summary request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Rap Back Identity History Summary requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall require a UCN in a Rap Back Identity History Summary request.

NGI shall require a unique Rap Back Notification Identifier in a Rap Back Identity History Summary request.

3.3.24.2 Rap Back Identity History Summary Request Processing

NGI shall validate that the Authorized Contributor is an active Rap Back Subscriber for the UCN provided in a Rap Back Identity History Summary request.

NGI shall retrieve the Identity History information for the UCN contained in a Rap Back Identity History Summary request.

NGI shall reject a Rap Back Identity History Summary request if the UCN is not valid.

NGI shall reject a Rap Back Identity History Summary request if the Rap Back Notification Identifier is not valid.

3.3.24.3 Rap Back Identity History Summary Request Outputs

NGI shall provide a response to a Rap Back Identity History Summary request in accordance with the latest EBTS version.

The EBTS TOT that supports a Rap Back Identity History Summary response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide an Identity History Summary in response to a Rap Back Identity History Summary request.

NGI shall indicate, on a Rap Back Identity History Summary response, the event that triggered the Rap Back Activity Notification associated with the submitted Rap Back Notification Identifier.

3.4 Investigation Services Functional Requirements

The following section contains the functional requirements supporting Investigation user services.

3.4.1 Subject Search Request

The Subject Search service provides the determination of the existence of an Identity History based upon searches using biographic descriptors such as name, date of birth, sex, and race. A Subject Search request contains biographic descriptors from which NGI generates a list of possible candidate matches.

3.4.1.1 Subject Search Request Inputs

NGI shall accept Subject Search requests from an Authorized Contributor in accordance with the III/NFF Operational and Technical Manual.

These requests arrive from the NCIC communications network.

The NGI STOT that supports a NCIC MKE Subject Search request is a Query History (QH).

NGI shall accept a Subject Search request from an Authorized Contributor via Machine Readable Data in accordance with the MRD Subject Search Manual.

The NGI STOT that supports Subject Search request via MRD is SSRM.

NGI shall allow an Authorized FBI Service Provider to submit a Subject Search request.

The NGI STOTs that support Subject Search requests are SPSS and FASS. The SPSS may be initiated by either an NGI or a NICS FBI Service Provider.

NGI shall allow an Authorized FBI Service Provider to designate repository(ies) as part of a Subject Search request.

NGI shall accept biographic data as part of a Subject Search request.

NGI will allow a UCN as a biographic descriptor data in addition to name, DOB, sex, race, etc. for a Subject Search request.

NGI shall accept an External Subject Search (ESS) Request in accordance with the latest EBTS version.

The NGI STOT that supports an External Subject Search (ESS) Request is an External Query History Request (EQHR).

3.4.1.2 Subject Search Request Processing

NGI shall search the repository(ies) designated as part of the Subject Search request.

NGI shall search the default repository when no repository is designated in the Subject Search request.

NGI shall perform a search using the biographic data contained in the Subject Search request.

NGI shall calculate a match score for each candidate resulting from a Subject Search request.

3.4.1.3 Subject Search Request Outputs

NGI shall provide a ranked candidate list of UCNs for up to the maximum number of candidates as the result of the Subject Search request.

NGI shall determine the response distribution method (i.e., electronic or hardcopy) for a Subject Search response.

NGI shall provide external system link identifier(s), when available, for each candidate as a result of the Subject Search request.

NGI shall provide an electronic response to a Subject Search request in accordance with the III/NFF Operational and Technical Manual.

The NGI STOT that supports a NCIC MKE Subject Search response will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall provide a candidate list in response to an MRD Subject Search request in accordance with the MRD Subject Search Manual.

NGI shall provide a hardcopy Identity History Summary for each candidate in response to an MRD Subject Search request.

NGI shall allow an Authorized FBI Service Provider to view the candidate list returned from the Subject Search request.

NGI shall allow an Authorized FBI Service Provider to view the record set returned as the single candidate from the Subject Search request.

NGI shall provide a response to an External Subject Search (ESS) Request in accordance with the latest EBTS version.

NGI shall provide an electronic Identity History Summary for each candidate in response to an External Subject Search (ESS) in accordance with the latest EBTS version.

A Subject Search Request submitted by an FBI Service Provider will include a Record Set in the response when only a single candidate is returned. The Record Set is an Identity History Summary formatted for internal FBI/CJIS use only.

NGI shall allow an Authorized FBI Service Provider to print the candidate list returned from the Subject Search request.

NGI shall allow an Authorized FBI Service Provider to print the record set returned as the single candidate from the Subject Search request.

3.4.2 Ad Hoc Subject Search Request

This service allows an Authorized FBI Service Provider to search on any biographic or event history data elements within the NGI Repositories. The response for the search is a candidate list containing zero or more candidates.

3.4.2.1 Ad Hoc Subject Search Inputs

NGI shall allow an Authorized FBI Service Provider to submit an Ad Hoc Subject Search request.

The NGI STOT that supports Ad Hoc Subject Search requests is AHSS.

NGI shall allow an Authorized FBI Service Provider to designate an NGI repository(ies) as part of the Ad Hoc Subject Search request.

NGI shall accept biographic data as part of an Ad Hoc Subject Search request.

NGI will allow the UCN and other assigned identifiers (e.g., SID, NIC), as well as descriptors such as Name, DOB, Hair and Eye color, etc. as part of the Ad Hoc Subject Search request. Also allowed are

individual data elements within each event. The III/FBI Ad Hoc Subject Search Manual provides a complete list of the biographic data that may be used in a search.

NGI shall accept a specification of the maximum number of candidates to return as part of an Ad Hoc Subject Search request.

NGI shall accept event data as part of an Ad Hoc Subject Search request.

3.4.2.2 Ad Hoc Subject Search Processing

NGI shall search the repository(ies) designated as part of the Ad Hoc Subject Search request.

NGI shall search the criminal repository when no repository is designated in the Ad Hoc Subject Search request.

NGI shall perform a search using the biographic data contained in the Ad Hoc Subject Search request.

NGI shall perform a search using the event data contained in the Ad Hoc Subject Search request.

3.4.2.3 Ad Hoc Subject Search Outputs

NGI shall provide a candidate list of UCNs for up to the maximum number of candidates as a response to the Ad Hoc Subject Search request.

NGI shall allow an Authorized FBI Service Provider to view the candidate list returned from the Ad Hoc Subject Search request.

NGI shall allow an Authorized FBI Service Provider to print the candidate list returned from the Ad Hoc Subject Search request.

NGI shall allow an Authorized FBI Service Provider to enroll the Ad Hoc Subject Search resulting candidate(s) to a designated SPC File.

Only a limited number of Authorized FBI Service Providers will be provided the capability to copy Ad Hoc Subject Search candidate(s) to an SPC File.

3.4.3 Tenprint Fingerprint Image Investigation Search Request

An Authorized Contributor will be able to submit a Fingerprint Image Investigation Search request with fingerprint images, fingerprint classification information, and biographic descriptors. The response consists of a candidate list and the fingerprint images for the specified number of top candidates. Images for the remaining candidates may be retrieved through separate Fingerprint Image Retrieval requests.

3.4.3.1 Tenprint Fingerprint Image Investigation Search Request Inputs

NGI shall accept a Tenprint Fingerprint Image Investigation Search request from Authorized Contributors in accordance with the latest EBTS version.

The EBTS TOT that supports the Fingerprint Image Investigation Search request is TPIS.

NGI shall allow an Authorized FBI Service Provider to submit a Fingerprint Image Investigation Search request.

The NGI STOT that supports the Fingerprint Image Investigation Search request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to submit fingerprint images via multiple methods (i.e., scanning, CD, DVD) for a Tenprint Fingerprint Image Investigation Search request.

NGI shall accept biographic descriptor data as part of a Tenprint Fingerprint Image Investigation Search request.

NGI shall accept fingerprint classification information as part of a Tenprint Fingerprint Image Investigation Search request.

NGI shall accept a designation of the repository(ies) as part of a Tenprint Fingerprint Image Investigation Search request.

NGI shall accept a specification of the maximum number of candidates to return in a Tenprint Fingerprint Image Investigation Search request.

NGI shall accept a specification of the number of candidate print images to return in a Tenprint Fingerprint Image Investigation Search request.

NGI shall accept an indicator on a Tenprint Fingerprint Image Investigation Search request that specifies which fingerprint information should be included with the Tenprint Fingerprint Image Investigation Search response.

3.4.3.2 Tenprint Fingerprint Image Investigation Search Request Processing

NGI shall perform an automated image quality check on a Tenprint Fingerprint Image Investigation Search request based on image quality standards.

NGI shall reject a Tenprint Fingerprint Image Investigation Search request that fails to meet minimum quality standards for fingerprints.

NGI shall extract fingerprint features from the fingerprint images provided in the Tenprint Fingerprint Image Investigation Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

NGI shall perform the Tenprint Fingerprint Image Investigation search of the repository(ies) designated in the Tenprint Fingerprint Image Investigation Search request.

NGI shall perform the Tenprint Fingerprint Image Investigation search of the default repository, when the repository is not specified in the Tenprint Fingerprint Image Investigation Search request.

NGI shall search using the fingerprint classification data, biographic data, and extracted fingerprint features from the Tenprint Fingerprint Image Investigation Search requests.

NGI shall perform all Tenprint Fingerprint Image Investigation searches against composite fingerprints.

NGI shall calculate a match score for each candidate resulting from a Tenprint Fingerprint Image Investigation Search request.

NGI shall retrieve up to the maximum number of candidates specified in the Fingerprint Image Investigation Search request.

NGI shall retrieve up to the default maximum number of candidates, when the maximum number of candidates to retrieve is not specified in the Tenprint Fingerprint Image Investigation Search request.

NGI shall retrieve the indicated number of composite fingerprint images and associated fingerprint information as part of a Tenprint Fingerprint Image Investigation Search request.

NGI shall retrieve the composite fingerprint images and associated fingerprint information for the highest ranking candidate when the number of fingerprint images to retrieve is not specified in a Tenprint Fingerprint Image Investigation Search request.

3.4.3.3 Tenprint Fingerprint Image Investigation Search Request Outputs

NGI shall provide a response to a Tenprint Fingerprint Image Investigation Search request in accordance with the latest EBTS version.

The EBTS TOT that supports a Tenprint Fingerprint Image Investigation Search response is SRT.

NGI shall provide a ranked candidate list containing zero or more candidates in response to a Tenprint Fingerprint Image Investigation Search request.

NGI shall provide a candidate list containing UCN(s) and optional fingerprint information in response to a Tenprint Fingerprint Image Investigation Search request.

NGI shall provide external system link identifier(s), when available, for each candidate as part of the Tenprint Fingerprint Image Investigation Search response.

NGI shall allow an Authorized FBI Service Provider to view the Tenprint Fingerprint Image Investigation Search response.

NGI shall allow an Authorized FBI Service Provider to print the Tenprint Fingerprint Image Investigation Search response.

3.4.4 Tenprint Fingerprint Feature Investigation Search Request

The Tenprint Fingerprint Feature Investigation Search requests will allow an Authorized Contributor to search using fingerprint features, pattern classification and biographic descriptors. The response consists of a candidate list and the fingerprint images for the specified number of top candidates. Images for the remaining candidates may be retrieved through separate Fingerprint Image Retrieval requests.

3.4.4.1 Tenprint Fingerprint Feature Investigation Search Request Inputs

NGI shall accept a Tenprint Fingerprint Feature Investigation Search request from Authorized Contributors in accordance with the latest EBTS version.

The EBTS TOT that supports the Tenprint Fingerprint Feature Search request is TPFS.

NGI shall allow an Authorized FBI Service Provider to submit a Tenprint Fingerprint Feature Investigation Search request.

The NGI STOT that supports the Tenprint Fingerprint Feature Search request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to submit fingerprint images via multiple methods (i.e., scanning, CD, DVD) for a Tenprint Fingerprint Feature Investigation Search request.

NGI shall accept fingerprint classification information as part of a Tenprint Fingerprint Feature Investigation Search request.

NGI shall accept biographic descriptor data as part of a Tenprint Fingerprint Feature Investigation Search request.

NGI shall accept a designation of the repository(ies) as part of a Tenprint Fingerprint Feature Investigation Search request.

NGI shall accept a specification of the maximum number of candidates to return in a Tenprint Fingerprint Feature Investigation Search request.

NGI shall accept a specified number of candidate print images to return in a Tenprint Fingerprint Feature Investigation Search request.

NGI shall accept an indicator on a Fingerprint Feature Investigation Search request that specifies which fingerprint information should be included with the Tenprint Fingerprint Feature Investigation Search response.

3.4.4.2 Tenprint Fingerprint Feature Investigation Search Request Processing

NGI shall allow an Authorized FBI Service Provider to manually extract fingerprint features from the fingerprint images as part of a Tenprint Fingerprint Feature Investigation Search request.

NGI shall perform the Tenprint Fingerprint Feature Investigation search of the repository(ies) designated in the Tenprint Fingerprint Feature Investigation Search request.

NGI shall perform the Tenprint Fingerprint Feature Investigation search of the default repository, when the repository is not specified in the Tenprint Fingerprint Feature Investigation Search request.

NGI shall search using the fingerprint feature, fingerprint classification, and biographic data contained within the Tenprint Fingerprint Feature Investigation Search request.

NGI shall perform all Tenprint Fingerprint Feature Investigation searches against composite fingerprints.

NGI shall calculate a match score for each candidate resulting from a Tenprint Fingerprint Feature Investigation Search request.

NGI shall retrieve up to the maximum number of candidates specified in the Tenprint Fingerprint Feature Investigation Search request.

NGI shall retrieve up to the default maximum number of candidates, when the maximum number of candidates to retrieve is not specified in the Tenprint Fingerprint Feature Investigation Search request.

NGI shall retrieve the composite fingerprint images for the highest ranking candidate when the number of fingerprint images to return is not specified in a Tenprint Fingerprint Feature Investigation Search request.

NGI shall retrieve the indicated number of composite fingerprint images and associated information as part of a Tenprint Fingerprint Feature Investigation Search request.

3.4.4.3 Tenprint Fingerprint Feature Investigation Search Request Outputs

NGI shall provide a response to a Tenprint Fingerprint Feature Investigation Search request in accordance with the latest EBTS version.

The EBTS TOT that supports a Tenprint Fingerprint Feature Investigation Search response is SRT.

NGI shall provide a ranked candidate list containing zero or more candidates in response to a Tenprint Fingerprint Feature Investigation Search request.

NGI shall provide a candidate list containing UCN(s) and optional fingerprint information in response to a Tenprint Fingerprint Feature Investigation Search request.

NGI shall provide external system link identifier(s), when available, for each candidate as part of the Tenprint Fingerprint Feature Investigation Search response.

NGI shall allow an Authorized FBI Service Provider to view the Tenprint Fingerprint Feature Investigation Search response.

NGI shall allow an Authorized FBI Service Provider to print the Tenprint Fingerprint Feature Investigation Search response.

3.4.5 Tenprint Fingerprint Rap Sheet Search Request

An Authorized Contributor will submit a Tenprint Fingerprint Rap Sheet Search request with fingerprint images, fingerprint classification information, and biographic descriptors. Only the criminal repository will be searched. The response will consist of a candidate list and the corresponding Identity History Summaries.

3.4.5.1 Tenprint Fingerprint Rap Sheet Search Request Inputs

NGI shall accept Tenprint Fingerprint Rap Sheet Search request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall accept Tenprint Fingerprint Rap Sheet Search request from an Authorized External System in accordance with the latest EBTS version.

The EBTS TOT that supports the Tenprint Fingerprint Search Rap Sheet Search request is TPRS.

NGI shall require fingerprint image data as part of a Tenprint Fingerprint Rap Sheet Search Request.

NGI shall accept biographic data as part of a Tenprint Fingerprint Rap Sheet Search request.

NGI shall accept fingerprint classification information as part of a Tenprint Fingerprint Rap Sheet Search request.

3.4.5.2 Tenprint Fingerprint Rap Sheet Search Request Processing

NGI shall perform an automated image quality check on a Tenprint Fingerprint Rap Sheet Search request based on image quality standards.

NGI shall reject a Tenprint Fingerprint Rap Sheet Search request when the fingerprint images fail to satisfy minimum image quality standards.

NGI shall extract fingerprint features from the fingerprint images provided in the Tenprint Fingerprint Rap Sheet Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

NGI shall search the criminal fingerprint repository using the fingerprint classification data and extracted fingerprint features from the Tenprint Fingerprint Rap Sheet Search request.

NGI shall calculate a match score for each candidate resulting from a Tenprint Fingerprint Rap Sheet Search request.

NGI shall retrieve the Identity History Summary for the highest ranked candidate(s) up to the maximum number as a result of Tenprint Fingerprint Rap Sheet Search request.

3.4.5.3 Tenprint Fingerprint Rap Sheet Search Request Outputs

NGI shall provide a response to a Tenprint Fingerprint Rap Sheet Search request in accordance with the latest EBTS version.

The EBTS TOT that supports a Tenprint Fingerprint Rap Sheet Search response is TPRR.

The search response may contain up to five top-scoring candidates in addition to any Identity History Records associated with those candidates.

NGI shall provide the Identity History Summary for the candidates, in ranked order, as part of the Tenprint Fingerprint Rap Sheet Search response.

3.4.6 Latent Penetration Query Request

The Latent Penetration Query request allows the user to receive an estimated percentage of the designated NGI repository(ies) that will be accessed by a Latent Fingerprint Image Search request or a Latent Fingerprint Feature Search request. The query contains the search parameters that will be defined in the search, but does not contain images or features. This will allow setting the search parameters to ensure that the maximum penetration allowed is not exceeded.

3.4.6.1 Latent Penetration Query Request Inputs

NGI shall accept Latent Penetration Query requests from Authorized Contributors in accordance with the latest EBTS version.

The EBTS TOT that supports the Latent Penetration Query requests is LPNQ.

NGI shall allow an Authorized FBI Service Provider to submit a Latent Penetration Query request.

The NGI STOT that supports Latent Penetration Query requests is ILPNQ.

NGI shall accept a designation of the repository(ies) to be included in a Latent Penetration Query request.

3.4.6.2 Latent Penetration Query Request Processing

NGI shall calculate the estimated percentage of the designated repository(ies) that would be searched using the latent search parameters provided in the Latent Penetration Query request.

NGI shall calculate the estimated percentage of the default repository(ies) that would be searched using the latent search parameters provided in the Latent Penetration Query request when no repository is designated.

3.4.6.3 Latent Penetration Query Request Outputs

NGI shall provide an electronic response to a Latent Penetration Query request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports a Latent Penetration Query response is LPNR.

NGI shall allow an Authorized FBI Service Provider to view the results of the Latent Penetration Query request.

3.4.7 Latent Friction Ridge Image Search Request

An Authorized Contributor will be able to submit a Latent Print Image Investigation Search request with a print image(s), pattern classification information, and biographic descriptors. The response consists of a candidate list of UCNs and fingerprint images.

3.4.7.1 Latent Friction Ridge Image Search Request Inputs

NGI shall accept a Latent Print Image Investigation Search request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall accept a Latent Print Image Investigation Search request from an External System (e.g., IDENT) in accordance with the latest EBTS version.

The EBTS TOT that supports a Latent Print Image Investigation Search request is LFIS.

NGI shall allow an Authorized FBI Service Provider to submit a Latent Print Image Investigation Search request.

The NGI STOT that supports the Latent Print Image Investigation Search request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to submit a latent print(s) via multiple methods (i.e., scanning, CD, DVD) for a Latent Print Image Investigation Search request.

NGI shall accept a designation of the internal NGI repository(ies) to be included in a Latent Print Image Investigation Search request.

NGI shall accept a designation of an External Repository(ies) (e.g., IDENT) against which latent print data should be searched as part of a Latent Print Image Investigation Search request.

NGI shall accept a print position(s) indicator when a single fingerprint is submitted in a Latent Print Image Investigation Search request.

An Authorized Contributor, External System, or FBI Service Provider can indicate which print position to search against in the NGI repository. If the Latent Print Image Investigation Search request contains a single print image, the contributor can indicate multiple print positions to be searched. If no print position is indicated, then all print positions will be searched.

NGI shall require a print position indicator for each fingerprint when multiple fingerprints are submitted as part of a Latent Print Image Investigation Search request.

NGI shall accept biographic descriptor data as part of a Latent Print Image Investigation Search request.

NGI shall accept fingerprint classification information as part of a Latent Print Image Investigation Search request.

NGI shall accept an indicator for enrollment in the ULF as part of the Latent Print Image Investigation Search request.

NGI shall accept specified NCIC fingerprint classification(s) to be used as a filter for a Latent Print Image Investigation Search request.

NGI shall accept an indicator that specifies the number of candidates that will be returned from each requested system in a Latent Print Image Investigation Search request.

If both internal and external repositories are designated for search, NGI will return the same specified number of candidates from each system indicated.

NGI shall accept a specified number of candidate print images to return in a Latent Print Image Investigation Search request.

NGI shall accept an indicator in a Latent Print Image Investigation Search request, to optionally return features and matching minutiae with candidate print images.

NGI shall accept a designation of transaction priority by which the Latent Print Image Investigation Search request should be performed.

3.4.7.2 Latent Friction Ridge Image Search Request Processing

NGI shall prioritize a Latent Print Image Investigation Search using established and specified priority criteria.

NGI shall perform an automated image quality check on a Latent Print Image Investigation Search request based on image quality standards.

NGI shall reject a Latent Print Image Investigation Search request when the print images fail to satisfy minimum image quality standards.

NGI shall extract fingerprint features from the print image(s) provided in the Latent Print Image Investigation Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

NGI shall perform latent print searches of the NGI repository(ies) designated in the Latent Print Image Investigation Search request.

NGI shall perform latent print searches of the default NGI repository(ies) when no repository is specified in the Latent Print Image Investigation Search request.

NGI shall perform the Latent Print Image search using the print position, fingerprint classification data, biographic data, and extracted fingerprint features from the Latent Print Image Investigation Search request.

NGI shall search all print positions for a Latent Print Image Investigation Search request containing a single print and no print position indicator.

NGI shall filter Latent Print Image Investigation Searches based upon specified NCIC fingerprint classification(s).

Filtering by NCIC class will only apply to those records that contain legacy NCIC classifications.

NGI shall perform Latent Print Image Investigation Searches against features of all individual event prints (non-composite) in the designated repository(ies), including plain impressions.

NGI shall perform latent print image searches against all fingerprint, Palmprint, and supplemental fingerprint and Palmprint information in the designated repository(ies) as part of a Latent Print Image Investigation Search request.

NGI shall perform a search of the RISC repository for all Latent Print Image Investigation Search requests.

NGI shall retrieve the number of candidates specified in the Latent Print Image Investigation Search request.

NGI shall calculate a match score for each candidate resulting from a Latent Print Image Investigation Search request.

NGI shall retrieve the default number of candidates, when the number of candidates to return is not specified in the Latent Print Image Investigation Search request.

NGI shall retrieve the indicated number of matched candidate print images and associated information as part of a Latent Print Image Investigation Search request.

NGI shall retrieve the default number of matched candidate print images, when the number of images to return is not specified in the Latent Print Image Investigation Search request.

NGI shall enroll an Identity into the ULF, when indicated, as a result of a Latent Print Image Investigation Search request.

NGI shall send an External Latent Print Image Investigation Search request to an External System, in accordance with the EBTS when the designated external system is not IDENT.

The EBTS TOT that supports an External Latent Print Image Investigation Search request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall send an External Latent Print Image Investigation Search request to IDENT, when designated, in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement.

NGI shall accept a response from an External System, when the external system is not IDENT, as a result of an External Latent Print Image Investigation Search request of external repositories in accordance with the latest EBTS version.

The EBTS TOT that supports an External Latent Print Image Investigation Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a response from IDENT as a result of an External Latent Print Image Investigation Search request of IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement.

Deleted.

NGI shall perform a cascaded fingerprint search of the marked Special Population Cognizant (SPC) Files as a result of all Latent Print Image Investigation Searches in accordance with cascaded search business rules.

3.4.7.3 Latent Friction Ridge Image Search Request Outputs

NGI shall provide a response to a Latent Print Image Investigation Search in accordance with the latest EBTS version.

NGI shall provide a response to an External System (e.g., IDENT) as a result of a Latent Print Image Investigation Search from an External System in accordance with the latest EBTS version.

The EBTS TOT that supports a Latent Print Image Investigation Search response is SRL.

NGI shall indicate on a Latent Print Image Investigation Search response whether or not additional fingerprint images, palmprints, or supplemental fingerprint and palmprint information is available for each candidate.

NGI shall provide a ranked candidate list in response to a Latent Print Image Investigation Search request.

NGI shall provide a candidate list containing UCN(s), specific event data, and external system link identifier(s), when available, in response to a Latent Print Image Investigation Search request.

NGI shall optionally include the features and matching minutiae data for each candidate print returned in a Latent Print Image Investigation Search response.

NGI shall include in the Latent Print Image Investigation Search response candidate list, zero or more print images, up to the number of candidate images specified in the Latent Print Investigation Search request.

NGI shall forward a response from an External System (e.g., IDENT) to the Authorized Contributor, independent from the NGI response, as a result of an External Latent Print Image Investigation Search request.

NGI shall allow an Authorized FBI Service Provider to view the Latent Print Image Investigation Search response.

NGI shall allow an Authorized FBI Service Provider to print the Latent Print Image Investigation Search response.

NGI shall allow an Authorized FBI Service Provider to save the Latent Print Image Investigation Search response onto removable media in a digital format.

3.4.8 Latent Friction Ridge Feature Search Request

The Latent Print Feature Investigation Search requests will allow an Authorized Contributor to search using fingerprint features, pattern classification, and biographic descriptors. The response consists of a candidate list of UCNs and fingerprint images.

3.4.8.1 Latent Friction Ridge Feature Search Request Inputs

NGI shall accept a Latent Print Feature Investigation Search request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall accept a Latent Print Feature Investigation Search request from an External System (e.g., IDENT) in accordance with the latest EBTS version.

The EBTS TOT that supports the Latent Fingerprint Feature Investigation Search request is LFFS.

NGI shall allow an Authorized FBI Service Provider to submit a Latent Print Feature Investigation Search request.

The NGI STOT that supports the Latent Fingerprint Feature Investigation Search request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to submit a latent print(s) via multiple methods (e.g., scanning, CD, DVD) for a Latent Print Feature Investigation Search request.

NGI shall accept fingerprint classification information as part of a Latent Print Feature Investigation Search request.

NGI shall accept one or more print position indicators when a single print is submitted in a Latent Print Feature Investigation Search request.

An Authorized Contributor, External System, or FBI Service Provider can indicate which print position to search against in the NGI repository. If the Latent Print Feature Investigation Search request contains a single print image, the contributor can indicate multiple print positions to be searched. If no print position is indicated, then all print positions will be searched.

NGI shall require a print position indicator for each print image when multiple print images are contained in the Latent Print Feature Investigation Search request.

NGI shall accept biographic descriptor data as part of a Latent Print Feature Investigation Search request.

NGI shall accept an indicator for enrollment in the ULF as part of the Latent Print Feature Investigation Search request.

NGI shall accept a designation of the internal NGI repository(ies) to be included in a Latent Print Feature Investigation Search request.

NGI shall accept a designation of an external repository(ies) (e.g., IDENT) against which latent print data should be searched as part of a Latent Print Feature Investigation Search request.

NGI shall accept specified NCIC fingerprint classification(s) to be used as a filter for a Latent Print Feature Investigation Search request.

NGI shall accept an indicator that specifies the number of candidates that will be returned from each requested system in a Latent Print Feature Investigation Search request.

If both internal and external repositories are designated for search, NGI will return the same specified number of candidates from each system indicated.

NGI shall accept a specified number of candidate print images to return in a Latent Print Feature Investigation Search request.

NGI shall accept an indicator in a Latent Print Feature Investigation Search request, to optionally return features and matching minutiae with candidate print images.

NGI shall accept a designation of transaction priority by which the Latent Print Feature Investigation Search should be performed.

3.4.8.2 Latent Friction Ridge Feature Request Processing

NGI shall allow an Authorized FBI Service Provider to manually extract print features from the print images as part of a Latent Print Feature Investigation Search request.

NGI shall prioritize a Latent Print Feature Investigation Search using established and specified priority criteria.

NGI shall perform latent print searches of the repository(ies) designated in the Latent Print Feature Investigation Search request.

NGI shall perform latent print searches of the default NGI repository(ies) when no repository is specified in the Latent Print Feature Investigation Search request.

NGI shall perform the Latent Print Feature search using the print position, fingerprint feature, fingerprint classification, and biographic data contained within the Latent Print Feature Investigation Search request.

NGI shall filter Latent Print Feature Investigation Searches based upon specified NCIC fingerprint classification(s).

Filtering by NCIC class will only apply to those records that contain legacy NCIC classifications.

NGI shall perform Latent Print Feature Investigation Searches against features of all individual event prints (non-composite), including plain impressions, contained within the designated repository(ies).

NGI shall perform latent print feature searches against all fingerprint, palmprint, and supplemental fingerprint and palmprint information as part of a Latent Print Feature Investigation Search request.

NGI shall perform a search of the RISC repository for all Latent Print Feature Investigation Search requests.

NGI shall calculate a match score for each candidate resulting from a Latent Print Feature Investigation Search request.

NGI shall retrieve the number of candidates specified in the Latent Print Feature Investigation Search request.

NGI shall retrieve the default number of candidates, when the number of candidates to return is not specified in the Latent Print Feature Investigation Search

NGI shall retrieve the indicated number of matched candidate print images and associated information as part of a Latent Print Feature Investigation Search request.

NGI shall retrieve the default number of matched candidate print images, when the number of images to return is not specified in the Latent Print Feature Investigation Search request.

NGI shall enroll an Identity into the ULF, when indicated, as a result of a Latent Print Feature Investigation Search request.

NGI shall send an External Latent Print Feature Investigation Search request to an External System, in accordance with the EBTS when the designated external system is not IDENT.

NGI shall send an External Latent Print Feature Investigation Search request to IDENT, when designated, in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement.

NGI shall accept a response from an External System, when the external system is not IDENT, as a result of an External Latent Print Feature Investigation Search request of external repositories in accordance with the latest EBTS version.

NGI shall accept a response from IDENT as a result of an External Latent Print Feature Investigation Search request of external repositories in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement.

Deleted.

NGI shall perform a cascaded fingerprint search of the marked Special Population Cognizant (SPC) Files as a result of all Latent Print Feature Investigation Searches in accordance with cascaded search business rules.

3.4.8.3 Latent Friction Ridge Feature Request Outputs

NGI shall provide a response to a Latent Print Feature Investigation Search in accordance with the latest EBTS version.

NGI shall provide a response to an External System (e.g., IDENT) as a result of a Latent Print Feature Investigation Search from an External System in accordance with the latest EBTS version.

The EBTS TOT that supports a Latent Print Feature Investigation Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall indicate on a Latent Print Feature Investigation Search response whether or not additional fingerprint images, palmprints, or supplemental fingerprint and palmprint information is available for each candidate.

NGI shall provide a ranked candidate list in response to a Latent Print Feature Investigation Search request.

NGI shall provide a candidate list containing UCN(s), specific event data, and external system link identifier(s), when available, in response to a Latent Print Feature Investigation Search request.

NGI shall optionally include the features and matching minutiae data for each candidate print returned in a Latent Print Feature Investigation Search response.

NGI shall include in the Latent Print Feature Investigation Search response candidate list, zero or more print images, up to the number of candidate images specified in the Latent Print Feature Investigation Search request.

NGI shall forward a response from an External System (e.g., IDENT) to the Authorized Contributor, independent from the NGI response, as a result of an External Latent Print Feature Investigation Search request.

NGI shall allow an Authorized FBI Service Provider to view the Latent Print Feature Investigation Search response.

NGI shall allow an Authorized FBI Service Provider to print the Latent Print Feature Investigation Search response.

NGI shall allow an Authorized FBI Service Provider to save the Latent Print Feature Investigation Search response onto removable media in a digital format.

3.4.9 Unsolved Latent Search Request

The Unsolved Latent Search request is a directed search against the ULF. Other fingerprint investigation searches may also be directed against this file through use with the designation of repositories.

3.4.9.1 Unsolved Latent Search Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit print data as part of an Unsolved Latent Search request.

The NGI STOTs that support Unsolved Latent Search requests are IULS and IULTS.

NGI shall allow an Authorized FBI Service Provider to input print data to initiate an Unsolved Latent Search request.

The NGI workstation will support multiple input methods for biometric images (scanning, CD-ROM, and other removable media). These methods will support the standards for output stated in ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, Data Format for the Interchange of Fingerprint Information" and with the EBTS.

NGI shall accept one or more print images as part of an Unsolved Latent Search request.

NGI will allow Tenprint fingerprint data (IULTS) or latent data (IULS) to be searched against the ULF.

NGI shall accept one or more print position indicators when a single print is submitted in an Unsolved Latent Search request.

An Authorized FBI Service Provider can indicate which print position to search against in the NGI repository. If the Unsolved Latent Search request contains a single fingerprint image, the Contributor or Service Provider can indicate multiple print positions to be searched. If no print position is indicated,

then all print positions will be searched.

NGI shall require a print position indicator for each print image when multiple print images are contained in the Unsolved Latent Search request.

NGI shall accept fingerprint classification information as part of an Unsolved Latent Search request.

3.4.9.2 Unsolved Latent Search Request Processing

NGI shall allow an Authorized FBI Service Provider to manually extract print features from the print images provided in the Unsolved Latent Search request.

NGI shall provide an automated method to extract print features from the print images provided in the Unsolved Latent Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

NGI shall search the ULF using the print position, print features, and fingerprint classification contained within the Unsolved Latent Search request.

NGI shall search all print positions for an Unsolved Latent Search request containing a single print and no finger position indicator.

NGI shall calculate a match score for each candidate resulting from an Unsolved Latent Search request.

NGI shall perform a cascaded fingerprint search of the marked SPC Files as a result of all Unsolved Latent Search request in accordance with cascaded search business rules.

3.4.9.3 Unsolved Latent Search Request Outputs

NGI shall provide a ranked candidate list of a default number of UCNs as part of the Unsolved Latent Search response.

NGI shall provide external system link identifier(s), when available, for each candidate as part of the Unsolved Latent Search response.

NGI shall allow an Authorized FBI Service Provider to view the candidate list returned from the Unsolved Latent Search request.

3.4.10 Latent Search Status and Modification Request

Latent Search Status and Modification request provides an Authorized Contributor or Authorized FBI Service Provider the capability to check the status of a latent search request, adjust priorities, adjust search order, or cancel a previously submitted latent search that are queued in NGI. If the Latent Search is already in process, this request will be rejected.

3.4.10.1 Latent Search Status and Modification Request Inputs

NGI shall accept a Latent Search Status and Modification request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Latent Search Status and Modification request is LSMQ.

NGI shall allow an Authorized FBI Service Provider to submit a Latent Search Status and Modification request.

The NGI STOT that supports Latent Search Status and Modification request is ILSMQ.

NGI shall accept Query Depth Detail (QDD) (i.e., ORI, state indicator, EID, case number and extension) as part of the Latent Search Status and Modification request.

NGI shall accept SCNA(s) of previously submitted Latent Search(es) as part of the Latent Search Status and Modification request.

3.4.10.2 Latent Search Status and Modification Request Processing

NGI shall retrieve the AFIS segment process control number (SCNA) of the referenced Latent Search(es) and the estimated time(s) to complete the search(es) when status request indicated as part of the Latent Search Status and Modification request.

NGI shall modify the priority of the specified Latent Search(es) when indicated as part of the Latent Search Status and Modification request.

NGI shall modify the processing order of the specified Latent Search(es) when indicated as part of the Latent Search Status and Modification request.

NGI shall retrieve the latent queue processing status when requested as part of the Latent Search Status and Modification request.

The latent queue status will include the operational status of NGI, as well as details on queue depth and search wait times.

NGI shall delete the specified Latent Search(es) when indicated as part of the Latent Search Status and Modification request.

NGI shall reject the Latent Search Status and Modification request when specified Latent Search(es) are not found in the Latent Search queue.

3.4.10.3 Latent Search Status and Modification Request Outputs

NGI shall provide the appropriate response to the Latent Search Status and Modification request in accordance with the latest EBTS version.

The EBTS TOT that supports a Latent Search Status and Modification response is LSMR.

NGI shall allow an Authorized FBI Service Provider to view the Latent Search Status and Modification request results.

3.4.11 Latent Repository Statistics Query

The Latent Repository Statistics Query request allows the user to receive a statistical representation, based on descriptive data, of a latent repository and is used in updating a user's statistical representation to be used in a penetration query.

3.4.11.1 Latent Repository Statistics Query Inputs

NGI shall accept Repository Statistics Query requests from Authorized Contributors in accordance with the latest EBTS version.

The EBTS TOT that supports the Repository Statistics Query requests is LRSQ.

3.4.11.2 Latent Repository Statistics Query Processing

NGI shall calculate a statistical representation of the descriptors in the Latent Cognizant File using the descriptive data provided in the Latent Repository Statistics Query request.

3.4.11.3 Latent Repository Statistics Query Outputs

NGI shall provide a response to a Latent Repository Statistics Query request in accordance with the latest EBTS version.

3.4.12 Comparison Print Image(s) Submission

The Comparison Print Image(s) Submission supports the comparison of provided Tenprint fingerprint images or other known prints against the provided latent impressions associated with a case. The Comparison Print Image(s) Submission is intended solely for FBI use (i.e., field offices, FBI investigators). The provided fingerprints may consist of the following:

1. Suspect known prints
2. Victim known prints
3. Known prints from individuals being compared for purposes of elimination
4. Other individuals involved in the case

The Comparison Print Image(s) Submission may include all the fingerprints normally enclosed in a Tenprint submittal plus optional additional prints (e.g., Palmprints), if applicable. The submitted fingerprints and latent prints will be analyzed and compared by an Authorized FBI Service Provider (Latent Examiner). Prints for several individuals must be sent as individual submissions. No electronic response is returned for this submission. The contributor will be manually (i.e., telephonically, email, mail, fax) notified of comparison results.

3.4.12.1 Comparison Print Image(s) Submission Inputs

NGI shall accept Comparison Print Image Submission requests from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Comparison Print Image Submission request is CFS.

NGI shall accept print image data as part of a Comparison Print Image Submission request.

NGI shall accept latent image data as part of a Comparison Print Image Submission request.

NGI shall accept palmprint image data as part of a Comparison Print Image Submission request.

3.4.12.2 Comparison Print Image(s) Submission Processing

NGI shall allow an Authorized FBI Service Provider to input print images for the Comparison Print Image Submission request.

NGI shall allow an Authorized FBI Service Provider to associate print images with the Comparison Print Image Submission request.

NGI shall allow an Authorized FBI Service Provider to perform a manual LFIC for each set of subject prints provided against latent prints provided as part of a Comparison Print Image Submission request.

NGI shall allow an Authorized FBI Service Provider to manually extract features from the print images as part of the Comparison Print Image Submission request.

NGI shall provide an automated method to extract features from the print images as part of the Comparison Print Image Submission request.

The print features extracted may include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

NGI shall require an Authorized FBI Service Provider to extract (i.e., automated or manual) print features prior to processing a Comparison Print Image Submission request.

NGI shall search using the finger position(s) and print features extracted from the print images as part of the Comparison Print Image Submission request.

NGI shall search all finger positions for a Comparison Print Image Submission request containing a single print when no finger position is indicated.

NGI shall allow an Authorized FBI Service Provider to search the NGI repository(ies) using the finger position(s) and print features extracted from the print images as part of the Comparison Print Image Submission request.

NGI shall enroll an Identity into the ULF, when appropriate, as a result of a Comparison Print Image Submission request.

3.4.12.3 Comparison Print Image(s) Submission Outputs

NGI shall allow an Authorized FBI Service Provider to view the results of a Comparison Print Image Submission request.

NGI shall allow an Authorized FBI Service Provider to print the results of a Comparison Print Image Submission request.

3.4.13 Deleted

Deleted MCP.

Deleted MCP.

Deleted MCP.

Deleted MCP.

Deleted MCP.

Deleted MCP.

Deleted MCP.

3.4.14 Evaluation Latent Fingerprint Submission Request

The Evaluation Latent Fingerprint Submission request (ELR) provides the capability for FBI field office personnel to have FBI Latent Fingerprint Section (LFPS) consult on cases. The ELR contains set of latent fingerprints. The ELR is processed similar to a Latent Identification Search request. Following receipt of the submission by NGI, these transactions will be manually processed by an Authorized Latent Examiner. The FBI LFPS will contact the Authorized Contributor (FBI field office) with results that may include the establishment of a latent case, a request for additional information, or an evaluation of the case feasibility and recommendations for further actions.

3.4.14.1 Evaluation Latent Fingerprint Submission Request Inputs

NGI shall accept fingerprint data as part of an Evaluation Latent Fingerprint Submission Search request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Evaluation Latent Fingerprint Submission Search request is ELR.

3.4.14.2 Evaluation Latent Fingerprint Submission Request Processing

NGI shall allow an Authorized FBI Service Provider to manually extract fingerprint features from the fingerprint images provided in the Evaluation Latent Fingerprint Submission Search request.

NGI shall provide an automated method to extract fingerprint features from the fingerprint images provided in the Evaluation Latent Fingerprint Submission Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

NGI shall allow Authorized FBI Service Provider to search the NGI repository(ies) using the finger position(s) and fingerprint features extracted from the fingerprint images provided in the Evaluation Latent Fingerprint Submission Search request.

NGI shall allow an Authorized FBI Service Provider to perform a manual LFIC for each candidate resulting from an Evaluation Latent Fingerprint Submission Search request.

NGI shall enroll an Identity into the ULF, when appropriate, as a result of an Evaluation Latent Fingerprint Submission Search request.

3.4.14.3 Evaluation Latent Fingerprint Submission Request Outputs

NGI shall provide a response to an Evaluation Latent Fingerprint Submission Search request in accordance with the latest EBTS version.

The EBTS TOT that supports an Evaluation Latent Fingerprint Submission Search response is NAR.

3.4.15 Text Based Facial Photo Search Request

3.4.15.1 Text-Based Facial Photo Search Request Inputs

NGI shall accept a Text-Based Facial Photo Search request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Text-Based Facial Photo Search requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a Text-Based Facial Photo Search request from an Authorized Contributor in accordance with the latest III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE for a Text-Based Facial Photo Search request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to submit a Text-Based Facial Photo Search request.

The NGI STOT that supports the Text-Based Facial Photo Search requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall accept a designation of the repository(ies) to be included in a Text-Based Facial Photo Search.

NGI shall accept a specification of the number of candidates to return in a Text-Based Facial Photo Search.

3.4.15.2 Text-Based Facial Photo Search Request Processing

NGI shall perform the text-based facial search of the repository(ies) designated in the Text-Based Facial Photo Search request.

NGI shall perform the text-based facial search of the default repository(ies), when the repository is not specified in the Text-Based Facial Photo Search request.

NGI shall retrieve up to the number of candidates specified in the Text-Based Facial Photo Search request.

NGI shall retrieve up to the default number of candidates, when the number of candidates to retrieve is not specified in the Text-Based Facial Photo Search request.

NGI shall retrieve the most recently taken frontal facial photo for each candidate on a Text-Based Facial Photo Search response.

NGI shall retrieve the most recently taken facial photo for any candidate on a Text-Based Facial Photo Search response, when no frontal facial photo is available for that candidate.

3.4.15.3 Text-Based Facial Photo Search Request Outputs

NGI shall provide a response to a Text-Based Facial Photo Search request in accordance with the latest EBTS version.

The EBTS TOT that supports a Text-Based Facial Photo Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide a response to a Text-Based Facial Photo Search request received via NCIC in accordance with the latest III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE for a Text-Based Facial Photo Search response will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to view the Text-Based Facial Photo Search response.

NGI shall allow an Authorized FBI Service Provider to print the Text-Based Facial Photo Search response.

NGI shall provide a ranked candidate list containing zero or more candidates in response to a Text-Based Facial Photo Search request.

NGI shall provide a candidate list containing UCN(s) and specific event data in response to a Text-Based Facial Photo Search request.

3.4.16 Text-Based SMT Photo Search Request

3.4.16.1 Text-Based SMT Photo Search Request Inputs

NGI shall accept a Text-Based SMT Photo Search request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Text-Based SMT Photo Search requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a Text-Based SMT Photo Search request from an Authorized Contributor in accordance with the latest III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE for a Text-Based SMT Photo Search request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to submit a Text-Based SMT Photo Search request.

The NGI STOT that supports the Text-Based SMT Photo Search requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall accept a designation of the repository(ies) to be included in a Text-Based SMT Photo Search.

NGI shall accept a specification of the number of candidates to return in a Text-Based SMT Photo Search.

3.4.16.2 Text-Based SMT Photo Search Request Processing

NGI shall perform the text-based SMT search of the repository(ies) designated in the Text-Based SMT Photo Search request.

NGI shall perform the text-based SMT search of the default repository, when the repository is not specified in the Text-Based SMT Photo Search request.

NGI shall retrieve up to the number of candidates specified in the Text-Based SMT Photo Search request.

NGI shall retrieve up to the default number of candidates, when the number of candidates to retrieve is not specified in the Text-Based SMT Photo Search.

NGI shall retrieve the matching SMT photos and any associated information for each candidate on a Text-Based SMT Photo Search response.

3.4.16.3 Text-Based SMT Photo Search Request Outputs

NGI shall provide a response to an Text-Based SMT Photo Search request in accordance with the latest EBTS version.

The EBTS TOT that supports the Text-Based SMT Photo Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide a response to a Text-Based SMT Photo Search request received via NCIC in accordance with the latest III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE for a Text-Based SMT Photo Search response will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to view the Text-Based SMT Photo Search response.

NGI shall allow an Authorized FBI Service Provider to print the Text-Based SMT Photo Search response.

NGI shall provide a ranked candidate list containing zero or more candidates in response to a Text-Based SMT Photo Search request.

NGI shall provide a candidate list containing UCN(s) and specific event data in response to a Text-Based SMT Photo Search request.

3.4.17 Facial Recognition Search Request

3.4.17.1 Facial Recognition Search Request Inputs

NGI shall accept a Facial Recognition Search request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Facial Recognition Search requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Facial Recognition Search request.

The NGI STOT that supports the Facial Recognition Search requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to submit photos via multiple methods (e.g., scanning, CD, DVD) for a Facial Recognition Search request.

NGI shall accept a designation of the repository(ies) to be included in a Facial Recognition Search.

NGI shall accept a Facial Recognition Search request with photos and biographic data.

NGI shall accept a specification of the number of candidates to return in a Facial Recognition Search request.

NGI shall accept a specified number of candidate photos to return in a Facial Recognition Search request.

NGI shall accept an indicator on a facial recognition search request that specifies if photos should be included with the Facial Recognition Search response.

NGI shall accept an indicator on a Facial Recognition Search request that specifies if photos should be enrolled into the UPF.

3.4.17.2 Facial Recognition Search Request Processing

NGI shall perform facial recognition searches using biographic and ANSI/NIST type-10 data as search criteria when provided in the Facial Recognition Search request.

NGI shall perform an automated image quality check of facial photo images submitted for Facial Recognition Searches.

NGI shall reject a Facial Recognition Search request that fails to meet minimum quality standards for facial recognition.

NGI shall perform facial recognition searches of the repository(ies) designated in the Facial Recognition Search request.

NGI shall perform facial recognition searches of the default photo repository when no repository is specified in the Facial Recognition Search request.

NGI shall calculate a match score for each candidate resulting from a Facial Recognition Search request.

NGI shall retrieve up to the number of candidates specified in the Facial Recognition Search request.

NGI shall retrieve up to the default number of candidates, when the number of candidates to return is not specified in the Facial Recognition Search request.

NGI shall retrieve up to the maximum number of photo images specified in the Facial Recognition Search request.

NGI shall retrieve up to the default number of photo images, when the number of photo images to return is not specified in the Facial Recognition Search request.

NGI shall enroll an Identity into the UPF when indicated as part of a Facial Recognition Search request.

NGI shall enroll photos into the UPF when indicated as part of a Facial Recognition Search request.

3.4.17.3 Facial Recognition Search Request Outputs

NGI shall provide a response to a Facial Recognition Search request in accordance with the latest EBTS version.

The EBTS TOT that supports the Facial Recognition Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide a ranked candidate list containing zero or more candidates in response to a Facial Recognition Search request.

NGI shall provide a candidate list containing UCN(s) and optional photos in response to a Facial Recognition Search request.

NGI shall allow an Authorized FBI Service Provider to view the Facial Recognition Search response.

NGI shall allow an Authorized FBI Service Provider to print the Facial Recognition Search response.

3.4.18 Deleted

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

3.4.19 Deleted

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

3.4.20 Deleted

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

3.4.21 Deleted

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

3.4.22 Iris Search Request

3.4.22.1 Iris Search Request Inputs

NGI shall accept an Iris Search request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Iris Search requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit an Iris Search request.

The NGI STOT that supports the Iris Search requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall allow an Authorized FBI Service Provider to submit iris images via multiple methods (e.g., scanning, CD, DVD) for an Iris Search request.

NGI shall accept a designation of the repository(ies) to be included in an Iris Search request.

NGI shall accept a specification of the number of candidates to return in an Iris Search request.

NGI shall accept an indicator on an Iris Search request that specifies if iris images should be included with the Iris Search response.

NGI shall accept a specified number of candidate iris images to return in an Iris Search request.

NGI shall accept an indicator on an Iris Search request that specifies if iris images should be enrolled into the UIF.

3.4.22.2 Iris Search Request Processing

NGI shall perform an automated image quality check of iris images submitted in an Iris Search request.

NGI shall reject an Iris Search request that fails to meet minimum quality standards for iris images.

NGI shall perform an Iris Search request using the biographic and iris data provided in the Iris Search request.

NGI shall search the repository(ies) designated in the Iris Search request.

NGI shall search the default iris repository when no repository is specified in the Iris Search request.

NGI shall calculate a match score for each candidate resulting from an Iris Search request.

NGI shall retrieve up to the number of candidates specified in the Iris Search request.

NGI shall retrieve up to the default number of candidates, when the number of candidates to return is not specified in the Iris Search request.

NGI shall retrieve up to the maximum number of iris images specified in the Iris Search request.

NGI shall retrieve up to the default number of iris images, when the number of iris images to return is not specified in the Iris Search request.

NGI shall enroll an Identity into the UIF when indicated as part of an Iris Search request.

NGI shall enroll iris data into the UIF when indicated as part of an Iris Search request.

3.4.22.3 Iris Search Request Outputs

NGI shall provide a response to an Iris Search request in accordance with the latest EBTS version.

The EBTS TOT that supports the Iris Search response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide a ranked candidate list containing zero or more candidates in response to an Iris Search request.

NGI shall provide a candidate list containing UCN(s) and optional iris images in response to an Iris Search request.

NGI shall allow an Authorized FBI Service Provider to view the Iris Search response.

NGI shall allow an Authorized FBI Service Provider to print the Iris Search response.

3.5 Notification Services Functional Requirements

The Notification Service provides Authorized Contributors with unsolicited notifications from the system based on event criteria (triggers). An unsolicited notification may be triggered by functions initiated by the system, Authorized FBI Service Providers, or Authorized Contributors. The notifications to the users may be in multiple formats (i.e., electronic, telephonic, hardcopy).

The following section contains the functional requirements supporting Notification user services.

3.5.1 Flash Notifications

A Flash Notification will be provided to an Authorized Contributor when activity or file maintenance occurs on a subject's record containing a Flash for that Contributor. Flashes may be placed on records for a subject whose activities are limited by court issued restrictions, supervision, protection orders, or deportation decrees.

Deleted.

NGI shall send a Flash Notification to an Authorized Contributor when an Identification Search results in a positive identification to a record containing a Flash for that Contributor.

NGI shall create a hardcopy Identity History Summary for a Flash Notification when appropriate.

3.5.2 Want Notifications

A Wanted Persons Notification will be provided to an Authorized Contributor when activity or file maintenance occurs on a subject's record containing a Want Notice for that Contributor. Wants are placed on a subject when a Wanted Person is entered into NCIC with a valid UCN. An Authorized FBI Service Provider may also place wants on a subject's record on behalf of an Authorized Contributor.

NGI shall send a Want Notification to an Authorized Contributor when file maintenance occurs on a subject's record containing a Want for that Contributor.

NGI shall send a Want Notification to an Authorized Contributor when their identification search results in a positive identification to a record containing a want.

NGI shall send a Want Notification to the wanting agency when external system activity occurs on a linked record containing an active want based on dissemination rules.

NGI shall create a hardcopy Identity History Summary for a Want Notification when appropriate.

NGI shall provide a Want Notification in accordance with the latest Nlets User and Technical Guide.

The NGI STOT that supports the Nlets MKE for a Want Notification is AM.

NGI shall send a Want Notification to the wanting agency when a fingerprint verification request matches a record containing an active want.

3.5.3 Sexual Offender Registry Notification

NGI will notify the original registering agency of activity on subject records that contain Sexual Offender Registry (SOR) data. When there is file maintenance on a subject's record (e.g., posting an

arrest, consolidating records, expungement of last cycle), NGI will send a notice to each registering agency.

NGI shall send a Sexual Offender Registry Notification to an Authorized Contributor when file maintenance occurs on a subject's record containing SOR data for that Contributor.

NGI shall provide a Sexual Offender Registry Notification in accordance with the latest Nlets User and Technical Guide.

The NGI STOT that supports the Nlets MKE for a Sexual Offender Registry Notification is AM.

3.5.4 Other Special Interest Notification

NGI will notify the appropriate agency of activity on subjects of Special Interest. When there is file maintenance on a subject's record (e.g., posting an arrest, consolidating records, expungement of last cycle), NGI will send a notice to the appropriate agency.

NGI shall send Special Interest Notifications to Authorized FBI Service Providers.

NGI shall send Special Interest Notifications to Authorized Contributors in accordance with the latest III/NFF Operational and Technical Manual.

NGI shall send Special Interest Notifications to External Systems when appropriate, in accordance with the latest EBTS version.

NGI shall send a Special Interest Notification when file maintenance occurs on a subject's record marked as Special Interest.

NGI shall send a Special Interest Notification to an Authorized Contributor when external system activity occurs on a linked record containing a special processing flag based on dissemination rules.

NGI shall create a hardcopy Special Interest Notification when appropriate.

3.5.5 III/NFF File Maintenance Notification

A State Bureau for a III/NFF state will be notified when file maintenance activities (e.g., posting an arrest, consolidating records or expungement of last cycle) occur against a record they own within NGI. Additionally, a III/NFF State Bureau will be notified of the search and record status resulting from a Tenprint Fingerprint Identification Search submitted by an Authorized Contributor within their state.

NGI shall send a File Maintenance Notification to an Authorized Contributor in accordance with the latest III/NFF Operational and Technical Manual.

NGI shall send a File Maintenance Notification to the III/NFF State Bureau when file maintenance activity occurs on a record owned by that State Bureau.

NGI shall send a File Maintenance Notification to the III/NFF State Bureau, when appropriate, indicating the search and record status resulting from a Tenprint Fingerprint Identification Search.

3.5.6 Unsolved Biometric Notification

An Unsolved Biometric Notification contains either a decision notification or an unsolved file match notification for any of the biometrics (i.e., fingerprint, latent, palm, photo, or iris). These notifications are sent to the owner of the biometric that could be an Authorized Contributor or an Authorized FBI Service Provider (e.g., Latent Examiner).

NGI shall send an Unsolved Biometric Notification to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Unsolved Biometric Notification is ULM.

NGI shall send an Unsolved Biometric Match Notification to an Authorized FBI Service Provider when appropriate.

The NGI STOT that supports the Unsolved Biometric Notification is ULM.

NGI shall send an Unsolved Biometric Match Notification to the owner of a ULF print when a potential tenprint fingerprint match has resulted from a cascaded search.

NGI shall send a positive tenprint Fingerprint Decision to the Unsolved Latent Owner if the decision was not made by the Unsolved Latent Owner.

NGI shall send an Unsolved Biometric Match Notification to the owner of a ULF print when a potential latent print match has resulted from a cascaded search.

NGI shall send a positive Latent Decision to the Unsolved Latent Owner if the positive latent decision was not made by the Unsolved Latent Owner.

NGI shall send an Unsolved Biometric Match Notification to the ULF latent owner when a potential palmprint match has resulted from a cascaded search.

Deleted.

NGI shall send an Unsolved Biometric Match Notification to the ULF latent owner when a potential supplemental fingerprint and palmprint match has resulted from a cascaded search.

Deleted.

NGI shall send an Unsolved Biometric Match Notification to the UPF photo owner when a potential facial photo match has resulted from a cascaded search.

NGI shall send a positive Photo Decision Notification to the UPF photo owner if the positive photo decision was not received from the owner.

NGI shall send an Unsolved Biometric Match Notification to the UIF iris owner when a potential iris match has resulted from a cascaded search.

NGI shall send a positive Iris Decision Notification to the UIF iris owner if the positive iris decision was not received from the iris owner.

NGI shall send an Unsolved Biometric Notification for each candidate resulting from a cascaded search that has a match score above the appropriate cascaded search match threshold.

3.5.7 Special Population Cognizant Notification

A Special Population Cognizant Notification is either a positive decision notification or an SPC File match notification for any biometric (e.g., fingerprint, latent, palm, photo, iris). These notifications are sent to the owner of the biometric, which could be an Authorized Contributor or an Authorized FBI Service Provider (e.g., Latent Examiner).

NGI shall send a Special Population Cognizant Notification to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Special Population Cognizant Notifications will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall send a Special Population Cognizant Notification to an Authorized FBI Service Provider when appropriate.

The NGI STOT that supports the Special Population Cognizant Notifications will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall send a Special Population Cognizant Notification to the owner of a marked SPC File when a potential tenprint fingerprint match has resulted from a cascaded search.

NGI shall send a positive tenprint Fingerprint Decision to the SPC File Owner if the decision was not made by the SPC File Owner.

NGI shall send a Special Population Cognizant Notification to the owner of a marked SPC File when a potential latent print match has resulted from a cascaded search.

NGI shall send a positive Latent Decision to the SPC File Owner if the positive latent decision was not made by the SPC File Owner.

NGI shall send a Special Population Cognizant Notification to the owner of a marked SPC File when a potential palmprint match has resulted from a cascaded search.

Deleted.

NGI shall send a Special Population Cognizant Notification to the owner of a marked SPC File when a potential supplemental fingerprint and palmprint match has resulted from a cascaded search.

Deleted.

NGI shall send a Special Population Cognizant Notification to the owner of a marked SPC File when a potential facial photo match has resulted from a cascaded search.

NGI shall send a positive Photo Decision Notification to the SPC File photo owner if the positive photo decision was not received from the owner.

NGI shall send a Special Population Cognizant Notification to the owner of a marked SPC File when a potential iris match has resulted from a cascaded search.

NGI shall send a positive Iris Decision Notification to the owner of a marked SPC File if the positive iris decision was not received from the Iris Owner.

NGI shall send a Special Population Cognizant Notification for each candidate resulting from a cascaded search that has a match score above the appropriate cascaded search match threshold.

3.5.8 Unsolicited Unsolved Latent Record Delete Notification

The Unsolicited Unsolved Latent Record Delete Notification informs the ULF record owner that their record has been deleted due to ULF reaching maximum capacity.

NGI shall send an Unsolicited Unsolved Latent Record Delete Notification to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Unsolicited Unsolved Latent Record Delete Notification is UULD.

NGI shall send an Unsolicited Unsolved Latent Record Delete Notification to an Authorized FBI Service Provider when appropriate.

The NGI STOT that supports the Unsolicited Unsolved Latent Record Delete Notification is UULD.

NGI shall send an Unsolicited Unsolved Latent Record Delete Notification to the owner of an unsolved latent print when their record is deleted as a result of ULF reaching maximum capacity resulting from an add to the ULF.

3.5.9 Biometric Deletion Notification

The Biometric Deletion Notification informs the contributor that the biometric used to make a positive decision has been deleted from NGI.

Deleted.

Deleted.

3.5.10 Rap Back Activity Notification

NGI shall send Rap Back Activity Notification in accordance with the latest EBTS version.

The EBTS TOT that supports the Rap Back Activity Notification is RBHN.

NGI shall send Rap Back Activity Notification to the appropriate Authorized Contributors based on Rap Back Notification Rules.

Rap Back Notification Rules will indicate if an Authorized Recipient receives pre-notification, an Identity History Summary or just triggering event information.

NGI shall send Rap Back Activity Notification to the appropriate Authorized Contributors that a Rap Back designated event has occurred against a Rap Back enrolled Identity as a result of a positive fingerprint identification.

An External System Link Activity request from an External System or NFF Criminal Print Ident request from an NFF State is considered a positive identification and may trigger Rap Back Activity Notifications. NFF States will only provide NFF Criminal Print Ident messages request when a criminal identification is made. RISC Notifications may be provided to both the arresting agency and the NFF State's CSO as a result of an NFF Criminal Print Ident message request.

NGI shall send Rap Back Activity Notification to the appropriate Authorized Contributors when a Rap Back designated event is part of a consolidation of Identity(ies) enrolled in Rap Back.

NGI shall send Consolidation Notifications to the appropriate Authorized Contributors when any identities involved in the consolidation are enrolled in Rap Back.

NGI shall send Rap Back Activity Notification to the appropriate Authorized Contributors when disposition activity occurs against a Rap Back enrolled Identity.

NGI shall send Rap Back Activity Notification to the appropriate Authorized Contributors when expungement activity occurs against a Rap Back enrolled Identity.

NGI shall send Rap Back Activity Notification to the appropriate Authorized Contributors when an External System Activity request is received for a Rap Back enrolled Identity.

NGI shall include a unique Rap Back Notification Identifier in a Rap Back Activity Notification.

NGI shall include an Identity History Summary in a Rap Back Activity Notification based on Rap Back Notification Rules.

NGI shall indicate the triggering event when an Identity History Summary is included as part of a Rap Back Activity Notification.

NGI shall create a hardcopy Identity History Summary for a Rap Back Activity Notification when appropriate.

3.5.11 Rap Back Renewal Notification

NGI shall send Rap Back Renewal Notification in accordance with the latest EBTS version.

The EBTS TOT that supports the Rap Back Renewal Notification will be developed in accordance with the ANSI/NIST Data Format for the Interchange of Fingerprints, Facial and other Biometric Information.

NGI shall send Rap Back Renewal Notification to the Authorized Contributor prior to expiration of a Rap Back subscription.

3.5.12 RISC Notification

A notification will be provided to the owner of a RISC record when a positive identification against that record is made.

NGI shall send RISC Notifications to RISC Record Owners in accordance with the latest EBTS version.

The EBTS TOT that supports the RISC Notifications will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall send RISC Notifications to RISC Record Owners in accordance with the latest ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

The ANSI/NIST-ITL TOT that supports the RISC Notifications will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall send RISC Notifications to Authorized Contributors in accordance with the Nlets User and Technical Guide.

NGI shall send a RISC Notification to the RISC record owner when any identification search results in a positive identification with their marked tier-1 or marked tier-2 RISC record.

NGI shall send a RISC Notification to the RISC record owner when any identification search results in a positive identification with their tier-3 RISC record.

NGI shall send a RISC Notification to the RISC record owner when any Verification request results in a positive identification with their marked tier-1 or marked tier-2 RISC record.

NGI shall send a RISC Notification to the RISC record owner when any Verification request results in a positive identification with their tier-3 RISC record.

An External System Link Activity Notification from an External System or NFF Criminal Print Ident Notification from an NFF State is considered a positive identification and may trigger RISC Notifications. NFF States will only provide NFF Criminal Print Ident Notifications when a criminal identification is made. RISC Notifications may be provided to both the arresting agency and the NFF State's CSO as a result of an NFF Criminal Print Ident Notification.

NGI will not notify the ITF record owner(s) when an International Terrorist Identification Search enrollment request, from another Authorized Contributor, results in a positive identification with the owner's tier-3 record and the enrollment's tier level indicator is "3".

NGI shall send a RISC Notification to the RISC record owner when a positive biometric decision is received on their marked tier-1 or marked tier-2 RISC record as a result of an investigative search.

NGI shall send a RISC Notification to the RISC record owner when a positive biometric decision is received on their tier-3 RISC record as a result of an investigative search.

A positive biometric decision may be a photo, iris, tenprint fingerprint, palmprint, supplemental fingerprint and palmprint, or latent decision.

NGI shall send a RISC Notification to the NFF State, using the multi-tiered dissemination rules, when an NFF Criminal Print Ident request is received for a positive identification on an Identity that is enrolled in the RISC repository.

NGI shall send a RISC Notification to the designated FBI entity when any Identification Search results in positive identification with a tier-3 ITF record.

NGI shall send a RISC Notification to the designated FBI entity when a cascaded search results in a potential match with tier-3 ITF record.

3.5.13 Immigration Violator File Notification

An Immigration Violator File Notification will be provided to the LESC when activity or file maintenance occurs on a subject's record containing an IVF indicator. IVF indicators are placed on a subject when an IVF record is entered into NCIC with a valid UCN.

NGI shall send an Immigration Violator File Notification to the LESC when a Fingerprint Verification request matches a record containing an IVF indicator.

NGI shall send an Immigration Violator File Notification to the LESC when an Identification Search request matches a record containing an IVF indicator.

NGI shall send an Immigration Violator File Notification to the LESC when file maintenance activity occurs on a record containing an IVF indicator.

NGI shall send Immigration Violator File Notification to the LESC when external system activity occurs on a linked record containing an IVF indicator based on dissemination rules.

NGI shall send an Immigration Violator File Notification to the LESC in accordance with the Nlets User and Technical Guide.

The NGI STOT that supports the Nlets MKE for an Immigration Violator File Notification is AM.

3.5.14 External System Link Notification

The following functional requirements are related to providing an External System notification of NGI activity on linked record(s).

NGI shall send a Linked Record Activity Notification to an External System when a Fingerprint Verification request matches a record containing a link to that External System.

NGI shall send a Linked Record Activity Notification to an External System when an identification search results in a positive identification to a record containing a link to that External System.

An NFF Criminal Print Ident Notification from an NFF State is considered a positive identification and may trigger a Linked Record Activity Notification. NFF States will only provide these notifications when a criminal identification is made.

NGI shall send a Linked Record Activity Notification to an External System when an NGI Identity Maintenance activity occurs on a record containing a link to that External System.

NGI shall provide the UCN and associated external system link identifier as part of the Linked Record Activity Notification to an External System.

NGI shall send Linked Record Activity Notification in accordance with the latest EBTS version.

The EBTS TOT that supports the Linked Record Activity Notifications will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall send a Link Failure Notification to an External System (e.g., IDENT) in accordance with the latest EBTS version when a link cannot be established.

The EBTS TOT that supports the Link Failure Notifications will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.5.15 Shared Data Notification

Shared Data Notifications are unsolicited messages between NGI (iDSM) and an External System (e.g., IDENT) system notifying the other agency of a positive identification against shared data.

NGI shall send a Shared Data Hit Notification to an External System (e.g., IDENT) when there is a positive identification against an image contained in the Shared Data as a result of an NGI Tenprint Identification Search request from an Authorized Contributor participating in Shared Data.

NGI shall include in the Shared Data Hit Notification to an External System (e.g., IDENT) the associated NGI submission type (e.g., criminal arrest, civil application) that resulted in a positive identification against the Shared Data.

NGI shall include in the Shared Data Hit Notification to an External System (e.g., IDENT) the associated Agency's Site Identifier for any NGI Tenprint Identification Search request of the Shared Data resulting in a positive identification.

NGI shall accept a Shared Data Hit Notification from an External System (e.g., IDENT) when there is a positive identification of a fingerprint submission against an NGI image contained in the shared data.

NGI shall accept as part of a Shared Data Hit Notification the reason for the External System's (e.g., IDENT) submission type (e.g., Port of Entry (POE), Customs and Border Protection (CBP), Visa, Latent Search) that resulted in a positive identification.

3.5.16 IDENT Hit Notification

An IDENT Hit Notification will be provided to the LESC for Tenprint submissions that have a match in the IDENT system. The notification will be implemented using an Immigration Alien Query (IAQ).

NGI shall send an IDENT Hit Notification to the LESC, based on LESC Notification Rules, when a Tenprint Fingerprint Identification Search results in a positive identification to an Identity containing an External System link for the IDENT system and the date of the event is within the LESC notification time limit.

This should include an Identity with an existing record link to the IDENT system or an Identity where the record link is established to IDENT as part of the Tenprint Fingerprint Identification Search. The date of the arrest or the civil event date must be within the configurable number of days.

NGI shall send an IDENT Hit Notification to the LESC, based on LESC Notification Rules, when a Tenprint Fingerprint Identification Search results in a match within the IDENT system and the date of the event is within the LESC notification time limit.

This will include a contributor directed search of IDENT where the subject is not retained within NGI or does not result in a positive identification to an existing NGI record. The event date must be within the configurable number of days.

Only one IDENT Hit Notification will be sent to the LESC per Tenprint Identification Search.

NGI shall send an IDENT Hit Notification to the LESC in accordance with the Nlets User and Technical Guide.

NGI shall send an IDENT Hit Notification to the LESC, based on LESC Notification Rules, when a NFF Criminal Print Ident request results in a positive identification to an Identity containing an External System link for the IDENT system.

A IDENT Hit Notification should not be sent to the LESC if an IAQ is already being sent as a result of other processing.

3.5.17 Foreign or Unknown Place of Birth Notification

A Foreign or Unknown Place of Birth Notification will be provided to the LESC for all criminal Tenprint submissions that indicate a foreign or unknown place of birth. The notification will be implemented using an Immigration Alien Query (IAQ).

NGI shall send a Foreign or Unknown Place of Birth Notification to the LESC, based on LESC Notification Rules, when a criminal Tenprint Fingerprint Identification Search contains a subject with a foreign or unknown place of birth and the date of the event is within the LESC notification time limit.

NGI shall send a Foreign or Unknown Place of Birth Notification to the LESC, based on LESC Notification Rules, when a criminal Tenprint Fingerprint Identification Search results in a positive identification to an Identity with a foreign or unknown place of birth and the date of the event is within the LESC notification time limit.

NGI shall send a Foreign or Unknown Place of Birth Notification to the LESC in accordance with the Nlets User and Technical Guide.

Only one Foreign or Unknown Place of Birth Notification will be sent to the LESC per Tenprint Identification Search.

3.6 Data Management Service Functional Requirements

The following section contains the functional requirements supporting Data Management user services.

3.6.1 Fingerprint Image Replacement Request

A Fingerprint Image Replacement request is a full replacement of composite fingerprint images and features.

3.6.1.1 Fingerprint Image Replacement Request Inputs

NGI shall accept Fingerprint Image Replacement requests from Authorized Contributors in accordance with the latest EBTS version.

NGI shall accept Fingerprint Image Replacement requests from Authorized External System in accordance with the latest EBTS version.

The EBTS TOT that supports the Fingerprint Image Replacement request is FIS.

NGI shall allow an Authorized FBI Service Provider to submit a Fingerprint Image Replacement request.

The NGI STOT that supports the Fingerprint Image Replacement request is IFIS.

NGI shall require Tenprint fingerprint images and a UCN as part of a Fingerprint Image Replacement request.

3.6.1.2 Fingerprint Image Replacement Request Processing

NGI shall retrieve the fingerprint images associated with the specified UCN as part of a Fingerprint Image Replacement request.

NGI shall reject the Fingerprint Image Replacement request when the specified UCN is invalid.

NGI shall perform III/Verify as part of a Fingerprint Image Replacement request for the specified UCN.

NGI shall extract fingerprint features from the fingerprint images provided in the Fingerprint Image Replacement request.

NGI shall perform an image quality check on a Fingerprint Image Replacement request based on image quality standards.

NGI shall compare the fingerprint features extracted from the fingerprint images provided in the Fingerprint Image Replacement request against the fingerprint features of the candidate provided to III/Verify.

NGI shall calculate a match score for the candidate resulting from a Fingerprint Image Replacement request.

NGI shall determine a non-identification decision for a candidate that has a match score below the minimum threshold for III/Verify as part of a Fingerprint Image Replacement request.

NGI shall determine a positive identification decision for a candidate that has a match score above the high confidence threshold as part of a Fingerprint Image Replacement request.

NGI shall require an Authorized FBI Service Provider to perform a manual FIC when the candidate returned as part of the Fingerprint Image Replacement request is below the high confidence threshold.

NGI shall require a second Authorized FBI Service Provider to perform a manual FIC to confirm a positive identification when the candidate returned as part of a Fingerprint Image Replacement request is below the low confidence threshold.

The second manual FIC will be performed independent of the first FIC decision. The decision made by the first service provider will not be made known to the second service provider.

NGI shall allow an Authorized FBI Service Provider to reject a Fingerprint Image Replacement request as a result of the manual FIC.

NGI will reject a Fingerprint Image Replacement request that results in a non-identification decision.

NGI shall replace fingerprint images and features associated with the specified UCN using the fingerprint images provided in a Fingerprint Image Replacement request that results in a positive identification decision.

NGI shall perform a cascaded fingerprint search of the ULF when the composite fingerprint images are updated in accordance with cascaded search business rules.

NGI shall perform a cascaded fingerprint search of marked SPC files when the composite fingerprint images are updated in accordance with cascaded search business rules.

3.6.1.3 Fingerprint Image Replacement Request Outputs

NGI shall provide a response to a Fingerprint Image Replacement request in accordance with the latest EBTS version.

The EBTS TOT that supports the Fingerprint Image Replacement response is FISR.

NGI shall provide the appropriate Fingerprint Image Replacement response to an Authorized FBI Service Provider.

3.6.2 Fingerprint Image Update Request

The following functional requirements relate to fingerprint image update requests performed by Authorized FBI Service Providers only. Updates to fingerprint images for a specific event include fingerprint sequence corrections and the application of missing, scars, and amputation stamps. The fingerprint composite will be rebuilt as part of a Fingerprint Image Update request.

3.6.2.1 Fingerprint Image Update Inputs

NGI shall allow an Authorized FBI Service Provider to submit a Fingerprint Image Update request.

The NGI STOT that supports the Fingerprint Image Update request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a Fingerprint Image Update request to contain a UCN and fingerprint specific information.

3.6.2.2 Fingerprint Image Update Processing

NGI shall retrieve the fingerprints specified in the Fingerprint Image Update request.

NGI shall allow the Authorized FBI Service Provider to view the fingerprints specified in the Fingerprint Image Update request.

NGI shall provide the capability to perform sequence error corrections for the specified fingerprints as part of a Fingerprint Image Update request.

NGI shall provide the capability to apply stamps to the specified fingerprints as part of a Fingerprint Image Update request.

NGI shall update the specified fingerprints as part of Fingerprint Image Update request.

NGI shall update the fingerprint composite as a result of a Fingerprint Image Update request.

3.6.2.3 Fingerprint Image Update Outputs

NGI shall provide the appropriate Fingerprint Image Update response to an Authorized FBI Service Provider.

3.6.3 Fingerprint Deletion Request

The following functional requirements relate to fingerprint maintenance. Updates to fingerprints for a specific event can be performed by deleting the desired fingerprints and then enrolling the new fingerprints.

3.6.3.1 Fingerprint Deletion Inputs

NGI shall accept a Fingerprint Deletion request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall accept a Fingerprint Deletion request from an Authorized External System in accordance with the latest EBTS version

The EBTS TOT that supports Fingerprint Deletion requests will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Fingerprint Deletion request.

The NGI STOT that supports the Fingerprint Deletion requests will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall accept Fingerprint Deletion requests for the ULF Repository.

NGI shall accept Fingerprint Deletion requests for the RISC.

NGI shall accept Fingerprint Deletion requests for an SPC File.

NGI shall require Fingerprint Deletion requests to contain a UCN.

NGI shall require Fingerprint Deletion requests to contain fingerprint specific information.

3.6.3.2 Fingerprint Deletion Processing

NGI shall delete the fingerprints specified in the Fingerprint Deletion request.

NGI shall reject a Fingerprint Deletion request if the specified UCN or fingerprints do not exist.

3.6.3.3 Fingerprint Deletion Outputs

NGI shall provide a Fingerprint Deletion response in accordance with the latest EBTS version.

The EBTS TOT that supports the Fingerprint Deletion response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate Fingerprint Deletion response to an Authorized FBI Service Provider.

3.6.4 Fingerprint Decision Request

Authorized Contributors and FBI Service Providers can return positive, negative, or inconclusive decisions for candidates provided to them as a result of a tenprint fingerprint investigation search request or unsolved biometric notification. These decisions are used internally for statistical and algorithm analysis. Additionally, a positive decision returned from an unsolved latent owner can result in automatic deletion of the unsolved latent.

3.6.4.1 Fingerprint Decision Inputs

NGI shall accept a Fingerprint Decision from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Fingerprint Decision will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Fingerprint Decision.

The NGI STOT that supports the Fingerprint Decision will be developed in accordance with the NGI Message Definition Database (MDD).

3.6.4.2 Fingerprint Decision Processing

NGI shall record the Fingerprint Decision.

NGI shall delete the referenced fingerprints from the ULF if a positive tenprint Fingerprint Decision is received from the ULF Fingerprint Owner.

3.6.4.3 Fingerprint Decision Outputs

NGI shall provide a reject response, as appropriate, for a Fingerprint Decision.

NGI shall provide a response to a Fingerprint Decision from an Authorized Contributor in accordance with the latest EBTS version.

There will be no EBTS normal NGI responses other than communication protocol acknowledgments for this transaction type. If there is an error in the submittal, a reject response will be returned.

3.6.5 Identity History Record Modification Request

Identity History Record Modification (SCHMOD) request provides the capabilities for an Authorized FBI Service Provider to modify Identity history information. This capability will allow the addition, modification, and deletion of selected data elements.

3.6.5.1 Identity History Record Modification Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit an Identity History Record Modification request.

The NGI STOT that supports the Identity History Record Modification requests is SCHD.

NGI shall require a UCN as part of an Identity History Record Modification request.

NGI shall require a designation of maintenance action as part of an Identity History Record Modification request.

Maintenance actions may include addition, modifications, or deletions of individual biographic data, event data, or other Identity History data elements. The maintenance action may also indicate deletion of entire Identity History records.

3.6.5.2 Identity History Record Modification Request Processing

NGI shall perform the designated biographic maintenance action on the specified Identity's history record as part of the Identity History Record Modification request.

NGI shall perform the designated Identity information maintenance action on the specified Identity's history record as part of the Identity History Record Modification request.

NGI shall perform the designated event maintenance action on the specified Identity's history record as part of the Identity History Record Modification request.

NGI shall reject the Identity History Record Modification request when specified UCN is invalid.

3.6.5.3 Identity History Record Modification Request Outputs

NGI shall provide the appropriate Identity History Record Modification response to an Authorized FBI Service Provider.

3.6.6 III Record Maintenance Request

III Identity Record Maintenance request provides the capabilities for an Authorized Contributor to modify Identity information. This capability will allow the addition, modification, and deletion of selected data elements.

3.6.6.1 III Record Maintenance Request Inputs

NGI shall accept a III Record Maintenance request for an Identity from an Authorized Contributor in accordance with the III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKEs for the SCH Record Modification requests are: MRS, EHN, and XHN.

NGI shall accept an III Record Maintenance request for an Identity from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the III Record Maintenance request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall require a UCN or SID as part of a III Record Maintenance request.

NGI shall allow an Authorized Contributor to add supplemental biographic identifiers as part of a III Record Maintenance request.

This supports the EHN III message.

NGI shall allow an Authorized Contributor to delete supplemental biographic identifiers as part of a III Record Maintenance request.

This supports the XHN III message.

NGI shall allow an Authorized Contributor to modify Identity Information as part of a III Record Maintenance request.

This supports the MRS III message.

3.6.6.2 III Record Maintenance Request Processing

NGI shall perform the designated biographic maintenance action on the specified Identity's history record as part of the III Record Maintenance request.

NGI shall perform the designated Identity information maintenance action on the specified Identity History Record as part of the III Record Maintenance request.

NGI shall reject the III Record Maintenance request when a specified UCN or SID is invalid.

3.6.6.3 III Record Maintenance Request Outputs

NGI shall provide the appropriate III Record Maintenance response to an Authorized Contributor in accordance with the III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE for a III Record Maintenance response will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall provide a response to a III Record Maintenance request in accordance with the latest EBTS version.

The EBTS TOT that supports the III Record Maintenance response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.6.7 External System Record Maintenance Request

External System Identity Record Maintenance request provides the capabilities for an External System to modify Identity information. This capability will allow the addition, modification, and deletion of selected data elements.

3.6.7.1 External System Record Maintenance Request Inputs

NGI shall accept an External System Record Maintenance request for an Identity from an Authorized External System in accordance with the latest EBTS version.

The EBTS TOT that supports the External System Record Maintenance request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall require a UCN and External System Identifier as part of an External System Record Maintenance request.

NGI shall accept supplemental biographic identifiers to be added as part of an External System Record Maintenance request.

NGI shall accept supplemental biographic identifiers to be deleted as part of an External System Record Maintenance request.

3.6.7.2 External System Record Maintenance Request Processing

NGI shall perform the designated biographic maintenance action on the specified Identity's history record as part of the External System Record Maintenance request.

Deleted.

NGI shall reject the External System Record Maintenance request when specified UCN or External System Identifier is invalid.

3.6.7.3 External System Record Maintenance Request Outputs

NGI shall provide a response to an External System Record Maintenance request in accordance with the latest EBTS version.

The EBTS TOT that supports the External System Record Maintenance response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.6.8 International Terrorist File Record Maintenance Request

3.6.8.1 International Terrorist File Record Maintenance Request Inputs

NGI shall accept an International Terrorist File Record Maintenance request from an Authorized ITF Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the International Terrorist File Record Maintenance request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow Authorized FBI Service Providers to submit International Terrorist File Record Maintenance requests.

The NGI STOT that supports the International Terrorist File Record Maintenance request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a UCN as part of an International Terrorist File Record Maintenance request.

NGI shall accept a designation of maintenance action (modify, delete, or copy) as part of an International Terrorist File Record Maintenance request.

Maintenance actions may include modifications or deletions of individual biographical data, event data, or other Identity History data elements. The maintenance action may also include changing tier designations and copying a record into the International Terrorist File from another NGI repository.

3.6.8.2 International Terrorist File Record Maintenance Request Processing

NGI shall perform the designated maintenance action to remove a record from the International Terrorist File as part of an ITF Record Maintenance request.

NGI shall perform the designated maintenance action to modify a record from the International Terrorist File as part of an ITF Record Maintenance request.

NGI shall perform the designated maintenance action to copy a record from another NGI repository into the International Terrorist File as part of an ITF Record Maintenance request.

NGI shall reject an International Terrorist File Record Maintenance request when the specified UCN is invalid.

3.6.8.3 International Terrorist File Record Maintenance Request Outputs

NGI shall provide a response to an International Terrorist File Record Maintenance request in accordance with the latest EBTS version.

The EBTS TOT that supports the International Terrorist File Record Maintenance response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate International Terrorist File Record Maintenance response to an Authorized FBI Service Provider.

3.6.9 Special Stops Maintenance Request

The Special Stops Maintenance request provides the capability for an Authorized FBI Service Provider to change Identity status or permissions. This capability also allows an Authorized FBI Service Provider to create an Identity with or without associated fingerprint image data.

3.6.9.1 Special Stops Maintenance Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit a Special Stops Maintenance request.

The NGI STOT that supports the Special Stops Maintenance request is SSMD.

NGI shall accept a UCN as part of a Special Stops Maintenance request.

NGI shall accept fingerprint image data as part of a Special Stops Maintenance request.

NGI shall accept a designation of the maintenance action to perform as part of a Special Stops Maintenance request.

Special Stops Maintenance actions include: removal of fingerprint images from a non-criminal Identity and the addition of fingerprint images to an Identity that does not contain fingerprint image data. Special Stops Maintenance actions will result in the modification of the record status based on AUD Codes (i.e., AUD T to AUD P, AUD P to AUD T).

NGI shall allow an Authorized FBI Service Provider to input fingerprint images as part of a Special Stops Maintenance request, when applicable.

The modification of a record's AUD code from AUD T to AUD P will require Service Provider input of the fingerprint images.

3.6.9.2 Special Stops Maintenance Request Processing

NGI shall perform the designated maintenance action on the specified Identity as part of the Special Stops Maintenance request.

Maintenance actions are designated by the Type of Stop (TYS) indicator (E [Change AUD T to AUD P] and D [Change AUD P to AUD T]).

NGI shall reject the Special Stops Maintenance request when the specified UCN is invalid.

3.6.9.3 Special Stops Maintenance Request Outputs

NGI shall provide the appropriate Special Stops Maintenance response to an Authorized FBI Service Provider.

3.6.10 Master Subject Criminal History (SCH) Record Conversion Request

Master SCH Record Conversion provides the capability for an Authorized FBI Service Provider to add event and corresponding fingerprint image data to an existing SCH record marked as a manual record.

3.6.10.1 Master SCH Record Conversion Inputs

NGI shall allow an Authorized FBI Service Provider to submit a Master SCH Record Conversion request.

The NGI STOT that supports the Master SCH Record Conversion is MRCD.

NGI shall require a UCN as part of a Master SCH Record Conversion request.

NGI shall require criminal history event information as part of a Master SCH Record Conversion request.

3.6.10.2 Master SCH Record Conversion Processing

NGI shall associate fingerprint image data and criminal history event information to the specified UCN's SCH record as part of Master SCH Record Conversion request.

NGI shall reject the Master SCH Record Conversion request when specified UCN is invalid.

3.6.10.3 Master SCH Record Conversion Outputs

NGI shall provide the appropriate Master SCH Record Conversion response to an Authorized FBI Service Provider.

3.6.11 Disposition Submission Request

The Disposition Submission request service updates a criminal history record by associating court and custody information to an arrest cycle. Disposition submissions will not contain fingerprints and may be

received via NCIC, the CJIS WAN or by mail (hardcopy and MRD).

3.6.11.1 Disposition Submission Request Inputs

NGI shall accept NCIC Disposition Submission requests from an Authorized Contributor in accordance with the latest III/NFF Operations and Technical Manual.

The NGI STOT that supports the NCIC MKE for the NCIC Disposition Submission requests is DSP.

NGI shall accept Disposition Submission requests from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Disposition Submission request is DSPE.

NGI shall accept Disposition Submission requests from Authorized Contributors in accordance with the MRD Disposition Manual.

The NGI STOT that supports the MRD Disposition Submission requests is DSPM.

NGI shall allow an Authorized FBI Service Provider to submit a Disposition Submission request.

The NGI STOT that supports the Authorized FBI Service Provider submitted Disposition Submission request is DSPD.

NGI shall require primary identifiers as part of a Disposition Submission request.

NCIC Disposition Submission requests will contain a UCN or SID as the primary identifier. UCN will take precedence and the SID will be ignored when both UCN and SID are provided.

EBTS Disposition Submission requests will contain one or more primary identifiers. Primary identifiers for EBTS Disposition Submission requests may include: UCN, SID, Social Security Number, and/or Miscellaneous Number.

MRD Disposition Submission requests will contain a UCN as the primary identifier.

Disposition Submission requests submitted from an Authorized FBI Service Provider will contain a UCN as the primary identifier.

NGI shall require secondary identifiers as part of a Disposition Submission request.

Secondary identifiers for NCIC Disposition Submission requests must include: Controlling Agency Identifier, Disposition Maintenance Indicator, Date of Arrest, Date of Arrest - Suffix, Identification for Firearms Sales, and Disposition Set which includes the Court Count, Court Offense Numeric, Court Offense Literal, and the Court Provisional Literal and must be submitted in the sequence listed.

Secondary identifiers for EBTS Disposition Submission requests may include: Place of Birth, Sex, Race, Height, Weight, Eye Color, Hair Color, State Arrest Number, and Court Case Number. EBTS Disposition Submission requests must contain two or more secondary identifiers. All Disposition Submission requests must contain associated court &/or custody information (CON/COL/CPL).

Secondary identifiers for MRD Disposition Submission requests may include: Contributor Assigned Identification Number, FBI Number, Date of Arrest, Date of Arrest – Suffix, Originating Agency

Identification Number, Court Disposition Quantity, Disposition Submission Type, Identification for Firearms Sales, Filler (Blank (b) hexadecimal value of 40), Court Offense Literal, Court Offense Numeric, and Court Provisional Literal (includes custody, supervisory, parole dispositions, and additional court dispositions).

Secondary identifiers for Disposition Submission requests submitted by Authorized FBI Service Providers may include: Name, Date of Birth, Sex , SID, Social Security Number, Origination Agency Identifier, Controlling Agency Identifier, Originating Agency Case Number, Identification for Firearms, Date of Arrest, Date of Arrest – Suffix, Court Offense Numeric, Court Offense Literal, and the Court Provisional Literal.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

3.6.11.2 Disposition Submission Request Processing

NGI shall determine the Identity associated with the Disposition Submission request.

NCIC and MRD Disposition Submission requests determine the Identity using primary and secondary identifiers.

EBTS and Authorized FBI Service Provider Disposition Submission requests use biographic validation, in addition to primary and secondary identifiers to determine the Identity.

NGI shall provide conflict resolution when an associated unique Identity can not be determined for a Disposition Submission request. .

NGI shall update the Identity with disposition data from a Disposition Submission request when a unique arrest event exists that matches the submitted DOA and ORI, and a disposition for that DOA does not already exist.

NCIC, EBTS and MRD Disposition Submission requests require a maintenance indicator that will determine whether disposition data may be automatically applied when disposition data already exists for the unique arrest event that matches the submitted DOA and ORI.

NGI shall provide conflict resolution for a Disposition Submission request when submitted disposition data cannot be automatically applied to the specified Identity.

Deleted.

NGI shall reject a Disposition Submission request when the specified primary identifier is invalid.

NGI shall reject a Disposition Submission request when the specified DOA is invalid.

3.6.11.3 Disposition Submission Request Outputs

NGI shall provide a response to an EBTS formatted Disposition Submission request in accordance with the latest EBTS version.

The EBTS TOT that supports the Disposition Submission response is DSPR.

NGI shall provide a response to a Disposition Submission request received via NCIC in accordance with the latest III/NFF Operations and Technical Manual.

The III messages that support the III DSP for the NCIC Disposition Submission responses are III Accept and III Reject Messages.

NGI shall provide a response to an MRD formatted Disposition Submission request in accordance with the latest MRD Disposition Manual.

NGI shall provide the appropriate Disposition Submission response to an Authorized FBI Service Provider.

3.6.12 Disposition Maintenance Request

The Disposition Maintenance service allows an Authorized Contributor to submit disposition maintenance requests to the NGI. This functionality includes the electronic update and deletion of disposition data.

3.6.12.1 Disposition Maintenance Request Inputs

NGI shall accept Disposition Maintenance requests from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Disposition Maintenance request is DSPE.

NGI shall accept Disposition Maintenance requests from an Authorized Contributor in accordance with the latest III/NFF Operations and Technical Manual.

The NGI STOT that supports the NCIC MKE for Disposition Maintenance request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a designation of file maintenance type (e.g., add, modify, delete) as part of a Disposition Maintenance request.

NCIC and EBTS Disposition Maintenance requests may contain Disposition Maintenance indicators of Add, Append, Replace or Delete.

MRD Disposition Maintenance requests will contain Disposition Submission Type indicators of "Blank" for first time submission or "R" for revision.

NGI shall require primary identifiers as part of a Disposition Maintenance request.

NCIC Disposition Maintenance requests will contain a UCN or SID as the primary identifier. UCN will take precedence and the SID will be ignored when both UCN and SID are provided.

EBTS Disposition Maintenance requests will contain one or more primary identifiers. Primary identifiers for EBTS Disposition Submission requests may include: UCN, SID, Social Security Number, and Miscellaneous Number.

NGI shall require secondary identifiers as part of a Disposition Maintenance request.

Secondary identifiers for NCIC Disposition Maintenance requests must include: Controlling Agency Identifier, Disposition Maintenance Indicator, Date of Arrest, Date of Arrest - Suffix, Identification for Firearms Sales, and Disposition Set which includes the Court Count, Court Offense Numeric, Court Offense Literal, and the Court Provisional Literal and must be submitted in the sequence listed.

Secondary identifiers for EBTS Disposition Maintenance requests may include: Place of Birth, Sex, Race, Height, Weight, Eye Color, Hair Color, State Arrest Number, and Court Case Number. EBTS Disposition Submission requests must contain two or more secondary identifiers. All Disposition Maintenance requests must contain associated court &/or custody information (CON/COL/CPL).

Deleted.

Deleted.

3.6.12.2 Disposition Maintenance Request Processing

NGI shall determine the Identity associated with the Disposition Maintenance request.

NCIC Disposition Maintenance requests determine the Identity using primary and secondary identifiers.

EBTS Disposition Maintenance requests use biographic validation, in addition to primary and secondary identifiers to determine the Identity.

NGI shall reject Disposition Maintenance requests when the supplied primary identifier does not exist.

NGI shall reject a Disposition Maintenance request when the specified primary identifier is invalid.

NGI shall reject a Disposition Maintenance request when the specified DOA is invalid.

NGI shall provide conflict resolution when an associated unique Identity can not be determined for a Disposition Maintenance request.

NGI shall perform the designated maintenance action on the Identity and event that matches the DOA and ORI submitted in a Disposition Maintenance request.

NGI shall provide conflict resolution for Disposition Maintenance requests that cannot be processed automatically.

3.6.12.3 Disposition Maintenance Request Outputs

NGI shall provide a response to an EBTS formatted Disposition Maintenance request in accordance with the latest EBTS version.

The EBTS TOT that supports the Disposition Maintenance response is DSPR.

NGI shall provide a response to a Disposition Maintenance request received via NCIC in accordance with the III/NFF Operations and Technical Manual.

The III messages that support the III DSP for the NCIC Disposition Submission responses are III Accept and III Reject Messages.

3.6.13 Expungement Submission Request

The Expungement Submission request removes identity history data for a specified arrest event, specific charges within an arrest event or an entire identity history record. If the last arrest event on a criminal-only record is expunged, then the entire record will be expunged. Expungement Submission requests may be hardcopy by mail, electronic, or machine readable data (MRD) media.

3.6.13.1 Expungement Submission Request Inputs

NGI shall accept electronic Expungement Submission requests from Authorized Contributors in accordance with the III Operation and Technical Manual.

The NGI STOT that supports the NCIC MKE for the Expungement Submission request is DRS.

NGI shall accept Expungement Submission requests from Authorized Contributors in accordance with the MRD Expungement Manual.

The NGI STOT that supports the MRD Expungement Submission requests is EXPM.

NGI shall allow an Authorized FBI Service Provider to submit an Expungement Submission request.

The NGI STOTs that support the Authorized FBI Service Provider submitted Expungement Submission request are EXPD and PEXD.

NGI shall require primary identifiers as part of an Expungement Submission request.

NCIC Expungement Submission request will contain a UCN as the primary identifier.

EBTS, MRD and Authorized FBI Service Provider Expungement Submission requests will contain two primary identifiers; Primary identifiers for EBTS Submission requests are UCN and Date of Arrest.

3.6.13.2 Expungement Submission Request Processing

NGI shall delete the arrest event data and appropriate Identity information associated with the primary identifiers provided in the Expungement Submission request.

NCIC Expungement Submission requests from Non-NFF III Participants will temporarily delete the arrest event data and appropriate Identity information associated with the State Identification Number (SID). When the Expungement Submission request is processed, the NGI will set a segment code to indicate Pending Expungement and make the arrest event data inactive. If within 30 days supporting documentation of the expungement is received from the requesting state, the deletion of all arrest event data and related Identity Information associated with the SID will occur. If supporting documentation of

the expungement is not received within the 30 day timeframe, the segment code will revert to the value it held prior to receiving the Expungement Submission request, all arrest event data associated with the SID will become reactivated, and the state pointer will become pseudo.

NCIC Expungement Submission requests from NFF III Participants will temporarily delete the arrest event data and appropriate Identity information associated with the SID. The NFF III Participant is allotted 1 hour to reverse the DRS with a MRS. After 1 hour all arrest event data and related Identity Information associated with the SID will be deleted.

MRD Expungement Submission requests will delete the arrest event data and appropriate Identity information associated with the specified UCN and DOA.

Authorized FBI Service Provider Expungement Submission requests will delete the arrest event specified by UCN and DOA. In the case of a Partial Expungement, only specified arrest data within the arrest event will be deleted.

NGI shall delete the entire Identity when the last arrest event is expunged from a criminal-only Identity as part of an Expungement Submission request.

NGI shall reject an Expungement Submission request when the specified UCN is invalid.

NGI shall reject an Expungement Submission request when the specified DOA is invalid.

3.6.13.3 Expungement Submission Request Outputs

NGI shall provide an MRD response to an Expungement Submission request in accordance with the MRD Expungement Manual.

NGI shall provide an electronic response to an Expungement Submission request in accordance with the III/NFF Operational and Technical Manual.

The III messages that support the III DRS for the NCIC Expungement Submission responses are III Accept and III Reject Messages.

NGI shall provide a hardcopy of criminal history information in response to an Expungement Submission request, if appropriate.

NGI shall provide the appropriate Expungement Submission response to an Authorized FBI Service Provider.

3.6.14 Civil Deletion Request

The Civil Deletion request removes civil data for a specified civil event. If the last civil event on a civil-only record is deleted, then the entire record will be deleted. Civil Deletion requests may be hardcopy by mail, or electronic via CJIS WAN.

3.6.14.1 Civil Deletion Request Inputs

NGI shall accept electronic Civil Deletion requests from Authorized Contributors in accordance with the latest EBTS version.

The EBTS TOT that supports the Civil Deletion request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Civil Deletion request.

The NGI STOT that supports the Authorized FBI Service Provider submitted Civil Deletion request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a UCN and Date of Event as part of a Civil Deletion request.

3.6.14.2 Civil Deletion Request Processing

NGI shall delete the civil event data and appropriate Identity information associated with the UCN and Date of Event provided in the Civil Deletion request.

NGI shall delete the entire Identity when the last civil event is deleted from a civil-only Identity as part of a Civil Deletion request.

NGI shall reject a Civil Deletion request when the specified UCN is invalid.

NGI shall reject a Civil Deletion request when the specified Date of Event is invalid.

3.6.14.3 Civil Deletion Request Outputs

NGI shall provide a response to a Civil Deletion request in accordance with the latest EBTS version.

The EBTS TOT that supports the Civil Deletion response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide a hardcopy of Identity history information in response to a Civil Deletion request, if appropriate.

NGI shall provide the appropriate Civil Deletion response to an Authorized FBI Service Provider.

3.6.15 Criminal Record Sealing Request

Criminal Record Sealing request allows an Authorized Contributor to restrict the access of the criminal history information associated with arrests that they own. The FBI will limit dissemination of criminal history data related to a sealed criminal arrest record. The III EHN MKE allows an NFF Authorized Contributor to "seal" the pointer to a specified state controlled record. An Authorized FBI Service Provider can "seal" individual arrest records on behalf of an Authorized Contributor.

3.6.15.1 Criminal Record Sealing Request Inputs

NGI shall accept electronic Criminal Record Sealing requests from Authorized Contributors in accordance with the III Operation and Technical Manual.

The NGI STOT that supports the III Message Key (MKE) for a Criminal Record Sealing request is EHN.

NGI shall allow an Authorized FBI Service Provider to submit a Criminal Record Sealing request.

The NGI STOT that supports the Authorized FBI Service Provider submitted Criminal Record Sealing request is RSD.

NGI shall require a seal indicator designating whether a specified criminal arrest record should be sealed or un-sealed as part of a Criminal Record Sealing request.

NGI shall require a UCN and arrest record specific information as part of a Criminal Record Sealing request.

3.6.15.2 Criminal Record Sealing Request Processing

NGI shall mark a criminal arrest record and associated criminal history information as sealed when indicated in the Criminal Record Sealing request.

NGI shall mark a criminal arrest record and associated criminal history information as un-sealed when indicated in the Criminal Record Sealing request.

NGI shall reject a Criminal Record Sealing request when the specified UCN is invalid.

NGI shall reject a Criminal Record Sealing request when the specified arrest record information is invalid.

3.6.15.3 Criminal Record Sealing Request Outputs

NGI shall provide an electronic response to a Criminal Record Sealing request in accordance with the III/NFF Operational and Technical Manual.

The NGI STOT that supports the III MKE for a Criminal Record Sealing response will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall provide the appropriate Criminal Record Sealing response to an Authorized FBI Service Provider.

3.6.16 Identity Consolidation Request

An Identity Consolidation request will be initiated when multiple Identity History Records are found to exist for the same individual. An Authorized FBI Service Provider will review the fingerprint images and determine if the records should be consolidated. The Identity Consolidation request causes the

information in the multiple records to be merged and the information associated with the secondary records to be deleted. As a result of the consolidation, a notification will be sent to the agency that submitted the fingerprints; any agencies that have submitted fingerprints pertinent to any of the records in the last year; and all state ID bureaus that have submitted fingerprints or records at any time on the consolidated subject.

3.6.16.1 Identity Consolidation Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit an Identity Consolidation request.

The NGI STOT that supports the Authorized FBI Service Provider submitted Identity Consolidation request is COND.

NGI shall accept an automated Identity Consolidation request when a Identification Search results in multiple positive identification decisions.

These are automated Identity Consolidation requests initiated as part of an Identification service request.

NGI shall require at least two UCNs as part of an Identity Consolidation request.

3.6.16.2 Identity Consolidation Request Processing

NGI shall determine "kept UCN" and "killed UCN(s)" from the UCNs provided as part of an automated Identity Consolidation request based on consolidation rules.

Deleted.

NGI shall perform Automated Consolidation of the Identity history information associated with the "killed UCN(s)" into the "kept UCN" provided as part of the Identity Consolidation request.

NGI shall allow an Authorized FBI Service Provider to perform Manual Consolidation when Automated Consolidation cannot be successfully completed as part of the Identity Consolidation request.

The Authorized FBI Service Provider will determine the "kept UCN" and "killed UCN," conduct research and perform the appropriate Identity maintenance to prepare the records for consolidation. An Identity Consolidation request will then be submitted to NGI by the Service Provider.

NGI shall send a Link Maintenance request to the appropriate External System for each Identity containing an external link as part of a consolidation of multiple Identities.

NGI shall include the "kept UCN," "killed UCN(s)," and External System Identifier(s) as part of the Consolidation Link Maintenance request.

NGI shall send a Link Maintenance request indicating consolidation to an External System in accordance with the latest EBTS version.

NGI shall accept a Consolidation Link Maintenance response from an External System in accordance with the latest EBTS version.

NGI shall perform exception processing when a Consolidation Link Maintenance request is rejected by an External System.

Exception processing may include notifying an Authorized FBI Service Provider or a System Administrator of the reject.

The following functional requirements are specific to data maintenance for the consolidation of Identities.

Deleted.

NGI shall re-associate the biographic information associated with the killed Identity(ies) to the kept Identity as part of an Identity Consolidation request.

NGI shall re-associate the biometric information associated with the killed Identity(ies) to the kept Identity as part of an Identity Consolidation request.

NGI shall re-associate the event information associated with the killed Identity(ies) to the kept Identity as part of an Identity Consolidation request.

NGI shall update the biographic compilation for the kept Identity, if applicable, as part of an Identity Consolidation request.

NGI shall update the biometric composite(s) for the kept Identity, if applicable, as part of an Identity Consolidation request.

NGI shall re-associate the Event certification copy(ies) associated with the killed Identity(ies) to the kept Identity as part of an Identity Consolidation request.

NGI shall reject an Identity Consolidation request, submitted by an Authorized FBI Service Provider, when the fingerprints for the UCNs are determined to not be the same individual.

NGI shall reject an Identity Consolidation request when record types for the submitted UCNs are not compatible.

3.6.16.3 Identity Consolidation Request Outputs

NGI shall provide the appropriate Identity Consolidation response to an Authorized FBI Service Provider.

Identity Consolidation requests result in unsolicited notifications to the appropriate Authorized Contributors. Tenprint Fingerprint Identification requests that trigger a Consolidation request will resume normal processing after consolidation activities are completed. Refer to the *Notification Services Functional Requirements* section for more information.

NGI shall provide a hardcopy Identity History Summary to each contributor that provided or received identity history information for the kept UCN during the last 12-month time period.

NGI will use the Computerized Records Sent file, along with information contained in the Identity History for the Kept Identity, to determine which agencies should receive a new Identity History Summary for that Identity.

3.6.17 Death Notice Request

Notification of the death of a subject is received via NCIC. These requests do not contain fingerprints. The NGI Identity is updated with the reported Death Notice information including date of death and reporting agency.

3.6.17.1 Death Notice Request Inputs

NGI shall accept a Death Notice request in accordance with the III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE for the Death Notice request is DEC.

NGI shall require a UCN in a Death Notice request.

3.6.17.2 Death Notice Request Processing

NGI shall update the specified UCN with information provided in a Death Notice request.

NGI shall reject a Death Notice request when the specified UCN is invalid.

3.6.17.3 Death Notice Request Outputs

NGI shall provide a response to a Death Notice request in accordance with the III/NFF Operational and Technical Manual.

The NGI STOT that supports the NCIC MKE for the Death Notice response will be developed in accordance with the NGI Message Definition Database (MDD).

3.6.18 Want Maintenance Request

Electronic Want Maintenance requests are received from NCIC when wanted person information is added, modified, or deleted within the NCIC wanted person file, and there is a UCN associated with the record. If NGI cannot process the electronic Want Maintenance request, a reject message is printed for an Authorized FBI Service Provider to review. Additionally, Authorized FBI Service Providers have the capability to manually submit Want Maintenance requests.

3.6.18.1 Want Maintenance Request Inputs

NGI shall accept Want Maintenance requests from NCIC in accordance with the latest NCIC Operating Manual.

The NGI STOT that supports the NCIC MKE for the Want Maintenance request is WPT.

NGI shall allow an Authorized FBI Service Provider to submit a Want Maintenance request.

The NGI STOT that supports the Authorized FBI Service Provider submitted Want Maintenance request is WPTD.

NGI shall require a UCN and biographical data as part of a Want Maintenance request.

NGI shall require a designation of file maintenance type (e.g., add, modify, delete) as part of a Want Maintenance request.

3.6.18.2 Want Maintenance Request Processing

NGI shall perform biographic validation using UCN and biographic data to validate the subject associated with the Want Maintenance request.

NGI shall update the Identity History record for the associated UCN using the designated file maintenance type and other data contained in the Want Maintenance request.

NGI shall reject a Want Maintenance request when the specified UCN is invalid.

NGI shall reject a Want Maintenance request when the biographic validation fails.

3.6.18.3 Want Maintenance Request Outputs

NGI does not provide any response when a Want Maintenance request completes successfully.

NGI shall create a hardcopy reject in response to a Want Maintenance request, when appropriate.

NGI shall provide the appropriate Want Maintenance response to an Authorized FBI Service Provider.

If appropriate, NGI will also send unsolicited notifications to Authorized Contributors. Refer to the *Notification Services Functional Requirements* section for more information.

3.6.19 Flash Submission Request

Flashes may be placed on records for a subject whose activities are limited by court issued restrictions, supervision, protection orders, or deportation decrees.

3.6.19.1 Flash Submission Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit a Flash Submission request.

The NGI STOT that supports the Authorized FBI Service Provider Flash Submission request is FLASH.

NGI shall require a UCN and Date of Arrest (DOA) as part of a Flash Submission request.

3.6.19.2 Flash Submission Request Processing

NGI shall update the Identity History record for the associated UCN and DOA using the information contained in the Flash Submission request.

NGI shall reject a Flash Submission request when the specified UCN is invalid.

NGI shall reject a Flash Submission request when the specified DOA is invalid.

3.6.19.3 Flash Submission Request Outputs

NGI shall provide the appropriate Flash Submission response to an Authorized FBI Service Provider.

NGI shall create a hardcopy response to a Flash Submission request, if appropriate.

If appropriate, NGI will also send unsolicited notifications to Authorized Contributors. Refer to the *Notification Services Functional Requirements* section for more information.

3.6.20 Sexual Offender Registry (SOR) Maintenance Request

Electronic SOR Maintenance requests are received from NCIC when sexual offender information is added, modified, or deleted within the NCIC sexual offender file, and there is a UCN associated with the record. If NGI cannot process the electronic SOR Maintenance request, a reject message is printed for an Authorized FBI Service Provider to review.

3.6.20.1 SOR Maintenance Request Inputs

NGI shall accept SOR Maintenance requests from NCIC in accordance with the latest NCIC Operating Manual.

The NGI STOT that supports the NCIC MKE for an SOR Maintenance request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a UCN and biographical data as part of an SOR Maintenance request.

NGI shall require a designation of file maintenance type (e.g., add, modify, delete) as part of an SOR Maintenance request.

3.6.20.2 SOR Maintenance Request Processing

NGI shall perform biographic validation using UCN and biographic data to validate the subject associated with the SOR Maintenance request.

NGI shall reject an SOR Maintenance request when the biographic validation fails.

NGI shall update the Identity History record for the associated UCN using the designated file maintenance type and other data contained in the SOR Maintenance request.

In the SOR Maintenance request, other data may include the registering agency, the date of registration, and the expiration of the registry.

NGI shall reject an SOR Maintenance request when the specified UCN is invalid.

3.6.20.3 SOR Maintenance Request Outputs

NGI shall create a hardcopy reject in response to an SOR Maintenance request, when appropriate.

If appropriate, NGI will also send unsolicited notifications to Authorized Contributors. Refer to the *Notification Services Functional Requirements* section for more information.

3.6.21 Computerized Contributor Address (CCA) File Maintenance Request

3.6.21.1 Computerized Contributor Address File Maintenance Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit a CCA File Maintenance request.

The NGI STOT that supports the CCA File Maintenance is CCAD.

NGI shall accept the designation to add a Contributor Address record as part of a CCA File Maintenance request.

NGI shall accept the designation to deactivate (retire) a Contributor Address record in the CCA File as part of a CCA File Maintenance request.

The association of deactivated Contributor entries to another active Contributor entry allows changes in contributor identifiers (ORIs) due to policy, business rules, and programmatic changes.

NGI shall accept a designation to modify a Contributor Address record as part of a CCA File Maintenance request.

3.6.21.2 Computerized Contributor Address File Maintenance Request Processing

NGI shall create a record in the CCA File based on Contributor Address data provided as part of an add contributor CCA File Maintenance request.

NGI shall mark a Contributor's Address record as deactivated based on information provided by an Authorized FBI Service Provider as part of a deactivate contributor CCA File Maintenance request.

NGI shall associate a Contributor's Address record that is marked as deactivated to another active Contributor's Address record when requested as part of a deactivate contributor CCA File Maintenance request.

There will be instances where a Contributor's agency or organizational structure changes requiring the consolidation of points of contact with the FBI. The deactivated points of contact (contributor address)

will need to be associated with the new or other existing Contributor Address information to facilitate inquiries and reporting of past events.

NGI shall perform the modification on the specified Contributor Address record data as part of the CCA File Maintenance request.

3.6.21.3 Computerized Contributor Address File Maintenance Request Outputs

NGI shall provide the appropriate CCA File Maintenance response to an Authorized FBI Service Provider.

3.6.22 Restore Identity History Request

3.6.22.1 Restore Identity History Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit a Restore Identity History request.

The NGI STOT that supports the Restore Identity History Information request is RFND.

NGI shall require a UCN as part of a Restore Identity History request.

3.6.22.2 Restore Identity History Request Processing

NGI shall restore the Identity History information of the subject contained in a Restore Identity History request within a specified period of time following a record expungement action.

NGI shall restore the Identity History information of the subject contained in a Restore Identity History request within a specified period of time following a record consolidation action.

The restore can be done within 30 days or until a subsequent file maintenance has occurred on the kept record.

NGI shall restore the Identity History information of the subject contained in a Restore Identity History request within a specified period of time following a Identity History record deletion action.

NGI shall reject a Restore Identity History request when the specified UCN is invalid.

3.6.22.3 Restore Identity History Request Outputs

NGI shall provide the appropriate Restore Identity History response to an Authorized FBI Service Provider.

NGI may also send unsolicited notifications to Authorized Contributors (e.g., III/NFF record owners, latent owners). Refer to the *Notification Services Functional Requirements* section for more information.

3.6.23 Statute Retrieval Requests

The purpose of the NGI Statute Retrieval request is to allow an Authorized FBI Service Provider to retrieve statutes for viewing or printing.

3.6.23.1 Statute Retrieval Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit Statute Retrieval requests.

3.6.23.2 Statute Retrieval Request Processing

NGI shall retrieve the statute(s) indicated in a Statute Retrieval request.

3.6.23.3 Statute Retrieval Request Outputs

NGI shall provide the capability for an Authorized FBI Service Provider to view the statute(s) returned from a Statute Retrieval request.

NGI shall provide the capability for an Authorized FBI Service Provider to print the statute(s) returned from a Statute Retrieval request.

3.6.24 Statute Maintenance Request

The purpose of the NGI Statute Maintenance Service is for an Authorized FBI Service Provider to perform statute maintenance. Once the necessary information is received to initiate a statute maintenance action, an Authorized FBI Service Provider can add, modify, or delete a statute and NGI will maintain a statute maintenance audit trail for each transaction.

3.6.24.1 Statute Maintenance Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit Statute Maintenance requests.

NGI shall require a designation of file maintenance type (e.g., add, modify, delete) as part of a Statute Maintenance request.

3.6.24.2 Statute Maintenance Request Processing

NGI shall perform the appropriate file maintenance for the statute as indicated in the Statute Maintenance request.

3.6.24.3 Statute Maintenance Request Outputs

NGI shall provide the appropriate response to an Authorized FBI Service Provider for a Statute Maintenance request.

3.6.25 Unsolved Latent Add Confirm Request

This request is used to confirm temporarily added unsolved latent file records.

3.6.25.1 Unsolved Latent Add Confirm Inputs

NGI shall accept Unsolved Latent Add Confirm Requests from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Unsolved Latent File Add Confirm request is ULAC.

NGI shall allow an Authorized FBI Service Provider to submit an Unsolved Latent Add Confirm request.

The NGI STOT that supports the Unsolved Latent File Add Confirm request is IULAC.

NGI shall require an AFIS segment process control number (SCNA) as part of an Unsolved Latent Add Confirm request.

NGI shall accept a Latent Case Number (LCN) and Latent Case Extension Number (LCX) as part of an Unsolved Latent Add Confirm request.

3.6.25.2 Unsolved Latent Add Confirm Processing

NGI shall mark the appropriate ULF image record as permanent in the ULF repository as part of an Unsolved Latent Add Confirm request.

NGI shall mark the appropriate ULF feature record as permanent in the ULF repository as part of an Unsolved Latent Add Confirm request.

3.6.25.3 Unsolved Latent Add Confirm Outputs

NGI shall provide an appropriate response to the Unsolved Latent Add Confirm Request in accordance with the latest EBTS version.

NGI shall provide the appropriate Unsolved Latent Add Confirm Request response to an Authorized FBI Service Provider.

3.6.26 Computerized Records Sent File Maintenance Request

The Computerized Records Sent file (CRS), maintained by III, may contain records of those agencies that receive copies of responses and records of modification actions by an Authorized FBI Service Provider. The Receiving Agency Notification Report is a report that is generated with input from the CRS file.

3.6.26.1 Computerized Records Sent File Maintenance Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit a Computerized Records Sent File Maintenance Request.

The internal STOT that supports the Computerized Records Sent File Maintenance Request is CRSD.

NGI shall require a UCN as part of a Computerized Records Sent File Maintenance Request.

NGI shall accept a designation of maintenance action as part of a Computerized Records Sent File Maintenance Request.

3.6.26.2 Computerized Records Sent File Maintenance Request Processing

Deleted.

NGI shall perform the designated maintenance action as part of a Computerized Records Sent File Maintenance Request.

NGI shall reject the Computerized Records Sent File Maintenance Request when the maintenance action is unsuccessful.

3.6.26.3 Computerized Records Sent File Maintenance Request Outputs

NGI shall provide the appropriate Computerized Records Sent File Maintenance Request response to an Authorized FBI Service Provider.

3.6.27 Conflict Resolution Service Request

The purpose of the Conflict Resolution Services is to allow Authorized FBI Service Providers to process Disposition Fingerprint Requests, Disposition Submission requests or Disposition Maintenance requests that can not be automatically processed by NGI.

3.6.27.1 Conflict Resolution Inputs

NGI shall provide a Conflict Resolution service to allow an Authorized FBI Service Provider to resolve discrepancies in disposition processing.

3.6.27.2 Conflict Resolution Processing

NGI shall provide, as part of Conflict Resolution service, the capability to defer Disposition Submission requests when disposition data cannot be applied.

NGI shall advise an Authorized FBI Service Provider when criminal activity occurs on an Identity containing disposition data with an associated default arrest cycle.

NGI shall provide, as part of Conflict Resolution service, the capability to add submitted disposition data with a default arrest cycle to the subject identified from a disposition fingerprint search.

NGI shall provide, as part of Conflict Resolution service, the capability to add disposition data to an Identity.

NGI shall provide, as part of Conflict Resolution service, the capability to reject Disposition Submission requests.

3.6.27.3 Conflict Resolution Outputs

NGI shall provide the appropriate Conflict Resolution response to an Authorized FBI Service Provider.

3.6.28 Direct Fingerprint Enrollment Request

3.6.28.1 Direct Fingerprint Enrollment Inputs

NGI shall accept a Direct Fingerprint Enrollment request from an Authorized Contributor in accordance with the latest EBTS version.

NGI shall accept Direct Fingerprint Enrollment requests in bulk via multiple methods (e.g., ftp, CD, DVD).

The EBTS TOT that supports the Direct Fingerprint Enrollment request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Direct Fingerprint Enrollment request.

The NGI STOT that supports the Direct Fingerprint Enrollment request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require an SPC File designation as part of a Direct Fingerprint Enrollment request.

NGI shall accept Direct Fingerprint Enrollment requests with ten or fewer flat fingerprints.

NGI shall accept Direct Fingerprint Enrollment requests with ten or fewer rolled fingerprints.

NGI shall accept a UCN as part of a Direct Fingerprint Enrollment request.

The UCN will be used to add additional fingerprints to an existing Identity in the specified SPC File.

3.6.28.2 Direct Fingerprint Enrollment Processing

NGI shall enroll the fingerprint data into the designated SPC File as a result of a Direct Fingerprint Enrollment request.

NGI shall reject a Direct Fingerprint Enrollment request when the submitted fingerprints fail to meet minimum quality standards.

NGI shall reject a Direct Fingerprint Enrollment request to an SPC File when the Authorized Contributor does not have write access to the SPC File.

NGI shall reject a Direct Fingerprint Enrollment request to an SPC File when an Authorized FBI Service Provider does not have write access to the SPC File.

NGI shall reject a Direct Fingerprint Enrollment request when the designated SPC File does not exist.

3.6.28.3 Direct Fingerprint Enrollment Outputs

NGI shall provide a response to an Authorized Contributor for a Direct Fingerprint Enrollment request in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Fingerprint Enrollment response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate Direct Fingerprint Enrollment response to an Authorized FBI Service Provider.

NGI shall provide a collective response for Direct Fingerprint Enrollment requests when submitted in bulk.

NGI collective responses will include individual enrollment responses/status provided as part of single collective response to the user.

3.6.29 Direct Latent Enrollment Request

3.6.29.1 Direct Latent Enrollment Inputs

NGI shall accept a Direct Latent Enrollment request for an SPC File from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Latent Enrollment request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Direct Latent Enrollment request for an SPC File.

The NGI STOT that supports the Direct Latent Enrollment request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall accept Direct Latent Enrollment requests for an SPC File in bulk via multiple methods (e.g., ftp, CD, DVD).

3.6.29.2 Direct Latent Enrollments Processing

NGI shall enroll the latent information into the designated SPC File as a result of a Direct Latent Enrollment request.

NGI shall reject a Direct Latent Enrollment request when the Authorized Contributor is not permitted access to the requested SPC File.

NGI shall reject a Direct Latent Enrollment request when the FBI Service Provider is not permitted access to the requested SPC File.

3.6.29.3 Direct Latent Enrollment into Outputs

NGI shall provide a Direct Latent Enrollment response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Latent Enrollment response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate Direct Latent Enrollment response to an Authorized FBI Service Provider.

NGI shall provide a collective response for Direct Latent Enrollment requests when submitted in bulk.

NGI collective responses will include individual enrollment responses/status provided as part of single collective response to the user.

3.6.30 Unsolved Latent File Delete Request

The Unsolved Latent File Delete request provides the capability for a ULF record owner to delete a latent print from the ULF.

3.6.30.1 Unsolved Latent File Delete Request Inputs

NGI shall accept Unsolved Latent File Delete requests from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Unsolved Latent File Delete requests is ULD.

NGI shall allow an Authorized FBI Service Provider to submit an Unsolved Latent File Delete request.

The NGI STOT that supports the Unsolved Latent File Delete request is IULD.

NGI shall require a UCN as part of an Unsolved Latent File Delete request.

3.6.30.2 Unsolved Latent File Delete Request Processing

NGI shall reject an Unsolved Latent File Delete request when the specified UCN does not exist.

NGI shall delete the latent data from the ULF associated with the UCN specified in the Unsolved Latent File Delete request.

3.6.30.3 Unsolved Latent File Delete Request Outputs

NGI shall provide a response to an Authorized Contributor for an Unsolved Latent File Delete request in accordance with the latest EBTS version.

The EBTS TOT that supports the Unsolved Latent File Delete response is ULDR.

NGI shall provide the appropriate Unsolved Latent File Delete response to an Authorized FBI Service Provider.

3.6.31 Latent Decision Request

Authorized Contributors and FBI Service Providers can return positive, negative, or inconclusive decisions for candidates provided to them as a result of a latent investigation search request or unsolved biometric notification. These decisions are used internally for statistical and algorithm analysis. Additionally, a positive decision returned from an unsolved latent owner can result in automatic deletion of the unsolved latent.

3.6.31.1 Latent Decision Inputs

NGI shall accept a Latent Decision from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Latent Decision will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Latent Decision.

The NGI STOT that supports the Latent Decision will be developed in accordance with the NGI Message Definition Database (MDD).

3.6.31.2 Latent Decision Processing

NGI shall record the Latent Decision.

NGI shall send a positive Latent Decision to an External System in accordance with the latest EBTS version on a candidate from that External System, when appropriate.

NGI shall delete the referenced latent prints from the ULF if a positive latent decision is received from the ULF Fingerprint Owner.

3.6.31.3 Latent Decision Outputs

NGI shall provide a reject response, as appropriate, for a Latent Decision.

NGI shall provide a response to a Latent Decision from an Authorized Contributor in accordance with the latest EBTS version.

3.6.32 Special Population Cognizant File Maintenance Request

The Special Population Cognizant File Maintenance request provides the capability for an Authorized FBI Service Provider (e.g., FBI Latent Examiner) to maintain (create/populate/delete) a Special Population Cognizant File.

3.6.32.1 Special Population Cognizant Maintenance Request Inputs

NGI shall allow an Authorized FBI Service Provider to submit an SPC File Maintenance request.

The NGI STOT that supports the Special Population Cognizant File Maintenance requests is SPCM.

NGI shall require an SPC identifier as part of a Special Population Cognizant File Maintenance request.

NGI shall require a designation of maintenance action as part of a Special Population Cognizant File Maintenance request.

Maintenance actions may include creation, deletion, modification, or copying of data to an SPC file.

NGI shall accept an SPC File creation maintenance action as part of a Special Population Cognizant File Maintenance request.

NGI shall accept an SPC File deletion maintenance action as part of a Special Population Cognizant File Maintenance request.

NGI shall provide the capability to mark an SPC File for cascaded searching as part of a Special Population Cognizant File Maintenance request.

NGI shall provide the capability to unmark an SPC File for cascaded searching as part of a Special Population Cognizant File Maintenance request.

NGI shall provide the capability to designate the primary owner of an SPC File as part of a Special Population Cognizant File Maintenance request.

NGI shall provide the capability to designate secondary user(s) access of an SPC File as part of a Special Population Cognizant File Maintenance request.

NGI shall provide the capability to copy Identity information from other NGI repositories into an SPC file as part of a Special Population Cognizant File Maintenance request.

3.6.32.2 Special Population Cognizant File Maintenance Request Processing

NGI shall perform the designated maintenance action on the specified SPC File as part of the Special Population Cognizant File Maintenance request.

NGI shall reject the Special Population Cognizant File Maintenance request when specified SPC File is invalid.

3.6.32.3 Special Population Cognizant File Maintenance Request Outputs

NGI shall provide the appropriate Special Population Cognizant File Maintenance response to an Authorized FBI Service Provider.

3.6.33 Direct Photo Enrollment Request

3.6.33.1 Direct Photo Enrollment Request Inputs

NGI shall accept a Direct Photo Enrollment request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Photo Enrollment request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Direct Photo Enrollment request.

The NGI STOT that supports the Direct Photo Enrollment request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall accept a multi-level SMT photo descriptor field as part of a Direct Photo Enrollment request.

NGI shall require a designation of the repository(ies) into which photos should be added in a Direct Photo Enrollment request.

NGI shall accept a Direct Photo Enrollment request without a UCN or fingerprints for enrollment into an SPC File.

NGI shall accept a Direct Photo Enrollment request with a UCN and ten or fewer fingerprints.

NGI shall accept a Direct Photo Enrollment request with a UCN and no fingerprints, when an MOU is in place with the Authorized Contributor.

NGI shall accept a Direct Photo Enrollment request with a UCN and event specific information.

NGI shall accept Direct Photo Enrollment requests in bulk via multiple methods (e.g., ftp, CD, DVD).

3.6.33.2 Direct Photo Enrollment Request Processing

NGI shall enroll the photo(s) in the designated repository(ies) as a result of a Direct Photo Enrollment request.

NGI shall provide the capability to uniquely identify photos enrolled as a result of a Direct Photo Enrollment request.

NGI shall reject a Direct Photo Enrollment request when the specified UCN or event does not exist.

NGI shall reject a Direct Photo Enrollment request when the specified UCN cannot be validated using the submitted fingerprints.

NGI shall reject a Direct Photo Enrollment request without fingerprints when an MOU is not in place for the Authorized Contributor.

NGI shall reject a Direct Photo Enrollment request if no photo repository is specified.

NGI shall perform a cascaded facial recognition search of the UPF if the photo submitted with a Direct Photo Enrollment request meets the minimum quality standard for facial recognition in accordance with cascaded search business rules.

NGI shall perform a cascaded facial recognition search of marked SPC Files if the photo submitted with a Direct Photo Enrollment request meets the minimum quality standard for facial recognition in accordance with cascaded search business rules.

3.6.33.3 Direct Photo Enrollment Request Outputs

NGI shall provide a Direct Photo Enrollment response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Photo Enrollment response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate Direct Photo Enrollment response to an Authorized FBI Service Provider.

NGI shall provide a collective response for Direct Photo Enrollment requests when submitted in bulk.

NGI collective responses will include individual enrollment responses/status provided as part of single collective response to the user.

NGI shall advise the Photo Owner when a photo is enrolled as a result of a Direct Photo Enrollment request, but fails to meet minimum quality standards for facial recognition.

3.6.34 Photo Deletion Request

3.6.34.1 Photo Deletion Request Inputs

NGI shall accept a Photo Deletion request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Photo Delete requests is CPD.

NGI shall allow an Authorized FBI Service Provider to submit a Photo Deletion request.

The NGI STOT that supports the Photo Delete request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require photo specific information as part of a Photo Deletion request.

3.6.34.2 Photo Deletion Request Processing

NGI shall delete the photos specified in the Photo Deletion request.

NGI shall reject a Photo Deletion request if the specified photo does not exist.

3.6.34.3 Photo Deletion Request Outputs

NGI shall provide a Photo Deletion response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Photo Delete response is PDR.

NGI shall provide the appropriate Photo Deletion response to an Authorized FBI Service Provider.

3.6.35 Photo Decision Request

Authorized Contributors and FBI Service Providers can return positive, negative, or inconclusive decisions for candidates provided to them as a result of a facial recognition search request or unsolved biometric notification. These decisions are used internally for statistical and algorithm analysis. Additionally, a positive decision returned from an unsolved photo owner can result in automatic deletion of the unsolved photo.

3.6.35.1 Photo Decision Inputs

NGI shall accept a Photo Decision from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Photo Decision request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Providers to submit a Photo Decision.

The NGI STOT that supports the Photo Decision will be developed in accordance with the NGI Message Definition Database (MDD).

3.6.35.2 Photo Decision Processing

NGI shall record the Photo Decision.

NGI shall delete the referenced photos from the UPF if a positive Photo Decision is received from the UPF Photo Owner.

3.6.35.3 Photo Decision Outputs

NGI shall provide a reject response, as appropriate, for a Photo Decision.

NGI shall provide a response to a Photo Decision from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Photo Decision response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.6.36 Direct Palmprint Enrollment Request

3.6.36.1 Direct Palmprint Enrollment Request Inputs

NGI shall accept a Direct Palmprint Enrollment request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Palmprint Enrollment request is PPE.

NGI shall allow an Authorized FBI Service Provider to submit a Direct Palmprint Enrollment request.

The NGI STOT that supports the Direct Palmprint Enrollment request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a designation of the repository(ies) into which palmprints should be added in a Direct Palmprint Enrollment request.

NGI shall accept a Direct Palmprint Enrollment request without a UCN or fingerprints into the SPC File.

NGI shall accept a Direct Palmprint Enrollment request with a UCN and ten or fewer fingerprints.

NGI shall accept a Direct Palmprint Enrollment request with a UCN and no fingerprints when an MOU is in place with the Authorized Contributor.

NGI shall accept a Direct Palmprint Enrollment request with a UCN and event specific information.

NGI shall accept Direct Palmprint Enrollment requests in bulk via multiple methods (e.g., ftp, CD, DVD).

3.6.36.2 Direct Palmprint Enrollment Request Processing

NGI shall perform a validation to ensure that submitted palmprint images match the submitted fingerprints, when fingerprints and the distal segments of the palmprint images are included as part of the Direct Palmprint Enrollment request.

NGI shall enroll the palmprint(s) in the designated repository(ies) as a result of a Direct Palmprint Enrollment request.

NGI shall provide the capability to uniquely identify palmprints enrolled as a result of a Direct Palmprint Enrollment request.

NGI shall reject a Direct Palmprint Enrollment request when the specified UCN or event does not exist.

NGI shall reject a Direct Palmprint Enrollment request when the specified UCN cannot be validated using the submitted fingerprints.

NGI shall reject a Direct Palmprint Enrollment request without fingerprints when an MOU is not in place for the Authorized Contributor.

NGI shall reject a Direct Palmprint Enrollment request when a designated repository is not specified.

NGI shall perform a cascaded palmprint search of the ULF if the palmprint submitted with a Direct Palmprint Enrollment request meets the minimum quality standard for palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded palmprint search of the marked SPC Files designated for cascaded searches, if the palmprint submitted with a Direct Palmprint Enrollment request meets the minimum quality standard for palmprints in accordance with cascaded search business rules.

3.6.36.3 Direct Palmprint Enrollment Request Outputs

NGI shall provide a Direct Palmprint Enrollment response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Palmprint Enrollment response is PPR.

NGI shall provide the appropriate Direct Palmprint Enrollment response to an Authorized FBI Service Provider.

NGI shall provide a collective response for Direct Palmprint Enrollment requests when submitted in bulk.

NGI collective responses will include individual enrollment responses/status provided as part of single collective response to the user.

NGI shall advise the Palmprint Owner when a palmprint is enrolled as a result of a Direct Palmprint Enrollment request but fails to meet minimum quality standards for palmprints.

3.6.37 Palmprint Deletion Request

3.6.37.1 Palmprint Deletion Request Inputs

NGI shall accept a Palmprint Deletion request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Palmprint Deletion request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Palmprint Deletion request.

The NGI STOT that supports the Palmprint Deletion request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require palmprint specific information as part of a Palmprint Deletion request.

3.6.37.2 Palmprint Deletion Request Processing

NGI shall delete the palmprints specified in the Palmprint Deletion request.

NGI shall reject a Palmprint Deletion request if the specified palmprint does not exist.

3.6.37.3 Palmprint Deletion Request Outputs

NGI shall provide a Palmprint Deletion response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Palmprint Deletion response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate Palmprint Deletion response to an Authorized FBI Service Provider.

3.6.38 Deleted

3.6.38.1 Deleted

Deleted.

Deleted.

3.6.38.2 Deleted

Deleted.

Deleted.

3.6.38.3 Deleted

Deleted.

Deleted.

3.6.39 Direct Supplemental Fingerprint and Palmprint Enrollment Request

The Supplemental Fingerprint and Palmprints request provides for the submission of Tenprint fingerprints, plus additional images of the extreme tips, sides, and lower joints of the fingers, and surface and extreme sides of palms for possible use in comparisons for a case. In addition, the submitted Supplemental Fingerprints and Palmprints may be searched against the NGI logical repositories, and providing that all required data is submitted, may be used to establish a new record or to update existing records for an Identity. A Major Case Print set is logically created when fingerprints, palmprints and supplemental fingerprint and palmprints exist for an Identity.

3.6.39.1 Direct Supplemental Fingerprint and Palmprint Enrollment Request Inputs

NGI shall accept a Direct Supplemental Fingerprint and Palmprint Enrollment request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Supplemental Fingerprint and Palmprint Enrollment request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Direct Supplemental Fingerprint and Palmprint Enrollment request.

The NGI STOT that supports the Direct Supplemental Fingerprint and Palmprint Enrollment request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a designation of the repository(ies) into which supplemental fingerprint and palmprints should be added in a Direct Supplemental Fingerprint and Palmprint Enrollment request.

NGI shall accept a Direct Supplemental Fingerprint and Palmprint Enrollment request without a UCN or fingerprints into the SPC File.

NGI shall accept a Direct Supplemental Fingerprint and Palmprint Enrollment request with a UCN and ten or fewer fingerprints.

NGI shall accept a Direct Supplemental Fingerprint and Palmprint Enrollment request with a UCN and no fingerprints when an MOU is in place with the Authorized Contributor.

NGI shall accept a Direct Supplemental Fingerprint and Palmprint Enrollment request with a UCN and event specific information.

NGI shall accept Direct Supplemental Fingerprint and Palmprint Enrollment requests in bulk via multiple methods (e.g., ftp, CD, DVD).

3.6.39.2 Direct Supplemental Fingerprint and Palmprint Enrollment Request Processing

NGI shall perform a validation to ensure that the submitted supplemental fingerprint and palmprint images match the submitted fingerprints, when fingerprints and the distal segments of the supplemental fingerprint and palmprint images are included in the Direct Supplemental Fingerprint and Palmprint Enrollment request.

Supplemental fingerprint and palmprint images will not be enrolled if the validation of the supplemental fingerprint and palmprint images to the submitted fingerprints fails.

NGI shall enroll the Supplemental Fingerprint and Palmprint information in the designated repository(ies) as a result of a Direct Supplemental Fingerprint and Palmprint Enrollment request.

NGI shall provide the capability to uniquely identify supplemental fingerprint and palmprint information enrolled as a result of a Direct Supplemental Fingerprint and Palmprint Enrollment request.

NGI shall reject a Direct Supplemental Fingerprint and Palmprint Enrollment request when the specified UCN or event does not exist.

NGI shall reject a Direct Supplemental Fingerprint and Palmprint Enrollment request when the specified UCN cannot be validated using the submitted fingerprints.

NGI shall reject a Direct Supplemental Fingerprint and Palmprint Enrollment request without fingerprints when an MOU is not in place for the Authorized Contributor.

NGI shall reject a Direct Supplemental Fingerprint and Palmprint Enrollment request when a designated repository is not specified.

NGI shall perform a cascaded search of the ULF if the supplemental fingerprint and palmprint submitted with a Direct Supplemental Fingerprint and Palmprint Enrollment request meets the minimum quality standard for supplemental fingerprint and palmprints in accordance with cascaded search business rules.

NGI shall perform a cascaded search of the marked SPC Files designated for cascaded searches, if the supplemental fingerprint and palmprint submitted with a Direct Supplemental Fingerprint and Palmprint Enrollment request meets the minimum quality standard for supplemental fingerprint and palmprints in accordance with cascaded search business rules.

3.6.39.3 Direct Supplemental Fingerprint and Palmprint Enrollment Request Outputs

NGI shall provide a Direct Supplemental Fingerprint and Palmprint Enrollment response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Supplemental Fingerprint and Palmprint Enrollment response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate Direct Supplemental Fingerprint and Palmprint Enrollment response to an Authorized FBI Service Provider.

NGI shall provide a collective response for Direct Supplemental Fingerprint and Palmprint Enrollment requests when submitted in bulk.

NGI collective responses will include individual enrollment responses/status provided as part of single collective response to the user.

NGI shall advise the Supplemental Fingerprint and Palmprint Owner when a supplemental fingerprint and palmprint is enrolled as a result of a Direct Supplemental Fingerprint and Palmprint Enrollment request, but fails to meet minimum quality standards for supplemental fingerprint and palmprint.

There will be no EBTS normal NGI responses other than communication protocol acknowledgments for this transaction type. If there is an error in the submittal, a reject response will be returned.

3.6.40 Supplemental Fingerprint and Palmprint Deletion Request

3.6.40.1 Supplemental Fingerprint and Palmprint Deletion Request Inputs

NGI shall accept a Supplemental Fingerprint and Palmprint Deletion request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Supplemental Fingerprint and Palmprint Deletion request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Supplemental Fingerprint and Palmprint Deletion request.

The NGI STOT that supports the Supplemental Fingerprint and Palmprint Deletion request will be

developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require supplemental fingerprint and palmprint specific information as part of a Supplemental Fingerprint and Palmprint Deletion request.

3.6.40.2 Supplemental Fingerprint and Palmprint Deletion Request Processing

NGI shall delete the supplemental fingerprint and palmprint specified in the Supplemental Fingerprint and Palmprint Deletion request.

NGI shall reject a Supplemental Fingerprint and Palmprint Deletion request if the specified Supplemental Fingerprint and Palmprint does not exist.

3.6.40.3 Supplemental Fingerprint and Palmprint Deletion Request Outputs

NGI shall provide a Supplemental Fingerprint and Palmprint Deletion response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Supplemental Fingerprint and Palmprint Deletion response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate Supplemental Fingerprint and Palmprint Deletion response to an Authorized FBI Service Provider.

There will be no EBTS normal NGI responses other than communication protocol acknowledgments for this transaction type. If there is an error in the submittal, a reject response will be returned.

3.6.41 Deleted

3.6.41.1 Deleted

Deleted.

Deleted.

3.6.41.2 Deleted

Deleted.

Deleted.

3.6.41.3 Deleted

Deleted.

Deleted.

3.6.42 Direct Iris Data Enrollment Request

3.6.42.1 Direct Iris Data Enrollment Request Inputs

NGI shall accept a Direct Iris Data Enrollment request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Iris Data Enrollment request is IIE.

NGI shall allow an Authorized FBI Service Provider to submit a Direct Iris Data Enrollment request.

The NGI STOT that supports the Direct Iris Data Enrollment request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a designation of the repository(ies) into which iris data should be added in a Direct Iris Data Enrollment request.

NGI shall accept a Direct Iris Data Enrollment request without a UCN or fingerprints into an SPC File.

NGI shall accept a Direct Iris Data Enrollment request with a UCN and ten or fewer fingerprints.

NGI shall accept a Direct Iris Data Enrollment request with a UCN and no fingerprints, when an MOU is in place with the Authorized Contributor.

NGI shall accept a Direct Iris Data Enrollment request with a UCN and event specific information.

NGI shall accept Direct Iris Data Enrollment requests in bulk via multiple methods (e.g., FTP, CD, DVD).

3.6.42.2 Direct Iris Data Enrollment Request Processing

NGI shall enroll the iris data in the designated repository(ies) as a result of a Direct Iris Data Enrollment request.

NGI shall provide the capability to uniquely identify iris data enrolled as a result of a Direct Iris Data Enrollment request.

NGI shall reject a Direct Iris Data Enrollment request when the specified UCN or event does not exist.

NGI shall reject a Direct Iris Data Enrollment request when the specified UCN cannot be validated using the submitted fingerprints.

NGI shall reject a Direct Iris Data Enrollment request if no iris data repository is specified.

NGI shall reject a Direct Iris Data Enrollment request without fingerprints when an MOU is not in place for the Authorized Contributor.

NGI shall perform a cascaded iris data search of the UIF if the iris data submitted with a Direct Iris Data Enrollment request meets the minimum quality standards for iris searches in accordance with cascaded search business rules.

NGI shall perform a cascaded iris data search of marked SPC File(s) if the iris data submitted with a Direct Iris Data Enrollment request meets the minimum quality standards for iris searches in accordance with cascaded search business rules.

3.6.42.3 Direct Iris Data Enrollment Request Outputs

NGI shall provide a Direct Iris Data Enrollment response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Iris Data Enrollment response is IIER.

NGI shall provide the appropriate Direct Iris Data Enrollment response to an Authorized FBI Service Provider.

NGI shall provide a collective response for Direct Iris Data Enrollment requests when submitted in bulk.

NGI collective responses will include individual enrollment responses/status provided as part of single collective response to the user.

NGI shall advise the Iris Owner when iris data is enrolled as a result of a Direct Iris Data Enrollment request, but fails to meet minimum quality standards for iris searches.

3.6.43 Iris Data Deletion Request

3.6.43.1 Iris Data Deletion Request Inputs

NGI shall accept an Iris Data Deletion request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Iris Data Deletion request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit an Iris Data Deletion request.

The NGI STOT that supports the Iris Data Deletion request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require iris specific information as part of an Iris Data Deletion request.

3.6.43.2 Iris Data Deletion Request Processing

NGI shall delete the iris data specified in the Iris Data Deletion request.

NGI shall reject an Iris Data Deletion request if the specified iris data does not exist.

3.6.43.3 Iris Data Deletion Request Outputs

NGI shall provide an Iris Data Deletion response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Iris Data Deletion response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate Iris Data Deletion response to an Authorized FBI Service Provider.

3.6.44 Iris Decision Request

Authorized Contributors and FBI Service Providers can return positive, negative, or inconclusive decisions for candidates provided to them as a result of an iris search request or unsolved biometric notification. These decisions are used internally for statistical and algorithm analysis. Additionally, a positive decision returned from an unsolved iris owner can result in automatic deletion of the unsolved iris.

3.6.44.1 Iris Decision Inputs

NGI shall accept an Iris Decision from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Iris Decision request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Providers to submit an Iris Decision.

The NGI STOT that supports the Iris Decision will be developed in accordance with the NGI Message Definition Database (MDD).

3.6.44.2 Iris Decision Processing

NGI shall record the iris decision.

NGI shall delete the referenced iris data from the UIF if a positive Iris Decision is received from the owner of the unsolved iris data.

3.6.44.3 Iris Decision Outputs

NGI shall provide a reject response, as appropriate, for an Iris Decision.

NGI shall provide a response to an Iris Decision from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Iris Decision response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.6.45 Direct Rap Back Enrollment Request

3.6.45.1 Direct Rap Back Enrollment Inputs

NGI shall accept a Direct Rap Back Enrollment request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Rap Back Enrollment request is RBRE.

NGI shall allow an Authorized FBI Service Provider to submit a Direct Rap Back Enrollment request.

The NGI STOT that supports the Direct Rap Back Enrollment request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall accept a Direct Rap Back Enrollment request with a UCN and ten or fewer fingerprints from an Authorized Contributor.

NGI shall accept a Direct Rap Back Enrollment request with a UCN from an Authorized FBI Service Provider.

NGI shall accept a Direct Rap Back Enrollment request with a UCN and specified biographic data from an Authorized Contributor.

NGI shall require, as part of a Direct Rap Back Enrollment request, a designation of which event type(s) (e.g., civil, criminal, external system) will trigger Rap Back Notifications for the associated Identity.

NGI shall accept, as part of a Direct Rap Back Enrollment request, a Rap Back subscription expiration date for the associated Identity.

NGI shall accept, as part of a Direct Rap Back Enrollment request, a designation of the Authorized Contributor(s) that should receive Rap Back Activity Notifications for the associated Identity.

NGI shall accept an indicator on a Direct Rap Back Enrollment request that specifies if an Identity History Summary should be included with the Direct Rap Back Enrollment response.

NGI shall accept Direct Rap Back Enrollment requests in bulk via multiple methods (e.g., ftp, CD, DVD).

3.6.45.2 Direct Rap Back Enrollment Processing

NGI shall assign a default Rap Back subscription expiration date when an expiration date is not specified as part of the Direct Rap Back Enrollment request.

NGI shall assign the default Rap Back subscription expiration date when the expiration date specified, as part of the Direct Rap Back Enrollment request, exceeds the maximum allowable Rap Back subscription period.

NGI shall enroll the specified Identity into Rap Back as part of a Direct Rap Back Enrollment request.

NGI shall reject a Direct Rap Back Enrollment request when the specified UCN cannot be validated using the submitted fingerprints.

NGI shall reject a Direct Rap Back Enrollment request when the specified UCN does not exist.

NGI shall reject a Direct Rap Back Enrollment request when the specified UCN cannot be validated using the submitted biographic information.

3.6.45.3 Direct Rap Back Enrollment Outputs

NGI shall provide a Direct Rap Back Enrollment response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Direct Rap Back Enrollment response is RBMR.

NGI shall provide the appropriate Direct Rap Back Enrollment response to an Authorized FBI Service Provider.

NGI shall provide a collective response for Direct Rap Back Enrollment requests when submitted in bulk.

NGI collective responses will include individual enrollment responses/status provided as part of single collective response to the user.

NGI shall optionally include, on a Direct Rap Back Enrollment response, the Identity History Summary for the specified UCN.

3.6.46 Rap Back Maintenance Request

3.6.46.1 Rap Back Maintenance Request Inputs

NGI shall accept a Rap Back Maintenance request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Rap Back Maintenance request is the RBM.

NGI shall allow an Authorized FBI Service Provider to submit a Rap Back Maintenance request.

The NGI STOT that supports the Rap Back Maintenance request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a Rap Back Maintenance request to contain a UCN.

NGI shall provide the capability to modify Rap Back event type triggers as part of a Rap Back Maintenance request.

NGI shall provide the capability to add Rap Back Notification recipient(s) as part of a Rap Back Maintenance request.

NGI shall provide the capability to delete Rap Back Notification recipient(s) as part of a Rap Back Maintenance request.

NGI shall provide the capability to cancel a Rap Back subscription from the specified Identity as part of a Rap Back Maintenance request.

NGI shall provide the capability to delete the civil event associated with a rap back, when canceling a Rap Back subscription as part of a Rap Back Maintenance request.

NGI shall accept Direct Rap Back Maintenance requests in bulk via multiple methods (e.g., ftp, CD, DVD).

3.6.46.2 Rap Back Maintenance Request Processing

NGI shall perform the requested maintenance as part of a Rap Back Maintenance request.

NGI shall reject a Rap Back Maintenance request when the specified UCN does not exist.

NGI shall reject a Rap Back Maintenance request when the specified Rap Back subscription does not exist.

NGI shall reject a Rap Back Maintenance request when the specified Rap Back Notification recipient(s) does not exist.

NGI shall delete the entire Identity when the last civil event is deleted from a civil-only Identity as part of a Rap Back Maintenance request.

3.6.46.3 Rap Back Maintenance Request Outputs

NGI shall provide a Rap Back Maintenance response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Rap Back Maintenance response is the RBMR.

NGI shall provide the appropriate Rap Back Maintenance response to an Authorized FBI Service Provider.

NGI shall provide a collective response for Direct Rap Back Maintenance requests when submitted in bulk.

3.6.47 Rap Back Subscription Renewal Request

3.6.47.1 Rap Back Subscription Renewal Request Inputs

NGI shall accept a Rap Back Subscription Renewal request from an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Rap Back Subscription Renewal request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall allow an Authorized FBI Service Provider to submit a Rap Back Subscription Renewal request.

The NGI STOT that supports the Rap Back Subscription Renewal request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a Rap Back Subscription Renewal request to contain a UCN and Rap Back subscription expiration date.

3.6.47.2 Rap Back Subscription Renewal Request Processing

NGI shall update the Rap Back subscription as part of a Rap Back Subscription Renewal request.

NGI shall assign the default Rap Back subscription expiration date when the expiration date specified, as part of the Rap Back Subscription Renewal request, exceeds the maximum allowable Rap Back subscription period.

NGI shall reject a Rap Back Subscription Renewal request when the specified UCN does not exist.

NGI shall reject a Rap Back Subscription Renewal request when the specified Rap Back subscription does not exist.

3.6.47.3 Rap Back Subscription Renewal Request Outputs

NGI shall provide a Rap Back Subscription Renewal response to an Authorized Contributor in accordance with the latest EBTS version.

The EBTS TOT that supports the Rap Back Subscription Renewal response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall provide the appropriate Rap Back Subscription Renewal response to an Authorized FBI Service Provider.

3.6.48 External System Link Maintenance Request

3.6.48.1 External System Link Maintenance Request Inputs

NGI shall accept an External System Link Maintenance request from an Authorized External System in accordance with the latest EBTS version.

The EBTS TOT that supports the External System Link Maintenance request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall require an External System Link Maintenance request to contain a UCN and external system link identifier.

3.6.48.2 External System Link Maintenance Request Processing

NGI shall update an Identity with the link information contained in an External System Link Maintenance request from an External System (e.g., IDENT).

NGI shall reject External System Link Maintenance requests from External Systems when the specified UCN or external system link identifier does not exist.

NGI shall delete the external system link identifier (e.g., FIN) from the NGI Identity as part of an External System Link Maintenance request.

3.6.48.3 External System Link Maintenance Request Outputs

NGI shall provide an External System Link Maintenance response to an Authorized External System in accordance with the latest EBTS version.

The EBTS TOT that supports the External System Link Maintenance response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.6.49 External System Link Activity Request

The following requirements are related to receiving and processing activity notifications on linked records from External Systems. All External System Link Activity requests will be based on positive biometric identifications and verifications.

3.6.49.1 External System Link Activity Inputs

NGI shall accept an External System Link Activity request from External Systems in accordance with the latest EBTS version.

The EBTS TOT that supports the External System Linked Record Activity Notification will be

developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a UCN and associated external system link identifier as part of the External System Link Activity request.

3.6.49.2 External System Link Activity Processing

NGI shall validate the UCN and external system link identifier included in the External system Link Activity request, prior to generating notifications to Authorized Contributors (e.g., Wanting Agency, LESC, Rap Back Subscriber).

External System linked record activity results in unsolicited notifications to the appropriate Authorized Contributors. Refer to the *Notification Services Functional Requirements* section for more information.

3.6.49.3 External System Link Activity Outputs

NGI shall send a External System Link Activity request response to an Authorized External System in accordance with latest EBTS version.

The EBTS TOT that supports the Linked Activity Notification response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

3.6.50 Immigration Violator File Maintenance Request

The following functional requirements support the maintenance of IVF information:

3.6.50.1 Immigration Violator File Maintenance Requests Inputs

NGI shall accept Immigration Violator File Maintenance requests from NCIC in accordance with the latest NCIC Operating Manual.

The NGI STOT that supports the NCIC MKE for an Immigration Violator File Maintenance request will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall require a UCN and biographic data as part of an Immigration Violator File Maintenance request.

NGI shall require a designation of file maintenance type (e.g., add, modify, delete) as part of an Immigration Violator File Maintenance request.

3.6.50.2 Immigration Violator File Maintenance Requests Processing

NGI shall perform biographic validation using UCN and biographic data to validate the subject associated with an Immigration Violator File Maintenance request.

NGI shall update the Identity History record for the associated UCN using the designated file maintenance type and other data contained in an Immigration Violator File Maintenance request.

NGI shall reject an Immigration Violator File Maintenance request when the specified UCN is invalid.

NGI shall reject an Immigration Violator File Maintenance request when the biographic validation fails.

3.6.50.3 Immigration Violator File Maintenance Requests Outputs

NGI shall create a hardcopy reject in response to an Immigration Violator File Maintenance request, when appropriate.

Hardcopy rejects are for internal use only and may be reviewed by FBI Service Providers to resolve processing issues.

If appropriate, NGI will send unsolicited notifications to Authorized Contributors. Refer to the *Notification Services Functional Requirements* section for more information.

3.6.51 NFF Criminal Print Ident Request

3.6.51.1 NFF Criminal Print Ident Request Inputs

NGI shall accept an NFF Criminal Print Ident request from an NFF State in accordance with the III/NFF Operations and Technical Manual.

The NGI STOT that supports the NCIC MKE for NFF Criminal Print Ident request is CPI.

NGI shall require a UCN and SID as part of the NFF Criminal Print Ident request.

3.6.51.2 NFF Criminal Print Ident Request Processing

NGI shall validate the UCN and SID included in the NFF Criminal Print Ident request, prior to generating notifications to Authorized Contributors (e.g., Wanting Agency, LESC, Rap Back Subscriber).

NFF Criminal Print Ident request results in unsolicited notifications to the appropriate Authorized Contributors. Refer to the *Notification Services Functional Requirements* section for more information.

NGI shall validate the UCN and SID included in the NFF Criminal Print Ident request, prior to generating searches to External Systems.

NGI shall retrieve the composite fingerprint images for the specified UCN included in the NFF Criminal Print Ident request.

NGI shall include a unique transaction control number (TCN) in an External Tenprint Fingerprint Identification Search request, as part of the NFF Criminal Print Ident request.

The CPI message does not contain any biographic data for populating the External Tenprint Identification Search request. (NOTE: Today for IAFIS Shared Services use Default Data as outlined in ICA - NAM 2.018 will contain "CPI, CPI" for CRIM TOT (CPI).)

NGI shall record the correlation between the identified UCN and the unique transaction control number (TCN) included in an External Tenprint Fingerprint Identification Search request, as part of the NFF Criminal Print Ident request.

NGI shall indicate as part of an External Tenprint Fingerprint Identification Search request against an external repository whether or not the External System should establish a link based on External System Search rules when the external system search results in a positive identification, as part of the NFF Criminal Print Ident request.

NGI shall send an External Tenprint Fingerprint Identification Search request to an External System (e.g., IDENT), based on External System Search rules, when no record link exists to that External System for the given UCN.

The external system search rules should designate which external systems receive searches based on Criminal Print Ident requests.

NGI shall send an External Tenprint Fingerprint Identification Search request to an External System, when the external system is not IDENT, in accordance with the latest EBTS as part of the NFF Criminal Print Ident request.

NGI shall send an External Tenprint Fingerprint Identification Search request to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement as part of the NFF Criminal Print Ident request.

NGI shall send an External Information request to an External System (e.g., IDENT) based on External System Search rules, when the designated repository is external and a record link exists to that External System, as part of the NFF Criminal Print Ident request.

An External Information request will be used to retrieve external record information when a NFF Criminal Print Ident request of NGI contains a UCN record containing a linked identifier to an External System.

An External Information Request should only be sent if the contributor has designated they want to receive IDENT/LESC information.

NGI shall include the UCN and the external system link identifier in an External Information request, as part of the NFF Criminal Print Ident request.

NGI shall send an External Information request in accordance with the latest EBTS version, when the external system is not IDENT as part of a NFF Criminal Print Ident request..

The EBTS TOT that supports an External Information request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall send an External Information request to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement as part of a NFF Criminal Print Ident request.

NGI shall accept a response from an External System as a result of an External Information request in accordance with the latest EBTS version when the external system is not IDENT, as part of the NFF Criminal Print Ident request.

NGI shall accept a response from IDENT as a result of an External Information request repositories in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement, as part of the NFF Criminal Print Ident request.

NGI shall accept a response from an External System as a result of an External Tenprint Fingerprint Identification Search request of external repositories in accordance with the latest EBTS version when the external system is not IDENT, as part of the NFF Criminal Print Ident request.

NGI shall accept a response from IDENT as a result of an External Tenprint Fingerprint Identification Search request of external repositories in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement, as part of the NFF Criminal Print Ident request.

NGI shall accept an external system link identifier and biographic data from an External System (e.g., IDENT) in a response to an External Tenprint Fingerprint Identification Search request, as part of the NFF Criminal Print Ident request.

NGI shall accept a unique transaction control number (TCN) from an External System (e.g., IDENT) in a response to an External Tenprint Fingerprint Identification Search request, as part of the NFF Criminal Print Ident request.

NGI shall determine the identified UCN using the unique transaction control number (TCN) returned in an External Tenprint Fingerprint Identification Search response, and the previously recorded UCN/TCN correlation when an External Tenprint Fingerprint Identification Search results in a positive identification, as part of the NFF Criminal Print Ident request.

NGI shall update an Identity with the information contained in an External Tenprint Fingerprint Identification Search response from an External System (e.g., IDENT), as part of the NFF Criminal Print Ident request.

NGI shall send a TCN/UCN correlation message to an External System (e.g., IDENT), providing the Identified UCN when an External Tenprint Fingerprint Identification Search results in a positive identification, as part of the NFF Criminal Print Ident request.

NGI shall send a TCN/UCN correlation message to an External System in accordance with the latest EBTS version when the external system is not IDENT, as part of the NFF Criminal Print Ident request.

NGI shall send a TCN/UCN correlation message to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement, as part of the NFF Criminal Print Ident request.

NGI shall send an IAQ to the LESC as part of a NFF Criminal Print Ident request when an IDENT record exists.

An IAQ should only be sent if the contributor has designated they want to receive IDENT/LESC information.

NGI shall send an IAQ to LESC in accordance with the Nlets User and Technical Guide.

NGI shall accept an IAR from the LESC in accordance with the Nlets User and Technical Guide.

3.6.51.3 NFF Criminal Print Ident Request Outputs

NGI shall provide an NFF Criminal Print Ident request response to an NFF State in accordance with III/NFF Operations and Technical Manual.

The NGI STOT that supports the NCIC MKE for NFF Criminal Print Ident request response will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall combine the LESC IAR and the External System Response when the External System is IDENT as part of an NFF Criminal Print Ident request.

NGI shall forward the External System Response independent of the NFF Criminal Print Ident request response to an Authorized Contributor in accordance with the latest EBTS version.

A response should only be sent if the contributor has designated they want to receive IDENT/LESC information.

3.6.52 Shared Data Direct Enrollment

The following section contains the functional requirements that support the enrollment of records into the Shared Data. The process of enrolling implies an addition to the Shared Data. The Shared Data files are comprised of the NGI Shared Want Files which contain NGI records and the DHS Shared Watch Files which contain IDENT records.

3.6.52.1 Shared Data Direct Enrollment Inputs

NGI shall enroll NGI Shared Data that meets enrollment criteria (e.g., wants or warrants) into the Shared Data File on a periodic basis.

The NGI Shared Want File contains specific information of all individuals for which there is a want or warrant posted in the Subject Criminal History file and for which fingerprint images are available.

NGI shall retrieve the NGI images as part of an NGI Shared Data enrollment.

NGI shall compress all images enrolled as part of an NGI Shared Data enrollment request in accordance with the latest version of the EBTS (e.g., using Wavelet Scalar Quantization (WSQ) at a ratio 15:1).

NGI shall include an FNU as part of an NGI Shared Data enrollment.

NGI shall include the subject's gender, name and date of birth (DOB) as part of an NGI Shared Data enrollment.

NGI shall accept Shared Data enrollment requests from an External System (e.g., IDENT) in accordance with the latest version of the EBTS.

Enrollment requests from IDENT will be stored in the DHS Shared Watch file.

NGI shall accept two ANSI/NIST Type 4 image records from an External System (e.g., IDENT) as part of a Shared Data enrollment request.

NGI shall accept 14 ANSI/NIST Type 4 image records from an External System (e.g., IDENT) as part of a Shared Data enrollment request.

NGI shall be able to read the latest version of fingerprint images available for all individuals provided by an External System (e.g., IDENT) as part of a Shared Data enrollment request.

NGI shall de-compress all fingerprint images in accordance with the latest version of the EBTS (e.g., using Wavelet Scalar Quantization (WSQ) at ratio 15:1) as part of a Shared Data enrollment request from an External System (e.g., IDENT).

3.6.52.2 Shared Data Direct Enrollment Processing

NGI shall extract fingerprint features from the fingerprint images provided by an External System (e.g., IDENT) as part of a Shared Data enrollment request.

NGI shall store in the Shared Data the extracted fingerprint features received as part of a shared data enrollment request from an External System (e.g., IDENT).

NGI shall remove fingerprint images received as part of a Shared Data enrollment request from an External System (e.g., IDENT) within 24 hours following a successful features extraction.

NGI shall perform a Tenprint Fingerprint Investigative Image Search as a result of a Shared Data enrollment request from an External System (e.g., IDENT).

NGI shall generate a list of candidates as the result of a Tenprint Investigative Image Search initiated by a Shared Data enrollment request from an External System (e.g., IDENT).

NGI shall calculate a match score for each candidate resulting from a Tenprint Fingerprint Investigative Image Search initiated by a Shared Data enrollment request from an External System (e.g., IDENT).

NGI shall determine a positive identification decision for each candidate that has a match score above the high confidence threshold as a result of a Tenprint Fingerprint Investigative Image Search initiated by a Shared Data enrollment request from an External System (e.g., IDENT).

NGI shall require an Authorized FBI Service Provider to perform a manual Fingerprint Identification Comparison (FIC) for each candidate resulting from a Tenprint Fingerprint Investigative Image Search initiated by a Shared Data enrollment request from an External System (e.g., IDENT) that is below the high confidence threshold.

NGI shall require a second Authorized FBI Service Provider to perform a manual FIC to confirm a positive identification for each candidate resulting from a Tenprint Fingerprint Investigative Image Search initiated by a Shared Data enrollment request from an External System (e.g., IDENT) that is below the low confidence threshold.

NGI shall store all candidates and their correlating EID resulting in a positive identification as a result of a Tenprint Investigative Image Search initiated by a Shared Data enrollment request from an External System (e.g., IDENT).

NGI will maintain the FNUs and DHS unique id (EIDs) of all Shared Watch List Candidates resulting in a positive identification.

3.6.52.3 Shared Data Direct Enrollment Outputs

NGI shall reject a Shared Data enrollment request that fails to include a valid ORI.

NGI shall generate an Error Message resulting from a failed Shared Data enrollment request.

3.6.53 Shared Data Maintenance

Maintenance messages from NGI include removals and demotions. A demotion is a canceled Want in NGI that may be maintained in an External System (e.g., IDENT) if a previous encounter has occurred.

3.6.53.1 Shared Data Maintenance Inputs

NGI shall accept a shared data removal requests from an External System (e.g., IDENT) in accordance with the latest version of the EBTS.

3.6.53.2 Shared Data Maintenance Processing

NGI shall process shared data removal requests for NGI Shared Data (e.g., wants or warrants) when indicated.

NGI shall process shared data demotion requests for NGI Shared Data (e.g., wants or warrants) when indicated.

NGI shall remove all biometric and biographic information for individuals identified in a shared data removal request.

NGI shall remove all biometric and biographic information for individuals identified in a shared data demotion request.

NGI shall remove all biometric and biographic information for individuals identified in a shared data removal request from an External System (e.g., IDENT).

NGI shall identify the unique identifier for any individuals for whom the External System (e.g., IDENT) received an order to remove or demote.

NGI shall be able to match the unique identifier and the corresponding images for each individual provided by an External System (e.g., IDENT).

3.6.53.3 Shared Data Maintenance Outputs

NGI shall generate an Error Message for a failed shared data maintenance request of NGI Shared Data.

NGI shall generate an Error Message to an External System (e.g., IDENT) resulting from a failed External System shared data maintenance request.

There will be no EBTS successful NGI response other than communication protocol acknowledgments for this transaction type.

3.7 Administrative and Control Services

The following section contains those functional requirements that are related to specific areas of the administrative and control functions of the NGI.

3.7.1 System Status and Reporting (SSR)

The System Status and Reporting (SSR) capability provides status information on current response time performance, resources allocated to each environment (operational, testing), the readiness and availability of hardware components, staffing resources, and other information to identify processing bottlenecks and tune system performance.

NGI shall allow an Authorized FBI System Administrator access to a centralized system status reporting service.

NGI shall allow an Authorized FBI Service Provider access to a centralized system status reporting service.

NGI shall provide a centralized system status reporting service.

NGI shall provide parameter-based system status reporting capabilities.

NGI shall provide pre-defined system status reporting capabilities.

NGI shall collect system status data (e.g., readiness, utilization, queue status) for system components.

NGI shall collect system performance data (e.g., response times, workload).

NGI shall provide system status reporting capabilities on each active system environment (e.g., operational, development, test).

NGI shall provide system performance reporting capabilities on each active system environment (e.g., operational, development, test).

NGI shall retain system status data.

NGI shall retain system performance data.

NGI shall be capable of reporting the number of positive identifications resulting from Tenprint Fingerprint Identification Searches against the NGI Shared Data.

NGI shall be capable of reporting the number of positive identifications resulting from Tenprint Fingerprint Identification Searches against an External System's (e.g., IDENT) Shared Data.

NGI shall be capable of reporting the number of Tenprint Fingerprint Identification Searches performed against the records contained in the NGI Shared Data.

NGI shall be capable of reporting the number of Tenprint Fingerprint Identification Searches performed against the records contained in an External System's (e.g., IDENT) Shared Data.

3.7.2 Data Management

This section provides all functional requirements specific to the data management of the NGI.

3.7.2.1 NGI Access Authorization Rules

Access to NGI repository files will be controlled based on a set of authorization rules. NGI will provide the capability to add, delete, and modify these authorization rules.

NGI shall provide the capability to maintain authorization rules (i.e., read/write/delete access) for all Identity History activities.

NGI shall provide the capability to maintain authorization rules (i.e., read/write/delete access) for all fingerprint maintenance activities.

NGI shall provide the capability to maintain authorization rules (i.e., read/write/delete access) for all Latent maintenance activities.

NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) the criminal repository.

NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) the civil repository.

NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) the RISC.

NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) an unsolved biometric file.

NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) an SPC File.

NGI shall provide the capability to maintain rules regarding who will be permitted to access (e.g., search, retrieve) a newly created NGI repository.

NGI shall support Authorized FBI Service Provider workgroup assignments.

NGI shall allow Authorized ITF Contributors to perform maintenance on only their Identity data.

NGI shall allow an Authorized External System to perform maintenance on only their Identity data.

NGI shall allow Authorized Contributors to perform Identity maintenance on only their Identity data.

NGI shall allow Authorized FBI Service Providers to perform Identity maintenance on all Identity data.

NGI shall allow Authorized Contributors to perform photo maintenance on their own photos.

NGI shall allow Authorized FBI Service Providers to perform photo maintenance on all photos.

NGI shall allow Authorized Contributors to perform palmprint maintenance on their own palmprints.

NGI shall allow Authorized FBI Service Providers to perform palmprint maintenance on all palmprints.

NGI shall allow Authorized Contributors to perform supplemental fingerprint and palmprint maintenance on their own supplemental fingerprint and palmprint information.

NGI shall allow Authorized FBI Service Providers to perform supplemental fingerprint and palmprint maintenance on all Supplemental Fingerprint and Palmprint information.

NGI shall allow Authorized Contributors to perform iris maintenance on their own iris data.

NGI shall allow Authorized FBI Service Providers to perform iris maintenance on all iris data.

NGI shall allow Authorized Contributors to perform Rap Back maintenance on their own Rap Back subscriptions.

NGI shall allow Authorized FBI Service Providers to perform Rap Back maintenance on all Rap Back subscriptions.

NGI shall allow Authorized Contributors to perform Rap Back subscription renewal on their own Rap Back subscriptions.

NGI shall allow Authorized FBI Service Providers to perform Rap Back subscription renewal on all Rap Back subscriptions.

NGI shall reject requests from Authorized Contributors who do not have valid authorization to perform requested system services.

3.7.2.2 NGI Dissemination Rules

NGI shall apply dissemination rules to all NGI Responses.

NGI shall apply dissemination rules to all NGI Notifications.

NGI shall provide the capability to maintain dissemination rules for information contained in the criminal repository.

NGI shall provide the capability to maintain dissemination rules for information contained in the civil repository.

NGI shall provide the capability to maintain dissemination rules in support of a RISC multi-tiered shared data infrastructure.

NGI shall provide the capability to maintain dissemination rules for information in an SPC File.

NGI shall provide the capability to maintain dissemination rules for information contained in a newly created NGI repository.

NGI shall provide the capability to maintain dissemination rules for all photo responses.

NGI shall provide the capability to maintain dissemination rules for all palmprint responses.

NGI shall provide the capability to maintain dissemination rules for all supplemental fingerprint and palmprint responses.

NGI shall provide the capability to maintain dissemination rules for all iris responses.

NGI shall provide the capability to maintain dissemination rules for all fingerprint responses.

NGI shall provide the capability to maintain dissemination rules for all Tenprint Identification Search responses.

NGI shall provide the capability to maintain dissemination rules for all Fingerprint Verification responses.

NGI shall provide the capability to maintain dissemination rules for International Terrorist Identification Search responses based upon a multi-tiered shared data structure.

NGI shall provide the capability to maintain dissemination rules for all Latent Fingerprint Investigation Search responses.

NGI shall provide the capability to maintain dissemination rules for all Latent Print Search responses.

NGI shall provide the capability to maintain dissemination rules for all Immigration Violator File Notifications.

NGI shall provide the capability to maintain dissemination rules for all Want Notifications.

NGI shall provide the capability to maintain dissemination rules for all Latent Decision Notifications.

NGI shall provide the capability to maintain dissemination rules for all Special Processing Flag Notifications.

NGI shall provide the capability to maintain dissemination rules for all Consolidation Notifications.

NGI shall provide the capability to maintain dissemination rules for all Rap Back Renewal Notifications.

NGI shall provide the capability to maintain dissemination rules for all Rap Back Notifications.

NGI shall provide the capability to maintain dissemination rules for information in an unsolved biometric file.

NGI shall provide the capability to maintain dissemination rules for all Identity History responses.

NGI shall provide the capability to maintain dissemination rules for all Investigation Search responses.

NGI shall provide the capability to maintain dissemination rules for all Linked Record Activity Notifications.

NGI shall provide the capability to maintain dissemination rules for all External System Linked Record Activity Notifications.

3.7.2.3 NGI Repository File Maintenance Rules

NGI shall perform maintenance of Identity history contained within the NGI Repositories as a result of fingerprint identification searches in accordance with Table 3-1 File Maintenance Rules.

NGI shall perform maintenance of biometric information contained within the NGI Repositories as a result of fingerprint identification searches in accordance with Table 3-1 File Maintenance Rules.

NGI shall maintain Identity information as a result of Identity maintenance requests in accordance with Table 3-1 File Maintenance Rules.

Table 3-1 File Maintenance Rules

Submission Type	Biographic compilation	Certification File	Biometric Composite	Retain Event
Criminal				
Ident-Retain	Update	Add	Quality Improvement	Yes
Ident-Return	No*	Add	Quality Improvement	No**
Non-Ident-Retain	Create	Add	Create	Yes
Non-Ident- Return	No	No	No	No
Civil				
Ident-Retain	Update	Add	Quality Improvement	Yes
Ident-Return	Update	Add	Quality Improvement	No**
Non-Ident-Retain	Create	Add	Create	Yes
Non-Ident-Return	No	No	No	No
Humanitarian Ident - Retain/Return	Update	Add	Quality Improvement	No
Humanitarian Non-Ident-Retain/Return	Create	Add	Create	No
Identity Maintenance				
Biometric Maintenance (e.g., palm, photo, iris, supplemental fingerprint and palmprint)	Update	Add	Update	Update
Biographic Maintenance (e.g., name, DOB)	Update	No	No	Update

*Except for Juvenile records for non-dissemination only.
** Event logged in record for historical information.

NGI shall provide the capability to maintain rules regarding enrollment into the criminal repository.

NGI shall provide the capability to maintain rules regarding enrollment into the civil repository.

NGI shall provide the capability to maintain enrollment rules regarding who will be permitted to enter information into an unsolved biometric file.

NGI shall provide the capability to maintain enrollment rules regarding who will be permitted to enter information into an SPC File.

NGI shall provide the capability to maintain enrollment rules regarding what types of records may be included in the RISC.

NGI shall provide the capability to maintain enrollment rules regarding who will be permitted to enter information into the RISC.

NGI shall enroll records to the RISC when record type satisfies enrollment rules for RISC.

Some special interest NGI records (e.g., wanted persons) will satisfy RISC enrollment rules.

NGI shall delete records from the RISC when record type no longer satisfies enrollment rules for RISC.

NGI shall provide the capability to maintain enrollment rules for a newly created NGI repository.

3.7.2.4 Identity History Summary

NGI shall provide event information as part of the Identity History Summary.

Event information may be retained as part of a criminal justice (e.g., notations of arrests, detention, criminal charges, and dispositions) or non-criminal justice (e.g., background checks) purpose.

NGI shall provide a UCN as part of the Identity History Summary.

NGI shall provide biographic data as part of the Identity History Summary.

NGI shall provide an external system link identifier(s) (e.g., FIN, NIC) as part of the Identity History Summary.

NGI shall provide active Want information as part of the Identity History Summary

NGI shall provide active Flash information as part of the Identity History Summary

NGI shall provide active SOR information as part of the Identity History Summary.

NGI shall provide Identity Theft information as part of the Identity History Summary.

NGI shall provide an IVF indicator as part of the Identity History Summary.

NGI shall indicate, on an Identity History Summary, whether or not photos are available for the specified subject.

NGI shall indicate, on an Identity History Summary, whether or not iris data is available for the specified subject.

NGI shall indicate, on an Identity History Summary, whether or not palmprints are available for the specified subject.

NGI shall indicate, on an Identity History Summary, whether or not supplemental fingerprint and palmprint data is available for the specified subject.

3.7.2.5 System Business Rules and Thresholds

Maintenance of business rules and thresholds allows for the modification of these parameters without impacting NGI availability.

NGI shall provide the capability to maintain Rap Back Notification rules.

Rap Back Notification rules will indicate if an Authorized Recipient receives pre-notification, an Identity History Summary or just triggering event information.

NGI shall provide the capability to maintain External System Search rules.

NGI shall provide the capability to maintain consolidation rules to support the Identity Consolidation function.

The following functional requirements are specific to the data management supporting Tenprint Fingerprint Services:

NGI shall provide the capability to maintain business rules to support AQC of textual data as part of a Tenprint Fingerprint Identification Search.

NGI shall provide the capability to maintain business rules to support the ASC function.

NGI shall support, and the CJIS Division will make publicly available, fingerprint image quality threshold for fingerprint retention based upon image quality standards required in the latest version of the EBTS.

NGI shall support, and the CJIS Division will make publicly available, a fingerprint image quality threshold for fingerprint searching based upon image quality standards required in the latest version of the EBTS.

NGI shall support a fingerprint image quality improvement threshold.

This threshold will be used to determine whether to submit a subsequent search to an External System when better fingerprints are received by NGI.

NGI shall provide the capability to maintain business rules to support the cascaded searching of NGI repositories.

The cascaded search business rules will provide the capability for states to optionally decline participation due to state laws or state statutes. In addition, NGI will not perform a cascaded search when enrolling a Tier-3 Identity or in the event of a positive identification against a Tier-3 Identity.

NGI shall support various fingerprint image resolutions in accordance with the latest EBTS version (e.g., 500ppi, 1000ppi).

Deleted.

Deleted.

NGI shall provide the capability to maintain minimum fingerprint match thresholds to support III/Verify function.

NGI shall provide the capability to maintain a minimum fingerprint match threshold to support cascaded fingerprint searches of the ULF.

NGI shall provide the capability to maintain a minimum palmprint match threshold to support cascaded palmprint searches of the ULF.

NGI shall provide the capability to maintain a minimum facial match threshold to support cascaded searches of the UPF.

NGI shall provide the capability to maintain a minimum iris match threshold to support cascaded searches of the UIF.

NGI shall provide the capability to maintain minimum fingerprint match thresholds to support cascaded searches of marked SPC files.

NGI shall provide the capability to maintain minimum palmprint match thresholds to support cascaded searches of marked SPC files.

NGI shall provide the capability to maintain minimum facial match thresholds to support cascaded searches of marked SPC files.

NGI shall provide the capability to maintain minimum iris match thresholds to support cascaded searches of marked SPC files.

NGI shall support fingerprint image compression algorithm in accordance with the latest version of the EBTS.

Once a Tenprint image has been placed into the system it will be compressed. All images will be transmitted in compressed format. All Tenprint print images should be compressed in accordance with the EBTS.

NGI shall provide the capability to maintain a high confidence threshold to support automated FIC.

This threshold provides decision point for automated or "lights-out" identification or verification decisions.

NGI shall provide the capability to maintain a low confidence threshold to support automated FIC.

This threshold provides decision point as to whether one or two manual FICs are required.

Deleted.

Deleted.

NGI shall provide the capability to maintain external system response time thresholds.

These thresholds will determine when NGI will send a partial response when a response has not been received from an External System within an allowable time limit.

NGI shall provide the capability to maintain a daily IAQ search limit.

NGI shall provide 95% segmentation accuracy of the plain impression in support of the Automated Fingerprint Sequence Check Service (e.g., produce highly matchable images, identify finger positions, detect segmentation failures).

NGI shall provide the capability to maintain fingerprint image quality standards.

NGI shall provide the capability to maintain latent fingerprint image quality standards.

NGI shall provide the capability to maintain latent print image quality standards.

NGI shall support, and the CJIS Division will make publicly available, photo image quality thresholds for facial recognition based upon image quality standards required in the latest EBTS version.

NGI shall support, and the CJIS Division will make publicly available, palmprint image quality thresholds for search based upon image quality standards required in the latest EBTS version.

NGI shall support, and the CJIS Division will make publicly available, supplemental fingerprint and palmprint image quality thresholds for search based upon image quality standards required in the latest EBTS version.

NGI shall support, and the CJIS Division will make publicly available, iris image quality reject thresholds for search based upon iris image quality standards required in the latest EBTS version.

NGI shall provide the capability to maintain limits for the maximum number of candidates to return for all Investigation searches.

NGI shall provide the capability to maintain a LESC notification time limit.

LESC does not want notifications where the Date of Event (e.g. arrest) for the submission is greater that a configurable amount of days.

NGI shall provide the capability to maintain LESC notification rules.

LESC Notification rules will indicate what type of submission (e.g. criminal, civil) from which users (CRI/ORI) should allow a notification to be sent to LESC.

3.7.2.6 Latent Data Management

NGI shall delete the oldest record from the ULF, when the ULF is at maximum capacity and a new record is received for enrollment.

NGI shall compare stored latent investigative search results to produce a Post Latent Processing (PLP) Correlation List.

The PLP Correlation List will consist of UCNs for the same candidate who appears in more than one set of search results for the same Latent Case (LCN).

NGI shall provide the capability to store latent search details.

3.7.2.7 Palmprint Data Management

NGI shall support a palmprint feature extraction method that is publicly available.

3.7.2.8 Identity Data Management

The following requirements are specific to the maintenance of Identity information.

NGI shall maintain a unique Identity across the multiple repositories (e.g., criminal, civil, RISC, unsolved biometric files).

NGI shall maintain the original source and date of all data associated with the Identity.

The source may be a system identifier, originating agency identifier, or other transaction source indicators.

NGI shall provide the capability for storing multiple occurrences up to a maximum number of biographic identifiers in each Identity History Record.

Biographic identifiers may include, but will not be limited to: Name/Alias Name, Date of Birth, Social Security Number, Miscellaneous Number, Scars, Marks and Tattoos, Sex, Race and Citizenship.

NGI shall provide the capability to mark an Identity for notification purposes.

Examples of notifications for which an Identity can be marked are Want, Flash, SOR, Identity Theft Victim, IVF, and Rap Back.

NGI shall support the synchronization of Identity History Data in accordance with the III/NFF Operational and Technical Manual.

A periodic III Identity History data synchronization will be conducted with state systems to ensure that data is consistent with the FBI systems. NGI data for specific states will be made available periodically via magnetic media or ftp for this synchronization process.

NGI shall provide the capability to perform inter-repository searches to identify potential Identity consolidations.

NGI shall provide the capability to perform intra-repository searches to identify potential Identity consolidations.

NGI shall provide the capability to perform comparisons of the fingerprint records contained in an External System (e.g., IDENT) with the fingerprint records contained in a specified NGI repository.

NGI shall associate photos with an event if submitted with information identifying a specific event.

NGI shall associate photos with the Identity record when submitted without information identifying a specific event.

NGI shall associate photos with the Identity record when the event related to the photos is deleted.

NGI shall associate palmprints with an event if submitted with information identifying a specific event.

NGI shall associate palmprints with the Identity record when submitted without information identifying a specific event.

NGI shall associate palmprints with the Identity record when the event related to the palmprints is deleted.

NGI shall associate supplemental fingerprint and palmprint information with an event if submitted with information identifying a specific event.

NGI shall associate supplemental fingerprint and palmprint information with the Identity record when submitted without information identifying a specific event.

NGI shall associate supplemental fingerprint and palmprint information with the Identity record when the event related to the Supplemental Fingerprint and Palmprint is deleted.

NGI shall associate iris information with an event if submitted with information identifying a specific event.

NGI shall associate iris information with the Identity when submitted without information identifying a specific event.

NGI shall associate iris information with the Identity when the event related to the iris information is deleted.

The following functional requirements are specific to the retrieval of Identity information.

NGI shall retrieve the requested biographic information from the designated repository(ies) for the specified criteria and Identity.

NGI shall retrieve the requested biographic compilation for the specified criteria and Identity.

NGI shall retrieve the requested event Identity information from the designated repository(ies) for the specified criteria and Identity.

NGI shall retrieve the requested biometric information from the designated repository(ies) for the specified criteria and Identity.

NGI shall retrieve the requested composite biometric information for the specified criteria and Identity.

The following functional requirements are specific to Identity enrollment.

NGI shall enroll an Identity as a result of a direct biometric enrollment request.

NGI shall create a unique UCN for the Identity as part of an Identity enrollment.

NGI shall create UCNs that do not indicate chronological order.

NGI shall create UCNs that do not indicate repository association.

NGI shall create UCNs that contain a built-in redundancy check.

A redundancy check may be a check digit that is computed from the other digits of the UCN. This ensures the validity of a UCN by eliminating typographical errors, and increases the security by making it more difficult to fabricate a UCN.

NGI shall determine a unique event identifier for the Identity and Event as part of an Identity enrollment.

NGI shall enroll biographic information into the designated repository(ies) as part of an Identity enrollment.

NGI shall associate the enrolled biographic information with the unique event identifier as part of an Identity enrollment.

NGI shall associate the enrolled biometric information with the unique event identifier as part of an Identity enrollment.

NGI shall enroll event information into the designated repository(ies) as part of an Identity enrollment.

NGI shall associate the enrolled event information with the unique event identifier as part of an Identity enrollment.

NGI shall create a biographic compilation as part of an Identity enrollment.

NGI shall associate the biographic compilation with the unique Identity as part of an Identity enrollment.

NGI shall create biometric composite(s) in accordance with biometric file maintenance business rules as part of an Identity enrollment.

NGI shall associate the biometric composite with the unique Identity as part of an Identity enrollment.

NGI shall create an Event certification copy containing all the original Identity data for a specific event as part of an Identity enrollment.

The following functional requirements are specific to an Identity update.

NGI shall determine a unique event identifier for the Identity and Event as part of an Identity update.

NGI shall enroll biographic information into the designated repository(ies) as part of an Identity update.

NGI shall associate biographic information with the unique event identifier as part of an Identity update.

NGI shall associate biometric information with the unique event identifier as part of an Identity update.

NGI shall enroll event information into the designated repository(ies) as part of an Identity update.

NGI shall associate event information with the unique event identifier as part of an Identity update.

NGI shall update the biographic compilation, if applicable, for the Identity as part of an Identity update.

NGI shall create a biometric composite(s) in accordance with biometric file maintenance business rules as part of an Identity update.

NGI shall associate the biometric composite(s) with the unique Identity as part of an Identity update.

NGI shall update the biometric composite(s) for the Identity in accordance with biometric file maintenance business rules as part of an Identity update.

The following functional requirements are specific to cascading searches when a biometric composite has been updated and a cascaded or direct search of these repositories has not completed for the transaction that triggered this update.

NGI shall perform a cascaded fingerprint search of the ULF using the updated fingerprint composite, in accordance with cascaded search business rules, as a result of a fingerprint composite update.

NGI shall perform a cascaded fingerprint search of the marked SPC Files using the updated fingerprint composite, in accordance with cascaded search business rules, as a result of a fingerprint composite update.

Deleted.

Deleted.

NGI shall create an Event certification copy containing all original identification information for a specific event as part of an Identity update.

The following functional requirement is specific to the update of biographic information associated with an Identity.

NGI shall update biographic information, if applicable, for the Identity as part of a biographic update.

The following functional requirement is specific to the update of event information associated with an Identity.

NGI shall update event information, if applicable, for the Identity as part of an event update.

The following functional requirements are specific to deletion of an entire Identity. This will occur when the last arrest is removed from a criminal-only record (Expungement), the last civil cycle is deleted from a civil-only record (Civil Deletion), or the entire Identity is deleted via an Identity History Record Modification request.

NGI shall delete all biographic information associated with the Identity as part of an Identity deletion.

NGI shall delete all biometric information associated with the Identity as part of an Identity deletion.

NGI shall delete the biographic compilation associated with the Identity as part of an Identity deletion.

NGI shall delete all biometric composite information associated with the Identity as part of an Identity deletion.

NGI shall delete all event information associated with the Identity as part of an Identity deletion.

NGI shall mark the UCN for a deleted Identity as deleted.

NGI shall allow complete restoration of an Identity within a specified period of time following Identity deletion.

NGI shall send a Link Maintenance request to the appropriate External System when an Identity containing an external link is deleted.

NGI shall include the deleted UCN and External System Identifier as part of a Link Maintenance request.

NGI shall send a Link Maintenance request indicating deletion to an External System in accordance with the latest EBTS version.

The EBTS TOT that supports the Link Maintenance request will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall accept a Link Maintenance response from an External System in accordance with the latest EBTS version.

The EBTS TOT that supports the Link Maintenance response will be developed in accordance with the ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information.

NGI shall perform exception processing when a Link Maintenance request is rejected by an External System.

Exception processing may include notifying an Authorized FBI Service Provider or a System Administrator of the reject.

The following functional requirements are specific to deletion of an Event from an Identity. Biographic and biometric information associated with an event will not be deleted as part of an event deletion, but can be deleted as a separate request. If an Authorized Contributor specifically requests the deletion of an Event and all associated biographic and biometric information, separate biographic, biometric, and event deletion requests will need to be initiated.

NGI shall re-associate the biographic information associated with the Event to the Identity as part of an Event deletion.

NGI shall re-associate the biometric information associated with the Event to the Identity as part of an Event deletion.

NGI shall delete the event information associated with the Event as part of an Event deletion.

NGI shall mark the unique Event identifier as deleted, for the deleted event as part of an Event deletion.

The following functional requirements are specific to deletion of biometric information from an Identity.

NGI shall delete the specified biometric information as part of a biometric deletion.

NGI shall delete the specified biometric information from the biometric composite in accordance with biometric file maintenance business rules as part of a biometric deletion.

NGI shall update the biometric composite(s) associated with the Identity in accordance with biometric file maintenance business rules as part of a biometric deletion.

The following functional requirements are specific to deletion of biographic information from an Identity.

NGI shall delete the specified biographic information as part of a biographic deletion.

NGI shall delete the specified biographic information from the biographic compilation, if applicable, as part of a biographic deletion.

NGI shall update the biographic compilation associated with the Identity, if applicable, as part of a biographic deletion.

The following requirements are specific to data retention.

NGI shall comply with the data retention rules for the External System (e.g., IDENT).

NGI shall provide the capability to maintain External System data retention rules for fingerprint transactions.

The following requirements are related to external system links.

NGI shall support the maintenance of external system link identifiers (i.e., FIN) for multiple External Systems.

NGI shall maintain one unique external system link identifier per External System for an Identity.

NGI shall associate an external system's link identifier with only one Identity.

NGI shall maintain the external system link identifier and source system.

3.7.2.9 Computerized Contributor Address File (CCA) Maintenance

NGI shall maintain the CCA File that contains contributor data (e.g., list of addresses) for Authorized Contributors.

The contributor data will be used for validation of incoming transactions and dissemination of responses.

NGI shall support the association of discontinued (retired) contributor identifiers to another active contributor record in the NGI CCA File.

NGI shall provide electronic responses to Authorized Contributors using contributor data (e.g., e-mail address) contained within NGI CCA File.

NGI shall provide hardcopy responses to Authorized Contributors using contributor data (e.g., mailing address) contained within NGI CCA File.

NGI will use the stored contributor data to verify the required destination when preparing responses to NGI submissions. These responses may be either electronic or hardcopy depending upon the individual contributors needs. NGI will determine if the contributor can accept electronic or hardcopy responses and transmit the responses accordingly. If hardcopy responses are required, the resolution of the hardcopy will be of sufficient quality to meet tenprint fingerprint image comparison requirements.

3.7.2.10 NCIC Data Synchronization

NGI shall accept an NCIC ORI File Maintenance message in accordance with the III/NFF Operations and Technical Manual.

The NGI STOT that supports the NCIC MKE for an NCIC ORI File Maintenance will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall update the NCIC ORI File using the data contained within the NCIC ORI File Maintenance message.

The NGI NCIC ORI file will be kept in synchronization with NCIC for message validation purposes.

NGI shall accept an NCIC Line File Maintenance message in accordance with the III/NFF Operations and Technical Manual.

The NGI STOT that supports the NCIC MKE for an NCIC Line File Maintenance Message will be developed in accordance with the NGI Message Definition Database (MDD).

NGI shall update the NCIC Line File using the data contained within the NCIC Line File Maintenance message.

The NGI NCIC Line file will be kept in synchronization with NCIC for message validation purposes.

NGI shall support the synchronization of internal code tables with corresponding NCIC code tables (e.g., SMT, eye, hair).

3.7.2.11 Maintain MOU Information

Information regarding what agencies have MOU's on file with CJIS will be maintained electronically. This is for the purpose of validating biometric enrollment submissions that do not contain fingerprints. If an agency does not have an MOU in place with CJIS, they must include fingerprints with secondary biometric enrollment submissions.

NGI shall provide the capability to maintain photo enrollment MOU information.

NGI shall provide the capability to maintain palmprint enrollment MOU information.

NGI shall provide the capability to maintain supplemental fingerprint and palmprint enrollment MOU information.

NGI shall provide the capability to maintain iris enrollment MOU information.

3.7.2.12 Data Conversion

NGI shall provide the capability to convert International standard messages into the latest EBTS format.

International standard will be in accordance with the latest ANSI/NIST-ITL Data Format for the Interchange of Fingerprint, Facial, and other Biometric Information version

NGI shall create a pre-conversion copy of International transactions for the NGI Certification File.

Certification file copies of International transactions will be saved both prior to and subsequent to data conversion.

NGI shall provide the capability to convert EBTS standard messages into other International standard formats.

3.7.2.13 Records Management

NGI shall comply with electronic recordkeeping requirements as outlined in the FBI Electronic Recordkeeping Certification (ERKC) Manual.

3.7.2.14 Computerized Records Sent File Maintenance

The Computerized Records Sent (CRS) database, maintained by III, contains records of those agencies that receive copies of responses.

NGI shall provide the capability to store all the necessary information for agencies that receive copies of responses in the Computerized Records Sent File.

3.7.2.15 Cascaded Searches

NGI shall search biometric information against the appropriate unsolved biometric file as a part of a cascaded search.

NGI shall search biometric information against the marked SPC files as part of a cascaded search.

NGI shall apply cascaded search business rules to all cascaded searches.

NGI shall calculate a match score for each candidate resulting from a cascaded search.

3.7.3 Repository Management

This section provides functional requirements specific to the maintenance of the NGI Repositories.

3.7.3.1 General Repository Management

NGI shall support multiple categories of fingerprint repositories (i.e., criminal, civil, ULF, SPC Files, RISC).

NGI shall support multiple categories of photo repositories (i.e., criminal, civil, UPF, SPC Files, RISC).

NGI shall support multiple categories of palmprint repositories (i.e., criminal, civil, ULF, SPC Files, RISC).

NGI shall support multiple categories of supplemental fingerprint and palmprint repositories (i.e., criminal, civil, ULF, SPC Files, RISC).

Deleted.

NGI shall support multiple categories of iris repositories (i.e., criminal, civil, UIF, SPC Files, RISC).

3.7.3.2 RISC Population

NGI shall provide the capability to populate the RISC with information from external repositories.

NGI shall maintain unique external repository identifiers for RISC records that are populated by external repositories.

NGI shall maintain the ITF as a subset of records within the RISC repository.

NGI shall provide the capability to synchronize the RISC with information from other repositories (internal or external).

3.7.3.3 Bulk Data Export

NGI shall write selected information contained in NGI repository(ies) to media (e.g., CD, DVD) as part of a bulk media export request.

NGI shall provide an automated capability for an Authorized FBI System Administrators to bulk export event certification copies.

NGI shall allow an Authorized FBI System Administrator to select information from the designated NGI repository(ies) as part of a bulk media export request.

NGI shall support removable media for bulk export of event certification copies.

3.7.3.4 Bulk Data Import

NGI shall support removable media for bulk import of fingerprint information.

NGI shall support removable media for the bulk enrollment of photos.

NGI shall support removable media for the bulk enrollment of palmprints.

NGI shall support removable media for the bulk enrollment of supplemental fingerprint and palmprint information.

NGI shall support removable media for bulk enrollment of iris information.

NGI shall support removable media for bulk enrollment of Rap Back information.

NGI shall accept bulk enrollment requests for the ITF via multiple methods (e.g., ftp, CD, DVD).

3.7.3.5 Repository Record Maintenance Log

NGI shall maintain a repository maintenance transaction log for each repository.

The repository maintenance log will contain adds, deletes, and modifications of repository data at the record level. This repository maintenance log will assist System Administrators and Database Administrators in recovering from database failures or inadvertent actions.

NGI shall create an entry in the repository maintenance transaction log for each creation, deletion and update action.

NGI shall support the use of the repository maintenance transaction log to restore the repository to a point in time.

3.7.3.6 Shared Data Management

NGI shall maintain a Shared Want Image File (SWIF) that is supported by NGI Shared Data updates.

NGI shall maintain a Shared Want Directory (SWD) that is supported by NGI Shared Data updates.

NGI shall maintain a Shared Want Activity Log (SWAL) that is supported by NGI Shared Data updates.

The SWIF, SWD and SWAL will be maintained on the SSC/FBI at the DOJ Rockville, MD facility. Features are extracted by IDENT from the images provided in the Shared Want Image File and maintained in the DHS Shared Want Directory for search by IDENT.

NGI shall maintain a Shared Watch Image File that is supported by an External System's (e.g., IDENT) Shared Data updates.

NGI shall maintain a Shared Watch Directory that is supported by an External System's (e.g., IDENT) Shared Data updates.

NGI shall maintain a Shared Watch Activity Log that is supported by an External System's (e.g., IDENT) Shared Data updates.

Features are extracted from the images provided in the Shared Watch Image File and maintained in the FBI Shared Watch Directory for search by NGI. These files will be maintained in the CJIS Data Center at the Clarksburg, WV facility.

3.7.4 System Administration

The System Administration (SA) function is responsible for handling all system alarms, errors, system diagnostics, system data backup and restore, system start and shutdown, resource allocation, and manual control of application/transaction processing priorities. These functions will be performed from the NGI Systems Management Center, the duty station of the Central System Administrators and Systems Security Administrators.

NGI shall allow Authorized System Security Administrators to terminate any or all transactions and processes occurring in any environment independent of other NGI environments.

NGI shall allow Authorized System Administrators to terminate any or all transactions and processes occurring in any environment independent of other NGI environments.

The System Security Administrators and System Administrators will be able to dynamically determine and reconfigure all resources available to each system environment without affecting the performance, availability, data confidentiality, and data integrity of another environment.

NGI shall support centralized control and display of system administration functions.

NGI shall support centralized control and display of system security administration functions.

NGI shall report system alarms to a centralized system administration display.

NGI will report alarms for various system thresholds (e.g., file system capacity, network traffic, server utilization).

NGI shall support an Authorized System Administrator initiating diagnostic testing of NGI or identified systems/functions.

NGI shall support an Authorized System Administrator initiating and controlling system data backup and restore functions.

NGI shall support an Authorized System Administrator initiating the start command for each component of the NGI system allowing for the orderly start of NGI operations.

NGI shall support an Authorized System Administrator initiating a shutdown command for each component of the NGI system allowing for the orderly shut down of NGI operations.

NGI shall support an Authorized System Administrator reallocating resources to level the processing workload.

NGI shall support an Authorized System Administrator changing transaction processing priorities.

NGI shall provide an Authorized System Administrator with the capability to cancel a transaction being processed, suspend a transaction, and redirect processing to another work queue.

The following functional requirements are specific to creation of new NGI repositories:

NGI shall allow an Authorized System Administrator to create a new NGI repository with no impact to NGI User Services.

NGI shall allow an Authorized System Administrator to create access rules for a new NGI repository.

NGI shall allow an Authorized System Administrator to create enrollment rules for a new NGI repository.

NGI shall allow an Authorized System Administrator to create dissemination rules for a new NGI repository.

NGI shall support automated scripts that daily check the availability of Shared Data processing servers.

NGI shall provide visual alarms to inform system operators or administrators of selected events or violations from the set of system parameters.

NGI shall support shared data terminals or workstations that provide direct access in a controlled environment.

3.7.5 Manage Workflow and Work Queues

The Manage Workflow function will be responsible for managing transactions through their complete processing cycle.

NGI shall provide an extensible workflow management capability.

NGI shall support the control, sequencing, management, input, and output of transactions that are processed as part of the workflow management function.

The workflow management capability will ensure transactions are processed in the appropriate manner and completed on a timely basis.

NGI shall provide a project work queue for staging transactions that have no response time requirements.

The NGI non-urgent response time will apply to these project work transactions once NGI inputs them into the workflow management function.

NGI shall allow an Authorized System Administrator to input transactions into the project work queue via multiple methods (e.g. CD, DVD, ftp).

NGI shall support the integration of new biometrics into the workflow management functions without negatively impacting existing NGI workflow.

NGI shall manage the processing of each transaction based on the transaction type and transaction processing rules.

NGI shall assign tasks to a work queue consistent with transaction processing rules.

Workgroup Loading will maximize productivity of NGI transaction processing. NGI will support rapid reassignment of work staff.

NGI shall allow an Authorized System Administrator the capability to adjust the rate of transactions input into NGI.

NGI shall collect data and statistics needed to support the management of work queues.

3.7.6 System Backup and Recovery

NGI backup and recovery functions will support System Administrator procedures to backup and recover system configurations, application software, and data. All NGI data and software necessary for recovery will be capable of being electronically backed-up on media that can be stored off-site. Recovery operations will be capable of providing partial restoration as well as complete NGI operational recovery.

NGI shall support the creation of backup data for NGI repository data.

NGI shall support the creation of backup data for NGI system files.

NGI shall support the creation of backup data for NGI application files.

NGI shall support the recovery of NGI repository data from backup files.

NGI shall support the recovery of NGI system files from backup files.

NGI shall support the recovery of NGI application files from backup files.

NGI shall provide core NGI services during backup operations.

NGI shall support export of backup data to removable media.

The NGI backup data will be stored off-site, in a storage facility having a controlled and secure environment. The storage site must be sufficiently removed from the primary NGI site so as not to expose it to the same risks that could disable the primary site.

3.7.7 System Interfaces and Communication Management

The System Interfaces and Communications Management function will support NGI communications with the other systems via various networks such as CJIS, NCIC, and Nlets. This function also identifies requirements for the management of the electronic communications internal to NGI.

NGI shall support an interface to NCIC in accordance with the III/NFF Operations and Technical Manual.

NGI shall support an interface to NCIC in accordance with the NCIC Operating Manual.

NGI shall support an interface to Nlets in accordance with the Nlets Users Guide.

NGI shall support an interface to the CJIS WAN in accordance with the latest EBTS version.

NGI shall support an interface to the Special Functions System.

NGI shall support an Internet interface for all NGI User Services.

NGI shall support a LEO interface for all NGI User Services.

NGI shall support an enhanced MRD interface for disposition processing.

NGI shall support an interface to external designated repositories in accordance with the latest EBTS version.

NGI shall support an interface to IDENT in accordance with the latest DHS/US-VISIT and DOJ/FBI Interoperability Interface Control Agreement.

NGI shall collect communications status information on external system interfaces.

NGI communication status information will include traffic flow, traffic status, line status, traffic

queuing, and communication error detection between the networks and NGI.

NGI shall report communications status of external system interfaces.

NGI shall collect communications status information on internal system interfaces.

NGI communication status information will include traffic flow, traffic status, traffic queuing, and communication error detection between the networks and NGI.

NGI shall report communications status of internal system interfaces.

3.7.8 System Training and Analysis Support

This section provides all functional requirements specific to the training and analysis support for the NGI.

NGI shall provide Authorized FBI Service Providers with Palmprint miss analysis tool capabilities.

NGI shall provide Authorized Contributors with palmprint information to support miss analysis tools.

NGI shall provide Authorized FBI Service Providers with fingerprint miss analysis tool capabilities.

NGI shall provide Authorized Contributors with fingerprint information to support miss analysis tools.

NGI shall provide Authorized FBI Service Providers with latent miss analysis tool capabilities.

NGI shall provide Authorized Contributors with latent information to support miss analysis tools.

NGI shall provide Authorized System Administrators with Subject Search miss analysis tool capabilities.

NGI shall provide Authorized FBI Service Providers with supplemental fingerprint and palmprint miss analysis tool capabilities.

NGI shall provide Authorized Contributors with supplemental fingerprint and palmprint information to support miss analysis tools.

NGI shall provide Authorized FBI Service Providers with iris miss analysis tool capabilities.

NGI shall provide Authorized Contributors with iris information to support miss analysis tools.

NGI shall provide Authorized FBI Service Providers with photo miss analysis tool capabilities.

NGI shall provide Authorized Contributors with photo information to support miss analysis tools.

NGI shall provide Authorized FBI Service Providers with training capabilities.

NGI shall provide Authorized FBI System Administrators with training capabilities.

3.7.9 Transaction History

The history records will be used to perform transaction audits and to generate statistical reports on NGI operations.

NGI shall collect transaction data for all transactions.

The routine transaction status data shall include transaction identification, status, and processing date/time.

NGI shall collect the processing history of all transactions.

NGI shall allow an Authorized FBI Service Provider access to transaction history data.

NGI shall allow an Authorized FBI Service Provider to view transaction history data.

NGI shall allow an Authorized FBI Service Provider to print transaction history data.

NGI will also provide access to the history records in order to generate statistical reports on NGI performance and activity.

NGI shall provide a centralized transaction history reporting service.

NGI shall allow an Authorized FBI Service Provider access to a centralized transaction history reporting service.

NGI shall provide the capability to generate statistical reports based on transaction history data.

NGI shall retain transaction history data.

NGI shall provide parameter-based transaction history reporting capabilities.

NGI shall provide pre-defined transaction history reporting capabilities.

NGI shall record the quality of fingerprints received as part of fingerprint transactions.

The following requirements apply to miss analysis tools.

NGI shall record the Fingerprint Investigation Search request information to support a fingerprint miss analysis tool.

Deleted.

NGI shall record the Iris Search request information to support an iris miss analysis tool.

NGI shall record the Facial Recognition Search request information to support a photo miss analysis tool.

NGI shall record the Latent Investigation Search request information to support a latent miss analysis tool.

Deleted.

NGI shall record Subject Search request information to support a Subject Search miss analysis tool.

The following requirements relate to biometric and biographic audit logs.

NGI shall record into a RISC audit log the dissemination of all RISC information.

NGI shall record into an ITF audit log the dissemination of all ITF information.

NGI shall provide the capability to identify which individual biometric information comprised the biometric composite at any specific time.

NGI shall record, into the biometric composite history log, information indicating which individual biometrics are included in the biometric composite when a biometric composite is created or updated.

NGI shall provide pre-defined biometric composite history log reporting capabilities

NGI shall allow an Authorized FBI Service Provider the capability to view the RISC audit log.

NGI shall allow an Authorized FBI Service Provider the capability to print the RISC audit log.

NGI shall record into a fingerprint audit log the dissemination of all fingerprint information.

The fingerprint audit log will include the disseminations of individual event fingerprints, as well as the dissemination of the composite and the individual fingerprints that make up the composite.

NGI shall record into an unsolved latent audit log the dissemination of all unsolved latent information.

NGI shall record statute maintenance requests in a statute maintenance audit log.

NGI shall record into a photo audit log the dissemination of all photos.

NGI shall record into a palmprint audit log the dissemination of all palmprints.

The palmprint audit log will include the disseminations of individual event palmprints, as well as the dissemination of the composite and the individual palmprints that make up the composite.

NGI shall record into a supplemental fingerprint and palmprint audit log the dissemination of all supplemental fingerprint and palmprint information.

The supplemental fingerprint and palmprint audit log will include the disseminations of individual supplemental fingerprint and palmprint images, as well as the dissemination of the composite and the individual supplemental fingerprint and palmprint images that make up the composite.

NGI shall record in an iris audit log the dissemination of all iris information

NGI shall support fingerprint statistical reporting.

NGI shall support RISC statistical reporting.

NGI shall support latent statistical reporting.

NGI shall support unsolved latent decision statistical reporting.

NGI shall support SPC File decision statistical reporting.

Deleted.

NGI shall have the capability to support fingerprint decision statistical reporting.

NGI shall support photo statistical reporting.

NGI shall support photo decision statistical reporting.

NGI shall support palmprint statistical reporting.

Deleted.

NGI shall support supplemental fingerprint and palmprint statistical reporting.

Deleted.

NGI shall support Identity statistical reporting.

NGI shall support Rap Back statistical reporting.

NGI shall support iris statistical reporting.

NGI shall support iris decision statistical reporting.

NGI shall support transaction statistical reporting.

NGI shall support fingerprint image quality statistical reporting of NGI Repositories.

NGI shall support latent print image quality statistical reporting of NGI Repositories.

NGI shall support supplemental fingerprint and palmprint image quality statistical reporting of NGI Repositories.

NGI shall support palmprint image quality statistical reporting of NGI Repositories.

NGI shall support iris image quality statistical reporting of NGI Repositories

NGI shall support photo image quality statistical reporting of NGI Repositories.

NGI shall support statistical reporting on external system links contained within NGI repositories.

NGI shall provide the capability to report to an External System (e.g., IDENT) on the biometrically-linked information associated with an Identity.

NGI shall support ITF statistical reporting.

NGI shall support ITF trend analysis reporting.

NGI shall provide parameter-based management information reporting capabilities.

NGI shall provide pre-defined management information reporting capabilities.

3.7.10 User Fee Billing Processing

NGI will collect user fee history data for NGI chargeable fingerprint and name search transactions. NGI will maintain administrative user fee data (tables, files, matrices) that support the calculation of user fees and generation of user fee bills. NGI will generate user fee bills and reports and provide capabilities to edit (correct) user fee bills.

NGI shall collect user fee history data.

NGI shall calculate user fees for each chargeable transaction based on user fee history data.

NGI shall allow Authorized FBI Service Providers access to user fee history, administrative, and billing data.

FBI Service Provider access to user fee history, administrative, and billing data will assist them in responding to user fee inquires from authorized user.

NGI shall provide the capability for Authorized FBI Service Providers to maintain (i.e., add, delete, and modify) user fee administrative data.

NGI shall provide the capability for Authorized FBI Services Providers to maintain user fee bills.

NGI shall assign a fee for each chargeable transaction.

NGI shall support the generation of user fee bills.

NGI shall provide the capability to generate hardcopy user fee bills.

NGI will provide the capability to generate hardcopy user fee bills for the FBI Finance Division.

NGI shall provide the capability to generate softcopy user fee bills.

NGI will provide the capability to generate softcopy (electronic) user fee bills for the FBI Finance Division.

NGI shall support generation of user fee reports.

NGI shall retain user fee billing history data.

NGI shall retain user fee administrative data.

NGI shall provide the capability to regenerate user fee bills.

3.7.11 Security

This section describes the NGI confidentiality, integrity, and availability requirements. NGI security requirements are based on the security policy, threats, and system configuration.

The security requirements described in this document provide a framework for the NGI.

3.7.11.1 Identification & Authentication

NGI shall uniquely identify and authenticate Direct Users or processes acting on behalf of users.

NGI shall identify and authenticate specific devices before establishing a connection.

NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by uniquely identifying each user.

NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by verifying the identity of each user.

NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by receiving authorization to issue a user identifier from an appropriate organizational official.

NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by ensuring that the user identifier is issued to the intended party.

NGI shall provide the capability for Authorized FBI System Administrators to manage Direct User identifiers by disabling user identifier after a period of inactivity defined in the System Security Plan.

NGI shall provide the capability for System Administrators to manage Direct User identifiers by archiving user identifiers.

NGI shall provide the capability for Authorized FBI System Administrators to manage information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by defining initial authenticator content.

NGI shall provide the capability for Authorized FBI System Administrators to manage information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.

NGI shall provide the capability for Authorized FBI System Administrators to manage information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by changing default authenticators upon information system installation.

NGI shall provide feedback to a Direct User during an attempted authentication and that feedback does not compromise the authentication mechanism.

3.7.11.2 Access Control

NGI shall provide capability for the FBI Administrator to manage NGI user accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

NGI shall provide the capability for the FBI Administrator to monitor NGI user accounts.

NGI Direct user privileges on the information system shall be consistent with the documented user authorizations.

NGI Indirect user privileges on the information system shall be consistent with the documented user authorizations.

NGI access list shall be restricted to, maintained by the system administrator or designated user account manager.

NGI controls shall be implemented to restrict a privileged user's system access to specific terminals when the need for such protection is identified in a risk analysis.

NGI access to security software shall be restricted to security administrators.

NGI separate libraries shall be maintained for program development and maintenance, testing, and production programs.

NGI source code shall be maintained in a separate library.

Access to all NGI programs, including production code, source code, and extra program copies, shall be protected by access control software and operating system features.

Direct users shall be assigned responsibilities and specific actions to ensure that access controls are implemented correctly.

Indirect users shall be assigned responsibilities and specific actions to ensure that access controls are implemented correctly.

Only specified, authorized, NGI personnel shall have access to the security functions and information of the information system.

Direct user privileges for accounts that have access to information security functions shall operate as documented in accordance with authorization requirements.

NGI shall enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

NGI shall enforce separation of duties.

NGI functions of significant criticality or sensitivity shall be subject to control by more than one individual.

No Direct user shall have access authorizations or privileges that may allow the user to perform multiple security functions for which the duties should be performed by separate people.

NGI shall not allow a single user to perform multiple functions/roles.

NGI specific actions and responsibilities shall be documented and defined to ensure that the principle of separation of duties is correctly applied within the information system.

NGI shall assign the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.

NGI shall ensure that access rights/privileges correspond to the authorized permissions on access documentation for the specified tasks.

NGI shall apply least privilege concepts in accordance with organizational policy and procedures.

NGI shall assign responsibilities and define specific actions to ensure that the principle of least privilege is correctly applied.

NGI shall enforce a limit of four consecutive invalid login attempts by a Direct user.

NGI shall automatically lock or disable the Direct user account when the maximum number of unsuccessful attempts is exceeded.

Attempts to login to an NGI Direct user account after it is locked or disabled shall fail.

An NGI System Administrator shall be assigned responsibility and have the capability to define specific actions to ensure that the information system enforces the limit on unsuccessful logon attempts and locks or disables the account when the limit is reached.

NGI shall display to the Direct User an FBI approved, system use notification message before granting system access informing potential users that the user is accessing a U.S. Government information system.

NGI shall display to the Direct User an FBI approved, system use notification message before granting system access informing potential users that system usage may be monitored, recorded, and subject to audit.

NGI shall display to the Direct User an FBI approved, system use notification message before granting system access informing potential users that unauthorized use of the system is prohibited and subject to criminal and civil penalties.

NGI shall display to the Direct User an FBI approved, system use notification message before granting system access informing potential users that use of the system indicates consent to monitoring and recording.

The NGI system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries).

The NGI system use notification message shall remain on the screen until the user takes explicit actions to log on to the information system.

NGI shall notify the Direct user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

NGI shall limit the number of concurrent sessions for any Direct user to 1 session only.

NGI shall prevent further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

NGI shall terminate a Direct user session after 30 minutes or less of inactivity.

Federal configuration standards may indentify stricter requirements based on the operating system environment.

NGI authentication tokens shall be destroyed when a session terminates.

Direct user web browsers shall have only session cookies enabled.

NGI shall assign responsibility and specific actions to Authorized FBI System Administrators defined to ensure that session terminations are implemented correctly within the information system.

NGI shall provide the capability for the FBI System Security Administrator to monitor and review the all user activities with respect to the enforcement and usage of information system access controls.

NGI shall provide the capability for the FBI System Security Administrator to identify specific user actions that can be performed on the information system without identification or authentication.

NGI shall control access to the system based on rules that restrict individual Direct Users according to their system defined roles or organizational membership and need-to-know requirements.

NGI shall prevent a requester from executing any process or function not specified in the requester's profile, or implicit in any roles or organizational memberships associated with the identifier.

No NGI Direct User will block other users from accessing resources.

No NGI Indirect User will block other users from accessing resources.

NGI shall prevent a requester from assuming any role not specified in the requester's profile, or implicit in any roles or organizational memberships associated with the identifier.

NGI shall provide transaction accountability for each Direct user activity on the system.

NGI shall provide transaction accountability for each Indirect user activity on the system.

NGI shall require that a response be first matched against an Indirect User message prior to sending the indirect user a response.

NGI shall provide an Administrator role to isolate administrative access.

3.7.11.3 Audit Accountability

NGI shall generate audit records for specific events (for example, account logon events, account management events, directory service access events, object access failures, policy change failures, privilege use failures, and system events.)

NGI shall produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

NGI shall allocate sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

In the event of an audit failure or audit storage capacity being reached, NGI shall alert appropriate organizational officials (by audible alert, email, or pager, as determined by local policy) and take the following additional actions: shutdown information system, and/or overwrite oldest audit records, and/or stop generating audit records.

NGI shall provide a warning when allocated audit record storage volume reaches 90% of capacity.

NGI shall provide the System Administrator with the necessary data to review/analyze inappropriate or unusual activity.

NGI shall provide the System Administrator with the necessary data to investigate suspicious activity or suspected violations.

NGI shall provide audit reduction and report generation capability.

NGI shall provide time stamps for use in audit record generation.

NGI shall protect audit information from unauthorized access, modification, and deletion.

NGI shall protect audit tools from unauthorized access, modification, and deletion.

NGI shall provide the capability to determine whether a given individual created information.

NGI shall provide the capability to determine whether a given individual sent a message.

NGI shall provide the capability to determine whether a given individual approved information [e.g., to indicate concurrence or sign a contract].

NGI shall provide the capability to determine whether a given individual received a message.

NGI shall have the capability to retain online audit logs for 30 days.

NGI shall have the capability to retain offline audit logs for 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

3.7.11.4 System & Communications Protection

NGI shall separate user functionality (including user interface services) from information system management functionality.

NGI shall isolate security functions from non-security functions.

NGI shall prevent unauthorized and unintended information transfer via shared system resources.

NGI shall protect against or limit the effects of hardware, software, or communications failures as denial of service attacks.

NGI shall protect against or limit the effects of the lack of communication bandwidth of web sites or internal networks as denial of service attacks.

NGI shall protect against or limit the effects of directed malicious attacks originating internally or externally to DOJ networks as denial of service attacks.

NGI shall limit the use of resources by priority.

NGI shall monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.

NGI shall protect the integrity of transmitted information.

NGI shall protect the confidentiality of transmitted information.

NGI shall terminate a network connection at the end of a session.

NGI shall establish a trusted communications path between the user and the security functionality of the system.

NGI shall employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

When cryptography is employed, NGI shall perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

NGI shall reliably associate security parameters (e.g., security labels and markings) with information exchanged between information systems.

NGI shall comply with organizational certificate policy and certification practice statement for the issuance of public key certificates.

NGI shall monitor the use of mobile code within the information system.

NGI shall control the use of mobile code within the information system.

Upon initial startup or recovery from an interruption in a CJIS criminal support systems [Target of Evaluation (TOE)] service, NGI shall not compromise its resources or those of any connected network.

3.7.11.5 Media Protection

NGI shall ensure that only authorized Direct users have access to information in printed form or on digital media removed from the information system.

NGI shall have external labels affixed to removable information storage media indicating the distribution limitations and handling caveats of the information.

NGI shall have external labels affixed to information system output indicating the distribution limitations and handling caveats of the information.

NGI shall sanitize information system digital media using approved equipment, techniques, and procedures.

NGI shall track media sanitization actions.

NGI shall document media sanitization actions.

NGI shall sanitize or destroy information system digital media before its disposal or release for reuse outside the organization.

3.7.11.6 Risk Assessment

NGI shall use DOJ-approved vulnerability scanning tools and techniques to routinely scan the operational system for vulnerabilities.

NGI shall support the use of DOJ-approved vulnerability scanning tools and techniques to scan the operational system when significant new vulnerabilities affecting the system are identified and reported.

3.7.11.7 System & Services Acquisition

NGI shall comply with software usage restrictions.

NGI shall enforce explicit rules governing the downloading and installation of software by users.

Deleted.

Deleted.

Deleted.

3.7.11.8 Configuration Management

NGI shall configure the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.

NGI shall allow the Administrators to configure NGI to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services:

FUNCTIONS <specified by system owner>

PORTS <specified by system owner>

PROTOCOLS <specified by system owner>

SERVICES <specified by system owner>

3.7.11.9 Contingency Planning

NGI shall conduct backups of user-level information contained in the information system within a component-defined time period.

NGI shall conduct backups of system-level information (including system state information) contained in the information system within a component-defined time period.

NGI shall store backup information at an appropriately secured location.

NGI shall employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

This Page Left Intentionally Blank.

4 OPERATIONAL REQUIREMENTS

This section describes the non-functional requirements, or general operational characteristics of the NGI as a whole.

4.1 Security

This section describes the NGI confidentiality, integrity, and availability requirements. NGI security requirements are based on the security policy, threats, and system configuration.

The security requirements described in this document provide a framework for the NGI.

Deleted.

4.1.1 Policy

NGI shall comply with the latest version of the CJIS Controlled Access Protection Profile (CAPP).

NGI shall comply with the DOJ Order 2640.2E dated November 28, 2003 "Information Security, Network and Computer Connection and Connections to Non-Department Entities".

NGI shall comply with the latest version of the CJIS Security Policy.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

4.1.2 Identification & Authentication

Deleted.

Deleted.

NGI Systems Security Functions [the TOE Security Functions (TSF)] shall use NIST FIPS 140-2 validated cryptography (methods and implementations) for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

NGI Security Functions shall provide cryptographic integrity mechanisms for TSF data while in transit to remote parts of the TOE.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

4.1.3 Access Control

Deleted.

Deleted.

Deleted.

Deleted.

NGI shall support the marking of output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

NGI information shall be appropriately labeled in storage, after processing, and after transmission in accordance with organizational policy and procedures.

NGI shall maintain all security labeling until changed by the appropriate personnel as determined by the data owner and all such changes are subject to audit.

Security labeling applies to all physical media and information system outputs (i.e. hardcopy or electronic).

NGI system configuration documentation shall explicitly define the security functions.

NGI access enforcement shall be consistently applied across the information system on an ongoing basis; any anomalies or problems encountered during access enforcement are being logged.

NGI separation of duties concepts shall be applied in accordance with organizational policy and procedures.

4.1.4 C&A and Security Assessments

Deleted.

Deleted.

An assessment of the NGI security controls shall be performed to determine the extent to which controls are implemented correctly.

An assessment of the NGI security controls shall be performed to determine the extent to which the controls are producing the desired outcome with respect to meeting the security requirements for the system.

NGI TSF shall provide authorized administrators with the necessary information for secure management.

NGI TSF shall provide authorized users with the necessary guidance for secure operations.

Deleted.

Deleted.

Deleted.

4.1.5 System & Communications Protection

Deleted.

NGI shall comply with organizational usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously.

NGI shall document the use of mobile code within the information system.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

Deleted.

4.1.6 Media Protection

Deleted.

Deleted.

Deleted.

Deleted.

NGI shall verify media sanitization actions.

NGI shall periodically test sanitization equipment/procedures to ensure correct performance.

4.1.7 Personnel Security

Deleted.

Deleted.

NGI shall comply with personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance with Department policy regarding minimum investigative requirements.

4.1.8 System & Services Acquisition

Deleted.

NGI shall design and implement the information system using security engineering principles.

NGI shall create a security test and evaluation plan.

NGI shall implement the security test and evaluation plan.

NGI shall document the results of the security test and evaluation plan which may be used in support of the security certification and accreditation process.

4.1.9 Configuration Management

Deleted.

NGI shall enforce access restrictions associated with changes to the information system.

4.1.10 Contingency Planning

Deleted.

NGI shall test and/or exercise the contingency plan for NGI using Department approved tests and exercises to determine the plan's effectiveness and the component's readiness to execute the plan.

NGI shall develop and implement a contingency plan for the information system addressing contingency roles, responsibilities, and activities associated with restoring the system after a disruption or failure.

4.2 Reliability

Reliability is the probability that a system will be able to process work correctly and completely without being aborted. Reliability is defined in terms of the system processing and biometric matching accuracy.

4.2.1 System Reliability

System reliability for NGI is the probability that the system will completely process all transactions under any condition.

NGI shall process all fingerprint transactions to completion.

NGI shall process all latent transactions to completion.

NGI shall process all Identity Management transactions to completion.

NGI shall process all Iris transactions to completion.

NGI shall process all Rap Back transactions to completion.

NGI shall process all Repository Management transactions to completion.

NGI shall process all disposition transactions to completion.

NGI shall process all photo transactions to completion.

NGI shall process all palmprint transactions to completion.

NGI shall process all supplemental fingerprint and palmprint transactions to completion.

NGI shall process all RISC transactions to completion.

NGI shall process all ITF transactions to completion.

NGI shall process all Rapid Tenprint Fingerprint Identification transactions to completion.

4.2.2 Accuracy

True Acceptance Rate (TAR) is the probability that the correct Identity will be selected as a candidate by the NGI provided that the Identity exists in the repository being searched. When operating in the verification task, TAR also equates to the percentage of times a system (correctly) verifies a true claim of Identity. False Acceptance Rate (FAR) is the rate of probability that the system incorrectly matches an Identity to another individual's existing Identity.

The following requirements apply to the automated fingerprint functions performed by the NGI system, independent of FBI Service Provider intervention. Candidates that are below the high confidence threshold will be provided to an FBI Service Provider for fingerprint image comparison.

NGI shall return the correct candidate a minimum of TAR=99.00% of the time, when it exists in the searched repository, as a result of a fingerprint feature search in support of fingerprint identification services.

NGI shall return an incorrect candidate a maximum of FAR=.0030 of the time, as a result of a fingerprint feature search in support of fingerprint identification services.

The following requirements apply to NGI verification services and III/Verify. Candidates that are below the high confidence threshold will be provided to an FBI Service Provider for fingerprint image comparison; however, the following rates represent performance without FBI Service Provider intervention.

NGI shall correctly verify the candidate at TAR=99.99% for a two finger comparison.

NGI shall correctly verify the candidate at TAR=99.25% for a single finger comparison.

NGI shall provide the incorrect candidate to III/Verify a maximum of FAR=0.2000.

The following requirements apply to RISC Rapid Searches. The candidates will be returned with no FBI Service Provider intervention.

NGI shall return the correct candidate a minimum of 98% of the time, when it exists in the RISC repository, as a result of a fingerprint feature search in support of RISC Rapid Searches.

NGI shall return an incorrect candidate a maximum of 5% of the time, as a result of a fingerprint feature search of the RISC Repository in support of RISC Rapid Searches.

The following requirements apply to the automated fingerprint functions performed by the NGI system in support of investigation services. The candidates will be returned with no FBI Service Provider intervention.

NGI shall return the correct candidate a minimum of 99% of the time, when it exists in the searched repository, as a result of a fingerprint feature search in support of fingerprint investigation services.

NGI shall return an incorrect candidate a maximum of 2% of the time, as a result of a fingerprint feature search in support of fingerprint investigation services.

Deleted.

Deleted.

NGI shall return the correct candidate a minimum of 85% of the time, when it exists in the searched repository, as a result of a facial recognition search in support of photo investigation services.

NGI shall return an incorrect candidate a maximum of 20% of the time, as a result of facial recognition search in support of photo investigation services.

NGI shall return the correct candidate a minimum of 98% of the time, when it exists in the searched repository, as a result of a iris search in support of iris investigation services.

NGI shall return an incorrect candidate a maximum of 10% of the time, as a result of an iris search in support of iris investigation services.

The following requirements apply to latent searches.

NGI shall return the correct candidate within the top ten positions a minimum of 75% of the time, when it exists in the searched repository, as a result of a feature search in support of latent investigation services.

The following requirements apply to cascaded searches of the unsolved biometric files.

NGI shall return the correct candidate a minimum of 75% of the time, when it exists in the ULF, as a result of a cascaded fingerprint search of the ULF.

NGI shall return an incorrect candidate no more than 0.02% of the time (FMR=0.0002) as a result of a cascaded fingerprint search of the ULF.

The cascaded fingerprint search of the ULF also includes palmprints and Supplemental Fingerprint and Palmprint.

NGI shall return the correct candidate a minimum of 75% of the time, when it exists in the UPF, as a result of a cascaded facial recognition search of the UPF.

NGI shall return the correct candidate a minimum of 75% of the time, when it exists in the UIF, as a result of a cascaded iris search of the UIF.

The following requirements apply to cascaded searches of the marked SPC files.

NGI shall return the correct candidate a minimum of 95% of the time, when it exists in the SPC File, as a result of a cascaded fingerprint search of an SPC File.

The cascaded fingerprint search of an SPC File also includes palmprints and Supplemental Fingerprint and Palmprint.

NGI shall return the correct candidate a minimum of 95% of the time, when it exists in the SPC File, as a result of a cascaded facial recognition search of an SPC File.

NGI shall return the correct candidate a minimum of 95% of the time, when it exists in the SPC File, as a result of a cascaded iris search of an SPC File.

The following requirements apply to Rapid Tenprint Fingerprint Indentification Searches. The candidates will be returned with no FBI Service Provider intervention.

NGI shall return the correct candidate a minimum of 98% of the time, when it exists in the searched repository, as a result of a fingerprint feature search in support of Rapid Tenprint Fingerprint Identification Searches.

NGI shall return an incorrect candidate a maximum of 5% of the time, as a result of a fingerprint feature search of the searched repository in support of Rapid Tenprint Fingerprint Identification Searches.

4.3 System Availability

System availability is the time when the application must be available for use. Required system availability is used in determining when maintenance may be performed.

4.3.1 NGI Availability

NGI shall provide functional support 24 hours a day, seven days a week.

NGI shall provide 99.7% availability, per quarter, in support of all user services except RISC Rapid Search capabilities.

NGI shall provide 99.95% availability, per quarter, in support of all International Terrorist Identification Search requests.

NGI shall provide 99.95% availability, per quarter, in support of all RISC Rapid Search capabilities.

NGI shall provide 99% availability, per month, in support of all Shared Data capabilities.

NGI shall provide the capability to perform back up activities with no impact to NGI User Services.

NGI shall provide a secure, prioritized, and highly available communications interface for authorized External Systems.

4.3.2 Disaster Recovery

NGI may operate in a disaster recovery mode when primary site services are no longer available. NGI may operate with degraded response times during periods when the secondary repositories are being

utilized.

NGI shall support disaster recovery of all NGI data.

NGI shall support disaster recovery for each of the NGI repositories to support critical user services.

NGI shall support secondary repositories that are synchronized copies of the NGI primary repositories.

NGI shall support secondary repositories that are capable of being geographically separated from the NGI primary repositories.

NGI shall provide a data replication from the NGI primary repositories to the secondary repositories with no more than a fifteen minute delta between primary and secondary repositories.

NGI shall support fail-over capabilities between the primary and secondary NGI repositories.

4.4 Supportability/Maintainability

This section includes any non functional requirement that enhances the supportability or maintainability of the system being built, including maintenance access, maintenance utilities, maintenance schedules, or architectural considerations required to provide for long term ease of maintenance.

4.4.1 Support Multiple System Environments

NGI must have the capability to concurrently support the system environments defined below:

- Operational: NGI operating in its normal configuration with complete data integrity and availability of all segments to normal users, service providers, and operators.
- Non-Operational Test: NGI operating with a separate subset of data that is unavailable to normal system users while providing segment and system test capabilities.
- Non-Operational Development: NGI operating with a separate subset of data that is unavailable to normal system users while providing segment development and maintenance.

NGI shall provide the capability to concurrently support multiple system environments (i.e., operational, testing, development).

NGI shall be able to perform system maintenance functions without negatively impacting the ability of NGI to meet availability requirements.

NGI shall support the routine system maintenance without negatively impacting services to an External System (e.g., IDENT).

NGI will ensure that the performance, availability, data confidentiality, and data integrity of the operational environment are not compromised.

NGI shall provide a test environment that supports the development of new hardware and software and the execution of operational tests and evaluations.

NGI shall provide a development system environment that supports the development of new hardware and software and the execution of operational tests and evaluations.

The test and development environment will support assessment of NGI operational effectiveness and operational suitability.

NGI shall comply with Section 508 of the Rehabilitation Act (29 USC 794d) for all system components, including but not limited to developed software, COTS and hardware.

4.4.2 Support NGI Diagnostic Tools

NGI shall support fingerprint diagnostic tools for all environments (i.e., operational, test, development).

NGI shall support fingerprint accuracy tests without impacting the ability of NGI to meet performance requirements.

NGI will support accuracy tests before and after the implementation of system changes to validate NGI TAR and FAR requirements.

NGI shall support fingerprint development and test tools.

NGI shall support latent diagnostic tools for all environments (i.e., operational, test, development).

NGI shall be capable of performing latent accuracy tests without impacting the ability of NGI to meet performance requirements.

NGI shall support latent development and test tools.

NGI shall support data management processing diagnostic tools for all environments (i.e., operational, test, development).

NGI shall support electronic disposition submission development and test tools.

NGI shall support Photo development and test tools.

NGI shall support Photo diagnostic tools for all environments (i.e., operational, test, development).

NGI shall be capable of performing Photo Facial Recognition accuracy tests without impacting performance requirements for other NGI services.

NGI shall support Palmprint diagnostic tools for all environments (i.e., operational, test, development).

NGI shall support supplemental fingerprint and palmprint diagnostic tools for all environments (i.e., operational, test, development).

NGI shall be capable of performing Palmprint Search Accuracy tests without impacting performance requirements for other NGI services.

Deleted.

NGI shall support Palmprint development and test tools.

NGI shall support Supplemental Fingerprint and Palmprint development and test tools.

NGI shall support Iris diagnostic tools for all environments (i.e., operational, test, development).

NGI shall be capable of performing Iris search accuracy tests without impacting performance requirements for other NGI services.

NGI shall support Iris development and test tools.

NGI shall support Rap Back diagnostic tools for all environments (i.e., operational, test, development).

NGI shall support Rap Back development and test tools.

NGI shall support repository management diagnostic tools for all environments (i.e., operational, test, development).

NGI shall support diagnostic tools to test access to external repositories for all environments (i.e., operational, test, development).

NGI shall support repository management development and test tools.

4.4.3 Support NGI Workstations

4.4.3.1 Support Staff Organization

NGI shall support a sufficient number of NGI workstations to maintain 24 hours per day, seven days per week operations.

4.4.3.2 Support Fingerprint Processing Workstations

NGI shall support all fingerprint functions using an NGI workstation.

NGI shall support all ITF functions using an NGI workstation.

NGI workstations will be capable of supporting fingerprint functionality that includes, but is not limited to:

- The capability to support devices compliant with HSPD-12 and FIPS 201.
- Image enhancement capabilities such as zooming, panning, contrast, and color.
- Fingerprint processing for searching against the Tenprint data files.
- The capability to display magnified fingerprint images.
- The capability to enter different search parameters for searching the Tenprint data files.

- The capability to review candidate lists and fingerprint images.
- The capability to classify fingerprints with the assistance of automated aids.
- The capability to display fingerprint images for comparison.
- The capability to apply compression and decompression algorithms.
- The capability to print images.

4.4.3.3 Support Latent Processing Workstation

NGI shall support all latent functions using an NGI workstation.

NGI shall provide the capability for FBI Service Providers to overlay features on images from an NGI latent workstation.

NGI workstations will be capable of supporting latent functionality that includes, but is not limited to:

- The capability to support devices compliant with HSPD-12 and FIPS 201.
- The capability to input Latent Fingerprint submissions at no less than 1000 pixels per inch (ppi) and 256 shades of gray.
- The capability to import latent fingerprint search images from removable media (e.g., CD, DVD).
- The capability to automatically and/or manually extract fingerprint features.
- The capability to classify fingerprints.
- A comprehensive digital image processing capability, such as to extract, identify, plot, and format ridge structure information.
- The capability to initiate fingerprint processing by performing Subject Searches and ad hoc inquiries.
- The capability to search against the latent cognizant files, unsolved latent image files, unsolved latent features files, and special files.
- The capability to save fingerprint features.
- The capability to review candidate lists and fingerprint images.
- The capability to display magnified fingerprint images for comparison.
- The capability to overlay drawings, notations, and marks to images.
- The capability to toggle on/off the feature overlay.
- The capability to print out the search fingerprint image and the candidate fingerprint image in actual size or enlarged with and without drawings, notations, and marks.
- The capability to save the search fingerprint image and the candidate fingerprint images in a digital format (e.g., jpeg, bmp, tiff).
- The capability to print images at the workstation or within the workgroup.
- Signal processing functions to reduce noise, clarify ridges, and help eliminate false fingerprint features.
- The capability to apply compression and decompression algorithms.
- Screen display times that do not have a negative impact on Authorized FBI Service Providers' capability to perform Latent Functions.

4.4.3.4 Support Data Management Services Workstation

NGI shall support all data management processing functions using an NGI workstation.

NGI workstations will be capable of supporting the following data management processing functionality:

- The capability to support devices compliant with HSPD-12 and FIPS 201.
- The capability to display the document data on the workstation monitor in sufficient detail to allow easy reading of the text.
- The capability to zoom on the whole document or a portion of the document.
- The capability to enhance poor images.
- The capability to apply compression and decompression algorithms.
- The capability to provide screen displays in data entry request format and text editing capabilities to minimize data entry errors.
- The capability to verify/validate the correctness of entered data and the presence of insufficient data and to generate appropriate notification to the service provider.
-

NGI shall be capable of performing the conflict resolution service for disposition transactions on an NGI workstation.

4.4.3.5 Support Photo Functions using NGI Workstations

NGI shall be capable of performing all Photo functions on an NGI workstation.

4.4.3.6 Support Palmprint Functions using NGI Workstations

NGI shall be capable of performing all Palmprint functions on an NGI workstation.

NGI shall be capable of performing all supplemental fingerprint and palmprint functions on an NGI workstation.

4.4.3.7 Support Iris Functions using NGI Workstations

NGI shall be capable of performing all Iris functions on an NGI workstation.

4.4.3.8 Support Rap Back using NGI Workstations

NGI shall be capable of performing all Rap Back functions on an NGI workstation.

4.4.3.9 Support Repository Management using NGI Workstations

NGI shall be capable of performing all repository management functions on an NGI workstation.

4.4.4 Support NGI Search Algorithms

NGI shall support the capability to replace the fingerprint search algorithms with no impact to NGI User Services.

NGI shall support the capability to replace the facial recognition search algorithms with no impact to NGI User Services.

NGI shall support the capability to replace the palmprint search algorithms with no impact to NGI User Services.

NGI shall support the capability to replace the supplemental fingerprint and palmprint search algorithms with no impact to NGI User Services.

NGI shall support the capability to replace the iris search algorithms with no impact to NGI User Services.

NGI shall support a fingerprint feature set solution that is publicly available.

4.4.5 Support Repository Management

NGI shall support enrollment rule management tools.

NGI shall support dissemination rule management tools.

NGI shall capable of performing inter-repository Identity consolidation searches without impacting performance requirements for other NGI services.

NGI shall be capable of performing intra-repository Identity consolidation searches without impacting performance requirements for other NGI services.

NGI shall provide a scalable repository.

NGI shall provide an extensible repository.

NGI will be capable of adding new biometrics without impacting the existing NGI repository infrastructure.

4.5 System Performance

System Performance includes non-functional requirements for response time for queries and updates, throughput, expected volume of data, and the expected volume of user activity (e.g., number of transactions during a specific time period).

4.5.1 Fingerprint Response Times

NGI shall respond to a high priority criminal Fingerprint Identification Search within ten minutes after receipt by NGI.

NGI shall respond to a routine priority criminal Fingerprint Identification Search within 30 minutes after receipt by NGI.

NGI shall respond to a low priority criminal Fingerprint Identification Search within 24 hours after receipt by NGI.

NGI shall respond to a non-urgent criminal Fingerprint Identification Search within 15 days after receipt by NGI.

NGI shall respond to a high priority civil Fingerprint Identification Search within 15 minutes after receipt by NGI.

NGI shall respond to a routine priority civil Fingerprint Identification Search within two hours after receipt by NGI.

NGI shall respond to a low priority civil Fingerprint Identification Search within 24 hours after receipt by NGI.

NGI shall respond to a non-urgent civil Fingerprint Identification Search within 15 days after receipt by NGI.

NGI shall respond to 99% of RISC Rapid Searches received during any continuous 24-hour period within within ten seconds after receipt by NGI when no additional Identity information is requested.

NGI shall respond to 99.9% of RISC Rapid Searches received during any continuous 24-hour period within seventeen seconds after receipt by NGI when no additional Identity information is requested.

NGI shall respond to 99% of RISC Rapid Searches received during any continuous 24-hour period within 20 seconds after receipt by NGI when additional Identity information is requested.

NGI shall respond to 99.9% of RISC Rapid Searches received during any continuous 24-hour period within twenty-seven seconds after receipt by NGI when additional Identity information is requested.

NGI shall respond to RISC Maintenance requests within 15 minutes after receipt by NGI.

NGI shall respond to an International Terrorist Identification Search within 15 minutes after receipt by NGI.

NGI shall respond to an International Terrorist File Maintenance request within 15 minutes after receipt by NGI.

NGI shall respond to a high priority Fingerprint Investigation Search within 30 seconds after receipt by NGI.

NGI shall respond to a routine priority Fingerprint Investigation Search within two minutes after receipt by NGI.

NGI shall respond to a low priority Fingerprint Investigation Search within 30 minutes after receipt by NGI.

NGI shall respond to a Fingerprint Verification request within 15 minutes after receipt by NGI.

NGI shall respond to a Fingerprint Image Retrieval request for a single UCN within five minutes after receipt by NGI.

NGI shall respond to a Fingerprint Image Retrieval request for up to 1000 UCNs within 48 hours after receipt by NGI.

NGI shall respond to a Fingerprint Audit Trail Retrieval request within 15 minutes after receipt by NGI.

NGI shall perform a fingerprint maintenance request within 15 minutes after receipt by NGI.

Fingerprint maintenance applies to direct fingerprint enrollments, fingerprint image replacements, and fingerprint deletions.

NGI shall complete a cascaded fingerprint search within 24 hours of NGI completing the original request on average.

NGI shall respond to a Rapid Tenprint Fingerprint Identification Search within 10 seconds on average, after receipt by NGI, on a daily basis.

4.5.2 Latent Response Times

NGI shall respond to a high priority Latent Search within a one hour average measured over a 24 hour period after receipt by NGI.

NGI shall respond to a routine priority Latent Search within four hours after receipt by NGI.

NGI shall respond to a low priority Latent Search within 24 hours after receipt by NGI.

NGI shall respond to a Latent Audit Trail Retrieval request within 15 minutes after receipt by NGI.

NGI shall send an External Latent Print Search request to an External System (e.g., IDENT) within 15 minutes of NGI receiving the request.

4.5.3 Identity History Response Times

NGI shall respond to a III Subject Search request within one second after receipt by NGI.

NGI shall respond to a III Identity History request within one second after receipt by NGI.

NGI shall respond to an Ad Hoc Subject Search request within two minutes after receipt by NGI.

NGI shall send an Identification Search request to Authorized External Systems (e.g., IDENT) for all newly enrolled Identities within 15 minutes following the NGI enrollment.

4.5.4 Photo Response Times

NGI shall respond to a Facial Recognition Search request within two hours after receipt by NGI.

NGI shall respond to a Text-Based Facial Photo Search request within 15 minutes after receipt by NGI.

NGI shall respond to a Text-Based SMT Photo Search request within 15 minutes after receipt by NGI.

NGI shall respond to a Photo Image Retrieval request for a single UCN within five minutes after receipt by NGI.

NGI shall respond to a Photo Features Retrieval request for a single UCN within five minutes after receipt by NGI.

NGI shall respond to a Photo Audit Trail Retrieval request within 15 minutes after receipt by NGI.

NGI shall perform a Photo Maintenance request within 15 minutes after receipt by NGI.

Photo maintenance applies to direct Photo enrollments and Photo deletions.

NGI shall send an External Photo Image Retrieval request to an External System within 15 minutes of NGI receiving the request.

NGI shall complete a cascaded Facial Recognition Search within 24 hours of NGI completing the original request.

4.5.5 Palmprint Response Times

Deleted.

NGI shall respond to a Palmprint Image Retrieval request for a single UCN within five minutes after receipt by NGI.

NGI shall respond to a Palmprint Feature Retrieval request for a single UCN within five minutes after receipt by NGI.

NGI shall respond to a Palmprint Audit Trail Retrieval request within 15 minutes after receipt by NGI.

NGI shall perform a Palmprint Maintenance request within 15 minutes after receipt by NGI.

Palmprint maintenance applies to direct Palmprint enrollments and Palmprint deletions.

NGI shall complete a cascaded Palmprint Search within 24 hours of NGI completing the original request.

4.5.6 Iris Response Times

NGI shall respond to an Iris Search request within two hours after receipt by NGI.

NGI shall respond to an Iris Image Retrieval request for a single UCN within five minutes after receipt by NGI.

NGI shall respond to an Iris Features Retrieval request for a single UCN within five minutes after receipt by NGI.

NGI shall respond to an Iris Audit Trail Retrieval request within 15 minutes after receipt by NGI.

NGI shall perform an Iris Maintenance request within 15 minutes after receipt by NGI.

Iris maintenance applies to direct Iris enrollments and Iris deletions.

NGI shall complete a cascaded Iris Search within 24 hours of NGI completing the original request.

4.5.7 Supplemental Fingerprint and Palmprint Response Times

Deleted.

NGI shall perform Supplemental Fingerprint and Palmprint Maintenance for a single UCN request within 15 minutes after receipt by NGI.

Supplemental fingerprint and palmprint maintenance applies to direct Supplemental Fingerprint and Palmprint enrollments, and Supplemental Fingerprint and Palmprint deletions.

NGI shall complete a cascaded Supplemental Fingerprint and Palmprint Search within 24 hours of NGI completing the original request.

4.5.8 Rap Back Response Times

NGI shall respond to Rap Back Subscription List Retrieval within 15 minutes after receipt by NGI.

NGI shall perform a Direct Rap Back Enrollment within 15 minutes after receipt by NGI.

NGI shall perform Rap Back Maintenance requests for a single UCN within 15 minutes after receipt by NGI.

4.5.9 Disposition Response Times

NGI shall respond to a Disposition Fingerprint Search within 24 hours after the receipt by NGI.

NGI shall respond to a NCIC Disposition Submission request within five seconds after the receipt by NGI.

NGI shall respond to an EBTS Disposition Submission request within 24 hours after the receipt by NGI.

NGI shall respond to an NCIC Disposition Maintenance request within five seconds after the receipt by NGI.

NGI shall respond to an EBTS Disposition Maintenance request within 24 hours after the receipt by NGI.

4.5.10 Link Maintenance Completion Response Times

NGI shall complete all Link Maintenance requests received from an Authorized External System within 15 minutes of NGI receiving the maintenance request.

4.5.11 Notification Response Times

NGI shall provide all Notifications within five minutes after completion of the triggering event.

This applies to all notifications detailed in the Notification Services Functional Requirements Section of this document.

4.5.12 Shared Data Response Times

NGI shall respond to a criminal Tenprint Fingerprint Identification Search of the Shared Data records within two hours after receipt.

NGI shall respond to a civil Tenprint Fingerprint Identification Search of the Shared Data records within twenty four hours after receipt by NGI.

NGI shall provide a response to a Shared Data search within the required time allotment 95% of the time measured over a month for the end-user, not including the LESC response time.

NGI shall provide the results of the Shared Data post processing (QA) on all positive identifications against the Shared Data records within 24 hours.

4.6 Workload

Workload capacity is defined as the capability of a system to handle expected data volume. For the purpose of this document, capacity requirements are stated in terms of the business and not in terms of system memory requirements or disk space.

4.6.1 Support Fingerprint Processing Workload

NGI shall be capable of meeting the estimated yearly fingerprint workloads contained in Table 4-1a.

NGI shall be capable of meeting the estimated average daily fingerprint workloads contained in Table 4-1b.

NGI shall be capable of meeting the estimated average hourly fingerprint workloads contained in Table 4-1c.

NGI shall be capable of meeting the estimated peak hourly fingerprint workloads contained in Table 4-1d.

The following are the assumptions used to support the development of the Fingerprint Workload Estimates depicted in Tables 4-1a, 4-1b, 4-1c, and 4-1d below.

- Criminal and Civil fingerprint workloads are based on the IISS Capacity Planning estimates from June 2008 and US-Visit Transaction Volume Spreadsheet (TVS) Version 4.2.
- NGI Verification searches are based on combined 1% Criminal and Civil workload (excluding special projects) and 1% NCIC Persons searches (assumed at 500,000 per day).
- Civil workload includes Identity Theft Victim File submissions that are estimated to be 25% increasing increments of the NCIC Identity Theft enrollments (MKE=EID).
- RISC Rapid searches are based on estimates established for the RISC Rapid Prototype for FY2008 with yearly incremental growth.
- RISC International Terrorist File (ITF) Identification searches are based on 10% of the RISC Rapid Search projections.
- Fingerprint Image and Feature requests are based upon historical NGI activity.
- Audit Trail Retrieval requests are estimated at 0.1% of the Image Retrieval requests per day.
- Fingerprint Deletion and Replacement requests are based upon historical NGI activity.
- Fingerprint Decision requests are estimated to be minimal, and will not substantially add to the fingerprint maintenance file.
- New NGI Repository infrastructure and functionality will be deployed in the Fiscal Year 2009.

- Direct Fingerprint Enrollments for FY2006-FY2008 reflect current Special Latent Cognizant workloads, NGI SRD Table 4-2.
- Direct Fingerprint Enrollments for FY2009-FY2012 are based on 10% growth each year.

Table 4-1a Yearly Fingerprint Workload Estimates

Yearly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services	**35,652,637**	**48,215,815**	**84,868,400**	**102,454,646**	**109,155,013**	**121,871,848**	**138,115,962**	**141,975,185**	**154,419,582**
Criminal Ten-Print	**15,401,138**	**22,215,773**	**54,440,794**	**56,317,137**	**58,400,121**	**60,713,344**	**63,283,130**	**66,138,851**	**69,313,280**
High Priority	804,372	3,420,050	3,905,938	4,062,175	4,224,661	4,393,648	4,569,394	4,752,170	4,942,256
Routine Priority	14,188,228	13,224,233	14,764,856	16,484,962	18,405,460	20,549,696	22,943,736	25,616,681	28,601,024
Low Priority	26,000	21,000	0	0	0	0	0	0	0
Non-Urgent	382,538	5,550,490	35,770,000	35,770,000	35,770,000	35,770,000	35,770,000	35,770,000	35,770,000
Rolled	*100%*	*66%*	*29%*	*32%*	*34%*	*36%*	*39%*	*41%*	*44%*
Flat	*0%*	*34%*	*71%*	*68%*	*66%*	*64%*	*61%*	*59%*	*56%*
Civil Ten-Print	**20,251,499**	**25,854,042**	**30,281,606**	**44,312,510**	**47,104,892**	**52,033,504**	**56,582,832**	**53,753,834**	**60,815,552**
High Priority	694,530	10,848,530	13,428,671	14,732,318	16,164,761	17,738,816	19,468,581	21,369,557	23,458,796
Routine Priority	16,417,099	10,892,067	12,772,354	15,993,292	16,735,136	19,330,947	22,324,706	25,800,802	29,818,160
Low Priority	2,639,870	2,750,525	3,001,931	3,238,586	3,519,605	3,857,002	3,156,124	3,291,699	3,423,878
Non-Urgent	500,000	1,362,920	1,078,650	10,348,313	10,685,391	11,106,738	11,633,422	3,291,776	4,114,718
Rolled	*85%*	*46%*	*44%*	*58%*	*56%*	*56%*	*56%*	*48%*	*49%*
Flat	*15%*	*54%*	*56%*	*42%*	*44%*	*44%*	*44%*	*52%*	*51%*
Sub-Total Ten-Print Identification Services	***35,652,637***	***48,069,815***	***84,722,400***	***100,629,646***	***105,505,013***	***112,746,848***	***119,865,962***	***119,892,685***	***130,128,832***
Criminal Rapid Searches	0	0	0	0	0	0	0	0	0
RISC Rapid Searches	0	146,000	146,000	1,825,000	3,650,000	9,125,000	18,250,000	20,075,000	22,082,500
RISC ITF Searches	0	0	0	0	0	0	0	2,007,500	2,208,250
Verification Services	**0**	**0**	**0**	**0**	**0**	**0**	**226,335**	**257,078**	**292,084**
Investigative Services	**2,822,910**	**2,863,100**	**2,977,566**	**3,096,806**	**34,974,114**	**37,867,397**	**39,382,867**	**40,958,994**	**42,598,207**
High Priority	986,960	1,026,380	1,067,260	1,109,965	32,907,670	35,655,025	37,081,226	38,564,475	40,107,054
Routine Priority	1,825,000	1,825,000	1,898,000	1,973,920	2,052,877	2,134,992	2,220,392	2,309,208	2,401,576
Low Priority	10,950	11,720	12,306	12,921	13,567	77,380	81,249	85,311	89,577
Information Services	**1,627,900**	**1,953,480**	**2,344,176**	**2,813,011**	**3,375,613**	**4,050,736**	**4,865,243**	**5,838,291**	**7,005,950**
Fingerprint Image Retrievals	1,481,900	1,778,280	2,133,936	2,560,723	3,072,868	3,687,441	4,424,930	5,309,916	6,371,899
Fingerprint Features Request	146,000	175,200	210,240	252,288	302,746	363,295	435,954	523,144	627,773
Fingerprint Audit Trail Requests	0	0	0	0	0	0	4,360	5,231	6,278
Data Management Services	**395,368**	**461,526**	**605,732**	**1,189,860**	**3,330,306**	**3,933,149**	**4,650,501**	**5,506,475**	**6,528,455**
Fingerprint Delete Requests (events)	375,220	402,595	431,795	463,185	496,765	532,900	570,203	610,117	652,825
Fingerprint Image Replacement	20,148	58,931	173,937	726,675	2,833,541	3,400,249	4,080,298	4,896,358	5,875,630
Direct Fingerprint Enrollment (SPC File ONLY)	30,000	30,000	33,000	36,300	39,930	43,923	48,315	53,147	58,462

Table 4-1b Average Daily Fingerprint Workload Estimates

Average Daily	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services	97,682	132,101	232,519	280,701	299,058	333,899	378,402	388,976	423,070
Criminal Ten-Print	42,197	60,866	149,154	154,295	160,001	166,339	173,379	181,203	189,900
High Priority	2,204	9,370	10,702	11,130	11,575	12,038	12,519	13,020	13,541
Routine Priority	38,872	36,231	40,452	45,165	50,426	56,301	62,860	70,183	78,359
Low Priority	72	58	0	0	0	0	0	0	0
Non-Urgent	1,049	15,207	98,000	98,000	98,000	98,000	98,000	98,000	98,000
Civil Ten-Print	55,485	70,835	82,965	121,406	129,057	142,560	155,023	147,273	166,620
High Priority	1,903	29,722	36,791	40,363	44,288	48,600	53,339	58,547	64,271
Routine Priority	44,979	29,842	34,993	43,818	45,850	52,962	61,164	70,688	81,694
Low Priority	7,233	7,536	8,225	8,873	9,643	10,568	8,647	9,019	9,381
Non-Urgent	1,370	3,735	2,956	28,352	29,276	30,430	31,873	9,019	11,274
Sub-Total Ten-Print Identification Services	*97,682*	*131,701*	*232,119*	*275,701*	*289,058*	*308,899*	*328,402*	*328,476*	*356,520*
Criminal Rapid Searches	0	0	0	0	0	0	0	0	0
RISC Rapid Searches	0	400	400	5,000	10,000	25,000	50,000	55,000	60,500
RISC ITF Searches	0	0	0	0	0	0	0	5,500	6,050
Verification Services	0	0	0	0	0	0	621	705	801
Investigative Services	7,734	7,845	8,158	8,485	95,821	103,747	107,900	112,218	116,709
High Priority	2,704	2,812	2,924	3,041	90,158	97,685	101,593	105,657	109,883
Routine Priority	5,000	5,000	5,200	5,408	5,625	5,850	6,084	6,327	6,580
Low Priority	30	33	34	36	38	212	223	234	246
Information Services	4,460	5,352	6,423	7,708	9,249	11,099	13,331	15,997	19,196
Fingerprint Image Retrievals	4,060	4,872	5,847	7,016	8,419	10,103	12,124	14,548	17,458
Fingerprint Features Request	400	480	576	692	830	996	1,195	1,434	1,720
Fingerprint Audit Trail Requests	0	0	0	0	0	0	12	15	18
Data Management Services	1,083	1,264	1,660	3,260	9,124	10,776	12,741	15,086	17,886
Fingerprint Delete Requests	1,028	1,103	1,183	1,269	1,361	1,460	1,562	1,672	1,789
Fingerprint Image Replacement	55	161	477	1,991	7,763	9,316	11,179	13,415	16,098
Direct Fingerprint Enrollment (SPC File ONLY)	82	82	90	99	109	120	132	146	160

Table 4-1c Average Hourly Fingerprint Workload Estimates

Average Hourly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services	4,070	5,504	9,689	11,696	12,460	13,913	15,766	16,207	17,628
Criminal Ten-Print	1,759	2,536	6,215	6,429	6,666	6,931	7,224	7,550	7,912
High Priority	92	390	446	464	482	502	522	543	564
Routine Priority	1,620	1,510	1,686	1,882	2,101	2,346	2,619	2,924	3,265
Low Priority	3	2	0	0	0	0	0	0	0
Non-Urgent	44	634	4,083	4,083	4,083	4,083	4,083	4,083	4,083
Civil Ten-Print	2,311	2,951	3,457	5,059	5,377	5,940	6,459	6,136	6,943
High Priority	79	1,238	1,533	1,682	1,845	2,025	2,222	2,439	2,678
Routine Priority	1,874	1,243	1,458	1,826	1,910	2,207	2,549	2,945	3,404
Low Priority	301	314	343	370	402	440	360	376	391
Non-Urgent	57	156	123	1,181	1,220	1,268	1,328	376	470
Sub-Total Ten-Print Identification Services	*4,070*	*5,487*	*9,672*	*11,488*	*12,043*	*12,871*	*13,683*	*13,686*	*14,855*
Criminal Rapid Searches	0	0	0	0	0	0	0	0	0
RISC Rapid Searches	0	17	17	208	417	1,042	2,083	2,292	2,521
RISC ITF Searches	0	0	0	0	0	0	0	229	252
Verification Services	0	0	0	0	0	0	26	29	33
Investigative Services	322	326	340	354	3,993	4,323	4,496	4,676	4,862
High Priority	113	117	122	127	3,757	4,070	4,233	4,402	4,578
Routine Priority	208	208	217	225	234	244	254	264	274
Low Priority	1	1	1	2	2	9	9	10	10
Information Services	186	223	268	321	386	463	556	667	800
Fingerprint Image Retrievals	169	203	244	292	351	421	505	606	727
Fingerprint Features Request	17	20	24	29	35	42	50	60	72
Fingerprint Audit Trail Requests	0	0	0	0	0	0	1	1	1
Data Management Services	45	53	69	136	380	449	531	629	746
Fingerprint Delete Requests	43	46	49	53	57	61	65	70	75
Fingerprint Image Replacement	2	7	20	83	323	388	466	559	671
Direct Fingerprint Enrollment (SPC File ONLY)	3	3	4	4	5	5	6	6	7

Table 4-1d Peak Hourly Fingerprint Workload Estimates

Peak Hour	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services	11,657	16,082	31,805	36,251	38,255	41,687	45,983	47,515	51,082
Criminal Ten-Print	7,033	10,146	24,859	25,716	26,666	27,723	28,897	30,200	31,650
Criminal Peak Increase %	400%	400%	400%	400%	400%	400%	400%	400%	400%
High Priority	367	1,562	1,784	1,855	1,929	2,006	2,087	2,170	2,257
Routine Priority	6,479	6,039	6,742	7,528	8,404	9,384	10,477	11,697	13,060
Low Priority	12	10	0	0	0	0	0	0	0
Non-Urgent	175	2,535	16,333	16,333	16,333	16,333	16,333	16,333	16,333
Civil Ten-Print	4,624	5,903	6,913	10,118	10,756	11,881	12,919	12,274	13,886
Civil Peak Increase %	200%	200%	200%	200%	200%	200%	200%	200%	200%
High Priority	159	2,477	3,066	3,364	3,691	4,050	4,445	4,879	5,356
Routine Priority	3,748	2,487	2,916	3,652	3,821	4,414	5,097	5,891	6,808
Low Priority	603	628	685	739	804	881	721	752	782
Non-Urgent	114	311	246	2,363	2,440	2,536	2,656	752	940
Sub-Total PEAK Hour Ten-Print Identification Services	*11,657*	*16,049*	*31,772*	*35,834*	*37,422*	*39,604*	*41,816*	*42,474*	*45,536*
Criminal Rapid Searches	0	0	0	0	0	0	0	0	0
RISC Rapid Searches	0	33	33	417	833	2,083	4,167	4,583	5,042
RISC ITF Searches	0	0	0	0	0	0	0	458	504
RISC Peak Increase %	0%	200%	200%	200%	200%	200%	200%	200%	200%
Verification Services	0	0	0	0	0	0	32	37	42
Peak Increase %	125%	125%	125%	125%	125%	125%	125%	125%	125%
Investigative Services	403	408	425	442	4,991	5,404	5,620	5,845	6,079
Peak Increase %	125%	125%	125%	125%	125%	125%	125%	125%	125%
High Priority	141	146	152	158	4,696	5,088	5,291	5,503	5,723
Routine Priority	260	260	271	282	293	305	317	330	343
Low Priority	2	2	2	2	2	11	12	12	13
Information Services	232	279	335	401	481	578	694	834	1,000
Peak Increase %	125%	125%	125%	125%	125%	125%	125%	125%	125%
Fingerprint Image Retrievals	211	254	305	365	438	526	631	758	909
Fingerprint Features Request	21	25	30	36	43	52	62	75	90
Fingerprint Audit Trail Requests	0	0	0	0	0	0	1	1	1
Data Management Services	57	65	87	170	475	561	663	786	931
Peak Increase %	125%	125%	125%	125%	125%	125%	125%	125%	125%
Fingerprint Delete Requests	54	57	62	66	71	76	81	87	93
Fingerprint Image Replacement	3	8	25	104	404	485	582	699	838
Direct Fingerprint Enrollment (SPC File ONLY)	9	24	100	416	2020	2425	3492	4194	5866

NGI shall be capable of meeting the projected yearly storage capacity for fingerprint processing as specified in Table 4-2.

The following are the assumptions used to support the development of the Yearly Fingerprint Capacity Estimates depicted in Table 4-2 below.

- Based on FY2007 fingerprint statistics and FY2006 repository capacities, NGI contains approximately 53 million subjects in the criminal file and 14 million civil subjects (electronic file).
- Individual yearly estimates include previous year's capacity projection.
- 93.82% of NGI normal (non-project) Criminal Fingerprint Workload will be retained based on historical statistics for AFIS new adds and IDENT rate.
- 40% of NGI normal (non-project) Civil Fingerprint Workload will be retained based on historical statistics for AFIS new adds and IDENT rate.
- 6% of DHS Criminal Workload that supports linked records will be retained based on Interoperability projections.
- 3% of DHS Civil Workload that supports linked records will be retained based on Interoperability PMO / DHS joint projections.
- RISC Fingerprint Capacity estimates for FY2007 are based on RISC Prototype initial capacity with 20% increase for FY2008-FY2012.
- New NGI Repositories in FY2009 are based upon 5 new repositories, each sized at 25% of the FY2008 Civil Retained Fingerprints.
- New NGI Repositories capacity for FY2010-FY2012 is based upon estimated 20% growth rate.
- New NGI Repository infrastructure and functionality will be deployed in the Fiscal Year 2009.
- New NGI Repository capacity represents total capacity for 5 repositories.

Table 4-2 Yearly Fingerprint Capacity Estimates

YEARLY	Baseline FY2006	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Total Criminal Fingerprint Certification File (per add & update)	69,379,393	82,461,995	95,302,609	112,070,944	128,832,026	147,446,715	168,126,994	191,109,383	216,657,792	245,066,705
Criminal Fingerprint Composites	52,900,000	53,200,000	62,800,000	68,842,786	75,500,020	82,839,707	90,937,628	99,878,242	109,755,696	120,674,940
Rolled Civil Fingerprint Capacity (per Event)	13,500,000	16,985,000	24,380,000	29,861,296	45,260,344	61,738,920	79,489,553	97,631,786	108,184,959	120,357,546
Flat Civil Fingerprint Capacity (per Event)	0	615,000	1,920,000	5,029,683	8,263,754	11,627,187	15,125,158	18,763,047	22,546,452	26,481,194
Total Civil Fingerprint Capacity (per Event)	13,500,000	17,600,000	26,300,000	34,890,979	53,524,098	73,366,107	94,614,711	116,394,833	130,731,411	146,838,740
RISC Fingerprint Capacity	0	1,000,000	1,200,000	1,440,000	1,728,000	2,073,600	2,488,320	2,985,984	3,583,181	4,299,817
New Repositories Fingerprint Capacity (x5)	0	0	0	0	0	0	0	0	29,098,708	69,836,900
Total Fingerprint Capacity	135,779,393	154,261,995	185,602,609	217,244,709	259,584,144	305,726,129	356,167,653	410,368,443	489,826,788	586,717,102
% Fingerprints at 500ppi	*100%*	*100%*	*100%*	*100%*	*90%*	*80%*	*70%*	*70%*	*70%*	*70%*
% Fingerprints at 1000ppi	*0%*	*0%*	*0%*	*0%*	*10%*	*20%*	*30%*	*30%*	*30%*	*30%*

4.6.1.1 Shared Data Processing Workload

NGI shall enroll NGI Shared Data at least once a day.

NGI shall accept Shared Data enrollment requests from an External System (e.g., IDENT) at least once a day.

NGI shall be capable of processing 1,000 Shared Data demotions from NGI per day.

NGI shall be capable of processing 1,000 Shared Data removals from NGI per day.

NGI shall be capable of processing 2,500 Shared Data enrollments from NGI per day.

NGI shall be capable of extracting feature vectors from an External System's (e.g., IDENT) Shared Data at a rate of 25 per day.

NGI shall be capable of supporting updates to an External System's (e.g., IDENT) Shared Data at a rate of 200 changes per day.

NGI shall support a configurable number of IAQ searches per day.

Currently, NGI limits the number of IAQs to LESC to 80 requests per day.

NGI shall be capable of conducting up to 1,000 NGI Tenprint Identification searches per day against Shared Data records.

NGI shall be capable of performing 1,000 fingerprint feature searches of NGI Tenprint submissions against Shared Data records feature vectors per day.

NGI shall have the storage capacity for 1,000,000 Shared Data records from NGI.

NGI shall have the storage capacity for 13 million NGI Shared Data Activity Log entries over five years.

NGI shall have the storage capacity for 1,000,000 Shared Data records from an External System (e.g., IDENT).

4.6.2 Support Latent Processing Workload

NGI shall be capable of meeting the estimated Yearly Latent workloads contained in Table 4-3a.

NGI shall be capable of meeting the estimated average Daily Latent workloads contained in Table 4-3b.

NGI shall be capable of meeting the estimated average Hourly Latent workloads contained in Table 4-3c.

Deleted.

The following are the assumptions used to support the development of the Latent Workload Estimates depicted in Tables 4-3a, 4-3b, and 4-3c below.

- Latent Searches are based on the NGI April 2007 and Interoperability Transaction Volume Spreadsheet Version 4.2 2008 estimates.
- Latent Information and Data Management request workloads are based on the NGI SRD dated 2006 unless otherwise specified.
- ULF Image and Feature Retrievals for FY2007-FY2008 are based on NGI SRD workloads September 2006.
- ULF Image and Feature Retrievals for FY2009 are estimated to increase by 10 times for FY2008, and increase by 30% for the out years.
- ULF Adds estimated to result from 6% of Latent Searches.
- ULF Audit Trail Retrievals are estimated at 0.1% ULF Retrievals.
- ULF Deletes based on FY2006 actual ULF Deletes.

Table 4-3a Yearly Latent Workload Estimates[1]

Yearly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Latent Print Submissions	20,075	22,265	24,455	26,645	29,565	32,485	35,734	39,307	43,238
Investigative Services									
Latent Searches (all repositories)	176,921	171,111	188,405	207,027	227,511	250,043	274,828	302,092	332,082
Latent Penetration Query	4,730	5,676	6,812	8,174	9,809	11,771	14,125	16,950	20,340
Latent Repository Statistics Query	3,650	3,650	3,650	3,650	3,650	3,650	3,650	3,650	3,650
Latent Search Status and Modification Query	6,835	8,200	9,840	11,810	14,170	17,000	20,400	24,480	29,376
Total Investigative Searches	***192,136***	***188,637***	***208,707***	***230,661***	***255,140***	***282,464***	***313,003***	***347,172***	***385,448***
Information Request									
Unsolved Latent File (ULF) Image Retrieval	730	730	7,300	9,490	12,337	16,038	20,849	27,104	35,235
Unsolved Latent File (ULF) Feature Retrieval	0	0	7,300	9,490	12,337	16,038	20,849	27,104	35,235
Unsolved Latent File (ULF) Audit Trail Retrieval	0	0	0	0	0	0	0	27	35
Total Information Requests	***730***	***730***	***14,600***	***18,980***	***24,674***	***32,076***	***41,698***	***54,235***	***70,505***
Data Management Requests									
ULF Add (via Latent Search request)	10,616	10,267	11,305	12,422	13,651	15,003	16,490	18,126	19,925
ULF Deletes	1,460	1,460	1,460	1,825	1,825	1,825	2,190	2,190	2,190

[1] 85% of submissions are expected to search fingerprints while 15% will search palmprints.

Table 4-3b Average Daily Latent Workloads Estimates[2]

Average Daily	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Latent Print Submissions	55	61	67	73	81	89	98	108	119
Investigative Services									
Latent Searches (all repositories)	485	469	517	568	624	686	753	828	910
Latent Penetration Query	13	16	19	23	27	33	39	47	56
Latent Repository Statistics Query	10	10	10	10	10	10	10	10	10
Latent Search Status and Modification Query	19	23	27	33	39	47	56	68	81
Total Investigative Searches	***527***	***518***	***573***	***634***	***700***	***776***	***858***	***953***	***1,057***
Information Request									
Unsolved Latent File (ULF) Image Retrieval	2	2	20	26	34	44	58	75	97
Unsolved Latent File (ULF) Feature Retrieval	0	0	20	26	34	44	58	75	97
Unsolved Latent File (ULF) Audit Trail Retrieval	0	0	0	0	0	0	0	1	1
Total Information Requests	***2***	***2***	***40***	***52***	***68***	***88***	***116***	***151***	***195***
Data Management Requests									
ULF Add (via Latent Search request)	30	29	31	35	38	42	46	50	55
ULF Deletes	4	4	4	5	5	5	6	6	6

[2] 85% of submissions are expected to search fingerprints while 15% will search palmprints.

Table 4-3c Average Hourly Latent Workloads Estimates[3]

Average Hourly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Latent Print Submissions	2	3	3	3	3	4	4	5	5
Investigative Services									
Latent Searches (all repositories)	20	20	22	24	26	29	31	35	38
Latent Penetration Query	1	1	1	1	1	1	2	2	2
Latent Repository Statistics Query	0	0	0	0	0	0	0	0	0
Latent Search Status and Modification Query	1	1	1	1	2	2	2	3	3
Total Investigative Searches	***22***	***22***	***24***	***26***	***29***	***32***	***35***	***40***	***43***
Information Request									
Unsolved Latent File (ULF) Image Retrieval	0	0	1	1	1	2	2	3	4
Unsolved Latent File (ULF) Feature Retrieval	0	0	1	1	1	2	2	3	4
Unsolved Latent File (ULF) Audit Trail Retrieval	0	0	0	0	0	0	0	0	0
Total Information Requests	***0***	***0***	***2***	***2***	***2***	***4***	***4***	***6***	***8***
Data Management Requests									
ULF Add (via Latent Search request)	1	1	1	1	2	2	2	2	2
ULF Deletes	0	0	0	0	0	0	0	0	0

NGI shall be capable of meeting the projected yearly unsolved latent capacity as specified in Table 4-4a.

NGI shall support a maximum ULF capacity of 1 million images.

NGI shall be capable of meeting the projected yearly Special Population Cognizant File capacity as specified in Table 4-4b.

NGI shall support a maximum SPC File capacity of 3 million images.

The following are the assumptions used to support the development of the Yearly Unsolved Latent and Special Population Cognizant File Capacity Estimates depicted in Tables 4-4a and 4-4b below.

[3] 85% of submissions are expected to search fingerprints while 15% will search palmprints.

- FY2006 NGI had approximately 140,000 Unsolved Latent records.
- ULF capacity estimates for FY2007-FY2008 are based on yearly ULF Adds resulting from Latent Workload.
- ULF capacity estimates for FY2009-2012 are based on yearly ULF Adds resulting from Latent, Palmprint, and MCP Supplementary Print Workloads.

Table 4-4a Yearly Unsolved Latent Capacity Estimates

YEARLY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Unsolved Latent Capacity Max	**300,000**	**300,000**	**1,000,000**	**1,000,000**	**1,000,000**	**1,000,000**	**1,000,000**	**1,000,000**	**1,000,000**
Unsolved Latent Capacity Allocated	150,616	160,883	172,188	184,610	198,261	226,204	256,917	290,677	327,788

Table 4-4b Yearly Special Population Cognizant File Capacity Estimates

YEARLY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Special Population Cognizant (SPC) File Capacity									
Max Capacity	1,500,000	1,500,000	3,000,000	3,000,000	3,000,000	3,000,000	3,000,000	3,000,000	3,000,000
SPC File Capacity Allocated by Biometric									
Fingerprint	225,000	375,000	450,000	600,000	1,050,000	1,500,000	1,500,000	1,500,000	1,500,000
	15%	*25%*	*15%*	*20%*	*35%*	*50%*	*50%*	*50%*	*50%*
Palm Print						450,000	450,000	450,000	450,000
						15%	15%	15%	15%
Supplemental						210,000	210,000	210,000	210,000
						7%	*7%*	*7%*	*7%*
Photo							750,000	750,000	750,000
							25%	*25%*	*25%*
Iris								90,000	90,000
								3%	*3%*
SPC File Total Projections	**225,000**	**375,000**	**450,000**	**600,000**	**1,050,000**	**2,160,000**	**2,910,000**	**3,000,000**	**3,000,000**

4.6.3 Support Disposition Processing Workload

NGI shall be capable of meeting the estimated yearly disposition workloads contained in Table 4-5a.

NGI shall be capable of meeting the estimated average daily disposition workloads contained in Table 4-5b.

NGI shall be capable of meeting the estimated average hourly disposition workloads contained in Table 4-5c.

NGI shall support 150% of average hourly disposition workload as the disposition peak hourly workload.

The following are the assumptions used to support the development of the Disposition Workload Capacity Estimates depicted in Tables 4-5a, 4-5b, and 4-5c below.

- Submission figures are based on the actual MRD and hardcopy disposition requests processed from 2005-2007. Anticipated disposition receipts are calculated on a 75% participation rate from the contributing agencies utilizing estimates of potential disposition requests conveyed during canvasses conducted during FY2006. From 2010 forward MRD, submissions are expected to level off due to phasing out of MRD transactions and the fact that NCIC and EBTS disposition submission messages are expected to be more widely used.
- Projected estimates for Legacy Bulk Dispositions are based on approximately 75 million legacy backlog dispositions for arrests that are anticipated to be sent via bulk load submission. Bulk load expected values during the first 3 years are anticipated to be approximately 60-65% of the total MRD/CD disposition submission receipts.
- Legacy Bulk Disposition Request includes paper/document disposition requests.

Table 4-5a Yearly Disposition Workload Estimates

Yearly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Electronic Disposition with Fingerprint Identification Searches	0	2,920,000	3,102,500	3,832,500	4,015,000	4,197,500	4,365,400	4,540,016	4,721,617
Data Management Services									
Electronic Disposition Submission Requests (EBTS)	0	118,625	124,100	127,750	133,225	138,700	144,248	150,018	156,019
Electronic Disposition Submission Requests (NCIC)	18,250,000	28,105,000	36,500,000	39,420,000	40,880,000	42,705,000	44,413,200	46,189,728	48,037,317
Electronic Disposition Submission Requests (MRD)	18,250,000	9,855,000	3,285,000	1,825,000	1,825,000	1,825,000	1,825,000	1,825,000	1,825,000
**Legacy Bulk Disposition Requests	2,933,110	14,078,930	14,078,930	10,559,197	7,919,398	5,939,548	4,157,684	2,910,379	2,037,265
Electronic Disposition Maintenance Requests (EBTS/EFTS)	0	156,950	164,250	169,725	177,025	182,500	189,800	197,392	205,288
Electronic Disposition Maintenance Requests (NCIC)	302,848	314,962	327,560	340,663	354,289	368,461	383,199	398,527	414,469

Table 4-5b Average Daily Disposition Workload Estimates

Average Daily	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Electronic Disposition with Fingerprint Identification Searches	0	8,000	8,500	10,500	11,000	11,500	11,960	12,438	12,936
Data Management Services									
Electronic Disposition Submission Requests (EBTS)	0	325	340	350	365	380	395	411	427
Electronic Disposition Submission Requests (NCIC)	50,000	77,000	100,000	108,000	112,000	117,000	121,680	126,547	131,609
Electronic Disposition Submission Requests (MRD)	50,000	27,000	9,000	5,000	5,000	5,000	5,000	5,000	5,000
**Legacy Bulk Disposition Requests	8,036	38,572	38,572	28,929	21,697	16,273	11,391	7,974	5,582
Electronic Disposition Maintenance Requests (EBTS/EFTS)	0	430	450	465	485	500	520	541	562
Electronic Disposition Maintenance Requests (NCIC)	830	863	897	933	971	1,009	1,050	1,092	1,136

Table 4-5c Average Hourly Disposition Workload Estimates

Average Hourly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Electronic Disposition with Fingerprint Identification Searches	0	333	354	438	458	479	498	518	539
Data Management Services									
Electronic Disposition Submission Requests (EBTS)	0	14	14	15	15	16	16	17	18
Electronic Disposition Submission Requests (NCIC)	2,083	3,208	4,167	4,500	4,667	4,875	5,070	5,273	5,484
Electronic Disposition Submission Requests (MRD)	2,083	1,125	375	208	208	208	208	208	208
**Legacy Bulk Disposition Requests	335	1,607	1,607	1,205	904	678	475	332	233
Electronic Disposition Maintenance Requests (EBTS/EFTS)	0	18	19	19	20	21	22	23	23
Electronic Disposition Maintenance Requests (NCIC)	35	36	37	39	40	42	44	46	47

NGI shall be capable of meeting the estimated annual disposition data capacities contained in Table 4-6.

NGI shall be capable of meeting the estimated annual deferred disposition submission data capacities contained in Table 4-6.

The following are the assumptions used to support the development of the Yearly Disposition Capacity depicted in Table 4-6.

- Figures are based on the 14,000,000 arrests in FY2005 (FBI's Estimated Number of Arrests, U.S. 2005), with an estimated growth of 4% per year.
- Disposition projections are based on IISS estimated workloads given to the OMB 300 Report.

Table 4-6 Yearly Disposition Capacity Estimates

YEARLY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Yearly Disposition Data	15,142,400	15,748,096	16,378,020	17,033,141	17,714,467	18,423,046	19,159,968	19,926,367	20,723,422
Yearly Deferred Disposition Submission Data	72,800	75,712	78,741	81,891	85,167	88,574	92,117	95,802	99,635

4.6.4 Support Photo Processing Workload

NGI shall be capable of meeting the estimated yearly photo workloads contained in Table 4-7a.

NGI shall be capable of meeting the estimated average daily photo workloads contained in Table 4-7b.

NGI shall be capable of meeting the estimated average hourly photo workloads contained in Table 4-7c.

NGI shall support 150% of average hourly photo workload as the photo peak hourly workload.

The following are the assumptions used to support the development of the Photo Workload Estimates depicted in Tables 4-7a, 4-7b, and 4-7c below.

- New NGI Repository infrastructure and functionality will be deployed in the FY2008.
- No additional photo workload is anticipated due to New NGI Repository functionality.
- Direct Photo Enrollments apply to any repository.

Table 4-7a Yearly Photo Workload Estimates

Yearly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprint w/Photo	2,228,325	4,252,250	20,498,400	25,860,250	29,070,425	31,324,300	34,456,730	37,902,403	41,692,643
Information Services									
Photo Retrievals	8,030,000	15,403,000	20,315,900	27,068,400	36,386,850	49,278,650	64,062,245	83,280,919	108,265,194
Photo Feature Retrievals	0	0	0	0	0	0	315,287	441,402	617,963
SMT Photo Retrievals	0	0	0	0	0	0	206,955	289,737	405,632
Photo Audit Trail Retrievals	0	0	0	0	0	0	64,585	84,013	109,289
Investigative Services									
Facial Recognition Searches	0	0	36,500	51,100	73,000	100,375	140,525	196,735	275,429
UPF Add (via Facial Recognition Search request)	0	0	0	0	0	0	8,432	11,805	16,526
SMT Text-Based Searches	0	0	0	0	0	0	648,970	908,558	1,271,981
Photo Text-Based Searches	0	0	0	0	0	0	64,782,025	90,694,835	126,972,769
Data Management Serivces									
Direct Photo Enrollments	0	0	0	0	0	0	0	12,092,450	14,379,175
Photo Deletions	49,275	441,650	857,750	1,222,750	1,596,875	1,985,600	2,124,592	2,273,313	2,432,445

Table 4-7b Average Daily Photo Workload Estimates

Average Daily	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprint w/Photo	6,105	11,650	56,160	70,850	79,645	85,820	94,402	103,843	114,227
Information Services									
Photo Retrievals	22,000	42,200	55,660	74,160	99,690	135,010	175,513	228,167	296,617
Photo Feature Retrievals	0	0	0	0	0	0	864	1,210	1,694
SMT Photo Retrievals	0	0	0	0	0	0	567	794	1,112
Photo Audit Trail Retrievals	0	0	0	0	0	0	177	231	300
Investigative Services									
Facial Recognition Searches	0	0	100	140	200	275	385	539	755
UPF Add (via Facial Recognition Search request)	0	0	0	0	0	0	24	33	46
SMT Text-Based Searches	0	0	0	0	0	0	1,778	2,490	3,485
Photo Text-Based Searches	0	0	0	0	0	0	177,485	248,479	347,871
Data Management Services									
Direct Photo Enrollments	0	0	0	0	0	0	0	33,130	39,395
Photo Deletions	135	1,210	2,350	3,350	4,375	5,440	5,821	6,229	6,665

Table 4-7c Average Hourly Photo Workload Estimates

Average Hourly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprint w/Photo	255	486	2,340	2,953	3,319	3,576	3,934	4,327	4,760
Information Services									
Photo Retrievals	917	1,759	2,320	3,090	4,154	5,626	7,314	9,507	12,360
Photo Feature Retrievals	0	0	0	0	0	0	36	51	71
SMT Photo Retrievals	0	0	0	0	0	0	24	34	47
Photo Audit Trail Retrievals	0	0	0	0	0	0	8	10	13
Investigative Services									
Facial Recognition Searches	0	0	5	6	9	12	17	23	32
UPF Add (via Facial Recognition Search request)	0	0	0	0	0	0	1	2	2
SMT Text-Based Searches	0	0	0	0	0	0	75	104	146
Photo Text-Based Searches	0	0	0	0	0	0	7,396	10,354	14,495
Data Management Services									
Direct Photo Enrollments	0	0	0	0	0	0	0	1,381	1,642
Photo Deletions	6	51	98	140	183	227	243	260	278

NGI shall be capable of meeting the estimated yearly photo capacities contained in Table 4-8.

The following are the assumptions used to support the development of the Yearly Photo Capacity Estimates depicted in Table 4-8 below.

- New NGI Repository photo capacity will be able to accommodate up to 5 new repositories each sized to retain subjects for 2.5% of the Civil photo enrollments beginning in FY2009.
- Projected growth of New NGI Repositories is 20% after FY2009.
- New NGI Repository capacity represents total capacity for 5 repositories.
- RISC Photo capacity is estimated to be 5% of RISC Fingerprint Capacity.

Table 4-8 Yearly Photo Capacity Estimates

YEARLY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Criminal Photo Record	6,293,791	26,103,196	30,355,446	50,853,846	76,714,096	105,784,521	137,108,821	183,658,001	235,939,579
Civil Photo Record	0	0	0	0	0	0	9,345,000	18,633,050	27,624,327
Unsolved Photo Record	0	0	0	0	0	197,138	67,170	115,387	152,643
RISC Photo Records	0	0	72,000	86,400	103,680	124,416	149,299	179,159	214,991
New Repositories Photo Records (up to 5)	0	0	0	0	0	0	0	233,625	931,653
New Repositories								1	2
Total Photo Records	6,293,791	26,103,196	30,427,446	50,940,246	76,817,776	106,106,075	146,670,290	202,819,222	264,863,192

4.6.5 Support Palmprint Processing Workload

NGI shall be capable of meeting the estimated yearly palmprint workloads contained in Table 4-9a.

NGI shall be capable of meeting the estimated average daily palmprint workloads contained in Table 4-9b.

NGI shall be capable of meeting the estimated average hourly palmprint workloads contained in Table 4-9c.

NGI shall support 150% of average hourly palmprint workload as the palmprint peak hourly workload.

The following are the assumptions used to support the development of the Palmprint Workload Estimates depicted in Tables 4-9a, 4-9b, and 4-9c below.

- FY2007-FY2008 Palmprint workload estimates based on informal stakeholder survey, April 2007, to support the Palmprint Quick Win.
- FY2009 - FY2012 is expected to receive a 10% increase per year.
- Palmprint Feature retrievals begin in FY2009 and are based on 50% of Image Retrievals.
- Audit Trail Retrievals are based on 0.1% of image and feature retrievals.
- FY2009-2012 Palmprint searches are estimated to be 75% of Latent Searches.
- ULF Adds are estimated to result from 6% of Palmprint Searches.
- New NGI Repository Palm enrollments will start FY2009.
- Direct Palmprint Enrollment includes enrollment to all repositories.
- Palm Print Updates would require a user to perform both a Palm Print Deletion and Palm Print Enrollment function.

Table 4-9a Yearly Palmprint Workload Estimates

Yearly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprints w/ palmprints	86,820	295,074	324,581	357,040	392,743	432,018	475,220	522,742	575,016
Information Services									
Palmprint Image Retrievals	0	0	0	0	0	0	0	1,634,616	1,961,539
Palmprint Feature Retrievals	0	0	0	0	0	0	0	817,308	980,770
Palmprint Audit Trail Retrievals	0	0	0	0	0	0	0	2,452	2,942
Investigative Services									
Palmprint Searches	0	0	0	0	0	187,532	206,121	226,569	249,062
Data Management Services									
Direct Palmprint Enrollment	0	0	0	0	0	0	0	5,755,320	6,906,384
ULF Add (via Palmprint Search request)	0	0	0	0	0	11,252	12,368	13,595	14,944
Palmprint Deletions	0	0	0	0	0	0	0	3,650	3,650
Palmprint Updates	0	0	0	0	0	0	0	365	365

Table 4-9b Average Daily Palmprint Workload Estimates

Average Daily	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprints w/ palmprints	2,894	808	889	978	1,076	1,184	1,302	1,432	1,575
Information Services									
Palmprint Image	0	0	0	0	0	0	0	4,478	5,374
Palmprint Feature Retrievals	0	0	0	0	0	0	0	2,239	2,687
Palmprint Audit Trail Retrievals	0	0	0	0	0	0	0	7	8
Investigative Services									
Palmprint Searches	0	0	0	0	0	514	565	621	682
Data Management Services									
Direct Palmprint	0	0	0	0	0	0	0	15,768	18,922
ULF Add (via Palmprint Search	0	0	0	0	0	31	34	37	41
Palmprint Deletions	0	0	0	0	0	0	0	10	10
Palmprint Updates	0	0	0	0	0	0	0	1	1

Table 4-9c Average Hourly Palmprint Workload Estimate

Average Hourly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprints w/ palmprints	121	34	38	41	45	50	55	60	66
Information Services									
Palmprint Image	0	0	0	0	0	0	0	187	224
Palmprint Feature Retrievals	0	0	0	0	0	0	0	94	112
Palmprint Audit Trail Retrievals	0	0	0	0	0	0	0	1	1
Investigative Services									
Palmprint Searches	0	0	0	0	0	22	24	26	29
Data Management Services									
Direct Palmprint	0	0	0	0	0	0	0	657	789
ULF Add (via Palmprint Search	0	0	0	0	0	2	2	2	2
Palmprint Deletions	0	0	0	0	0	0	0	1	1
Palmprint Updates	0	0	0	0	0	0	0	1	1

NGI shall be capable of meeting the estimated yearly palmprint capacities contained in Table 4-10.

The following are the assumptions used to support the development of the Yearly Palmprint Data Capacity Estimates depicted in Table 4-10 below.

- RISC Palmprint capacity is estimated to be 10% of the RISC Fingerprint capacity.
- New NGI Repository Palmprint capacity will initially, in FY2009, be able to accommodate up to 5 new repositories each sized to be 1% of the Criminal Palmprint Records.
- Projected growth of New NGI Repositories is 20% after FY2009.
- New NGI Repository capacity represents total capacity for 5 repositories.

Table 4-10 Yearly Palmprint Data Capacity Estimates

YEARLY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Criminal Palmprint Records	86,820	381,894	706,475	1,063,515	1,456,258	1,888,276	2,363,496	2,886,237	3,461,253
Civil Palmprint Records	0	0	0	0	0	0	0	0	0
Unsolved Palmprint Records	0	0	0	0	0	11,252	23,620	37,215	52,159
RISC Palmprint Records	0	0	144,000	172,800	207,360	248,832	298,598	358,318	429,982
New Repositories (up to 5) Palmprint Records	0	0	0	0	0	0	0	28,862	69,225
New Repositories								1	2
Total Palmprint Records	**86,820**	**381,894**	**850,475**	**1,236,315**	**1,663,618**	**2,148,360**	**2,685,714**	**3,310,633**	**4,012,619**

4.6.6 Support Supplemental Fingerprint and Palmprint Processing Workload

NGI shall be capable of meeting the estimated yearly supplemental fingerprint and palmprint workloads contained in Table 4-11a.

NGI shall be capable of meeting the estimated average daily supplemental fingerprint and palmprint workloads contained in Table 4-11b.

NGI shall be capable of meeting the estimated average hourly supplemental fingerprint and palmprint workloads contained in Table 4-11c.

NGI shall support 150% of average hourly supplemental fingerprint and palmprint workload as the supplemental fingerprint palmprint peak hourly workload.

The following are the assumptions used to support the development of the Supplemental Fingerprint and Palmprint Workload Estimates depicted in Tables 4-11a, 4-11b, and 4-11c below.

- Supplemental Fingerprint and Palmprint transactions estimated to be 15% of Palmprint transactions.
- Audit Trail Retrievals are based on 0.1% of image and feature retrievals.
- Direct Supplementary Fingerprint (FP) and Palmprint Enrollments may be to any repository.

- Supplemental Fingerprint and Palm Print Updates would require a user to perform both a Supplemental Fingerprint and Palm Print Deletion and Supplemental Fingerprint and Palm Print Enrollment function.

Table 4-11a Yearly Supplemental Fingerprint and Palmprint Workload Estimates

Yearly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprints w/ Supplemental Prints	0	0	48,687	53,556	58,912	64,803	71,283	78,411	86,252
Information Services									
Supplemental FP and Palmprints Image	0	0	0	0	0	0	170,273	245,192	294,231
Supplemental Prints Feature Retrievals	0	0	0	0	0	0	85,136	122,596	147,116
Supplemental FP and Palmprint Audit Trail Retrievals	0	0	0	0	0	0	255	368	441
Investigative Services									
Supplemental Prints Searches	0	0	0	0	0	28,130	30,918	33,985	37,359
Data Management									
Direct Supplemental Print Enrollments	0	0	0	0	0	0	0	863,298	1,035,958
ULF Add (via Supplemental Print Search request)	0	0	0	0	0	1,688	1,855	2,039	2,242
Supplemental Prints Deletions	0	0	0	0	0	0	0	548	548
Supplemental Prints Updates	0	0	0	0	0	0	0	55	55

Table 4-11b Average Daily Supplemental Fingerprint and Palmprint Workload Estimates

Average Daily	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprints w/ Supplemental Prints	0	0	134	147	162	178	196	215	237
Information Services									
Supplemental FP and Palmprints Image Retrievals	0	0	0	0	0	0	467	672	807
Supplemental Prints Feature Retrievals	0	0	0	0	0	0	234	336	404
Supplemental FP and Palmprint Audit Trail Retrievals	0	0	0	0	0	0	1	2	2
Investigative Services									
Supplemental Prints Searches	0	0	0	0	0	78	85	94	103
Data Management Services									
Direct Supplemental Print Enrollments	0	0	0	0	0	0	0	2,366	2,839
ULF Add (via Supplemental Print Search request)	0	0	0	0	0	5	6	6	7
Supplemental Prints Deletions	0	0	0	0	0	0	0	2	2
Supplemental Prints Updates	0	0	0	0	0	0	0	1	1

Table 4-11c Average Hourly Supplemental Fingerprint and Palmprint Workload Estimates

Average Hourly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprints w/ Supplemental Prints	0	0	6	6	7	7	8	9	10
Information Services									
Supplemental FP and Palmprints Image Retrievals	0	0	0	0	0	0	19	28	34
Supplemental Prints Feature Retrievals	0	0	0	0	0	0	10	14	17
Supplemental FP and Palmprint Audit Trail Retrievals	0	0	0	0	0	0	0	0	0
Investigative Services									
Supplemental Prints Searches	0	0	0	0	0	3	4	4	4
Data Management Services									
Direct Supplemental Print Enrollments	0	0	0	0	0	0	0	99	118
ULF Add (via Supplemental Print Search request)	0	0	0	0	0	0	0	0	0
Supplemental Prints Deletions	0	0	0	0	0	0	0	0	0
Supplemental Prints Updates	0	0	0	0	0	0	0	0	0

NGI shall be capable of meeting the estimated yearly Supplemental Fingerprint and Palmprint capacities contained in Table 4-12.

The following are the assumptions used to support the development of the yearly supplemental fingerprint and palmprint capacity estimates depicted in Table 4-12 below.

- Supplemental Fingerprint and Palmprint capacities estimated to be 15% of Palmprint capacities.
- RISC Supplemental Fingerprint and Palmprint capacity estimated to be 3% of RISC Fingerprint capacity.
- New NGI Repository capacity represents total capacity for 5 repositories.

Table 4-12 Yearly Supplemental Fingerprint and Palmprint Capacity Estimates

YEARLY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Criminal Supplemental Print Records	0	0	105,972	159,528	218,439	283,242	354,525	432,936	519,188
Civil Supplemental Print Records	0	0	0	0	0	0	0	0	0
Unsolved Supplemental Print Records	0	0	0	0	0	1,688	3,543	5,583	7,824
RISC Supplemental Print Records	0	0	43,200	51,840	62,208	74,650	89,580	107,495	128,995
New Repositories (up to 5) Supplemental Print Records	0	0	0	0	0	0	0	4,330	10,384
Total Supplemental Print Records	**0**	**0**	**149,172**	**211,368**	**280,647**	**359,580**	**447,648**	**550,344**	**666,391**

4.6.7 Support Iris Processing Workload

NGI shall be capable of meeting the estimated yearly iris workloads contained in Table 4-13a.

NGI shall be capable of meeting the estimated average daily iris workloads contained in Table 4-13b.

NGI shall be capable of meeting the estimated average hourly iris workloads contained in Table 4-13c.

NGI shall support 150% of average hourly iris workload as the iris peak hourly workload.

The following are the assumptions used to support the development of the Iris Workload Estimates depicted in Tables 4-13a, 4-13b, and 4-13c below.

- Iris enrollments and retrievals will not start until FY2009.
- Iris enrollments will initially have very low volume while the NGI user community develops capabilities.
- Iris enrollments are estimated to increase by 300% each year FY2010-FY2012.
- Direct enrollments will be approximately 5% of fingerprints with iris enrollment workload.
- Full Iris functionality will not start until FY2009.
- Iris Search workloads are estimated to be 22% of the iris enrollment workloads projections for FY2007.
- Iris Image Retrieval workloads are estimated to be 0.3% of the iris enrollment workloads.
- Iris Unsolved File adds are estimated to result from 6% of Iris investigative searches.

- Iris Deletions workloads are estimated to be 0.7% of the iris enrollment workloads.
- No additional Iris workload will be anticipated due to creation of new NGI Repositories.

Table 4-13a Yearly Iris Workload Estimates

Yearly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprint w/Iris	0	0	0	0	0	0	0	73,000	219,000
Information Services									
Iris Image Retrievals	0	0	0	0	0	0	0	219	657
Iris Feature Retrievals	0	0	0	0	0	0	0	730	1,095
Iris Audit Trail Retrievals	0	0	0	0	0	0	0	365	365
Investigative Services									
Iris Searches	0	0	0	0	0	0	0	16,863	50,589
Data Management Services									
Direct Iris Enrollments	0	0	0	0	0	0	0	3,650	10,950
UIF Add (via IRIS Search request)	0	0	0	0	0	0	0	1,012	3,036
Iris Deletions	0	0	0	0	0	0	0	537	1,610

Table 4-13b Average Daily Iris Workload Estimates

Average Daily	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprint w/Iris	0	0	0	0	0	0	0	200	600
Information Services									
Iris Image Retrievals	0	0	0	0	0	0	0	1	2
Iris Feature Retrievals	0	0	0	0	0	0	0	2	3
Iris Audit Trail Retrievals	0	0	0	0	0	0	0	1	1
Investigative Services									
Iris Searches	0	0	0	0	0	0	0	47	139
Data Management Services									
Direct Iris Enrollments	0	0	0	0	0	0	0	10	30
UIF Add (via IRIS Search request)	0	0	0	0	0	0	0	3	9
Iris Deletions	0	0	0	0	0	0	0	2	5

Table 4-13c Average Hourly Iris Workload Estimates

Average Hourly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Fingerprint w/Iris	0	0	0	0	0	0	0	9	25
Information Services									
Iris Image Retrievals	0	0	0	0	0	0	0	1	1
Iris Feature Retrievals	0	0	0	0	0	0	0	1	1
Iris Audit Trail Retrievals	0	0	0	0	0	0	0	1	1
Investigative Services									
Iris Searches	0	0	0	0	0	0	0	2	6
Data Management Services									
Direct Iris Enrollments	0	0	0	0	0	0	0	1	2
UIF Add (via IRIS Search request)	0	0	0	0	0	0	0	1	1
Iris Deletions	0	0	0	0	0	0	0	1	1

NGI shall be capable of meeting the estimated yearly iris capacities contained in Table 4-14.

The following are the assumptions used to support the development of the Yearly Iris Capacity Estimates depicted in Table 4-14 below.

- New NGI Repository Iris capacity will start FY2009.
- Iris enrollments will split 50/50 between civil and criminal iris capacity.
- Unsolved Iris capacity will be based on 0.1% of the Criminal Iris capacity.
- RISC Iris capacity estimated to be 0.1% of RISC Fingerprint Capacity.

- New NGI Repository Iris capacity initially will be able to accommodate up to 5 new repositories each based on 0.1% FY2009 Civil Iris enrollments.
- New NGI Repository capacity represents total capacity for 5 repositories.
- Projected growth of New NGI Repositories is 20% after FY2009.

Table 4-14 Yearly Iris Capacity Estimates

YEARLY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Criminal Iris Records	0	0	0	0	0	0	0	36,500	146,000
Civil Iris Records	0	0	0	0	0	0	0	36,500	146,000
Unsolved Iris Records	0	0	0	0	0	0	0	37	146
RISC Iris Subjects	0	0	0	0	0	0	0	3,584	4,300
New Repositories (each) Iris Records	0	0	0	0	0	0	0	365	1,460
New Repositories in Operation	0	0	0	0	0	0	0	1	2
Total New Repositories (up to 5) Iris Records	0	0	0	0	0	0	0	365	2,920

4.6.8 Support Identity Management Processing Workload

NGI shall be capable of meeting the average daily submission volume of expungements and miscellaneous transactions, as specified in Table 4-15.

- Expungements and Miscellaneous Documents estimated 7.5% annual growth rate after FY 2005.
- Projections are based on NGI SRD September 2006, Table 4-6.

Table 4-15 Average Daily Expungement and Miscellaneous Document Workload

Average Daily	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Data Management Services									
Total Criminal Expungements	1,887	2,029	2,182	2,346	2,522	2,712	2,916	3,135	3,371
Total Correspondence and Miscellaneous Documents	513	552	594	639	687	739	795	855	920

NGI shall be capable of meeting the estimated yearly Identity capacities contained in Table 4-16.

The following are the assumptions used to support the development of the Yearly Identity Management Capacity Estimates depicted in Table 4-16 below.

- FY2006 criminal and civil file sizes were used to baseline the criminal and civil repository Identity capacity estimates.
- Criminal new Identity enrollment (adds) are based on 25.82% of criminal retains, and subtracting 1% of the criminal identities to reflect records contained within RISC.
- Civil new Identity enrollment estimates based on historical civil add rate of 28.55%, reduced by a 28.7% civil IDENT rate based on the Bureau of Labor Statistics, 2006 Volunteer Rates for Employed Persons.
- Civil consolidation begins FY2009 and assumes a 25% consolidation rate of the existing civil only identities, and 0.5% consolidation rate of existing civil file with the criminal file.
- RISC unique identities based on the addition of new International customers from FY2008-FY2012 at a rate of 2 countries per year each with 20,000 unique identities.
- Unsolved File unique identities based on sum of Unsolved Latent, Iris, and Photo file adds and deletes for a year.
- Special Population Cognizant File Identities based on the 105% of the SPC Fingerprint File Capacity to accommodate for unique identities based on fingerprints as well as a limited number of unique identities based on other biometrics (i.e., palmprints, supplemental prints, iris, or photos).
- New Repository capacity based on 5 new repositories each sized at 25% of FY2009 civil identity enrollments.
- New NGI Repository capacity represents total capacity for 5 repositories.
- Criminal Identity deletions are estimated to equal 60% of Expungements.
- Civil Identity deletions are estimated to equal 70% of Rap Back Subscription Deletions.

Table 4-16 Yearly Identity Capacity Estimated

Repository	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
New Criminal Adds (CMF)	5,564,462	5,598,265	6,042,786	6,657,235	7,339,687	8,097,921	8,940,614	9,877,454	10,919,244
New Civil File Adds	10,335,240	8,210,090	8,590,979	18,633,119	19,842,009	21,248,604	21,780,123	14,336,578	16,107,328
(less)Civil Identities shared with civil - Consolidation	0	0	0	0	0	0	0	-37,519,915	-4,622,803
(less)Civil Identities shared with criminal - Consolidation	0	0	0	0	0	0	0	-653,657	-71,683
Unique Criminal Identities	53,200,000	62,800,000	68,842,786	75,500,020	82,839,707	90,937,628	99,878,242	109,755,696	120,674,940
Unique Civil Identities	17,600,000	26,300,000	34,890,979	53,524,098	73,366,107	94,614,711	116,394,833	130,731,411	146,838,740
Unique RISC Identities (ITF)	0	0	0	0	0	0	0	40,000	80,000
Unique Identities for New Repositories	0	0	0	0	0	0	0	29,098,708	69,836,900
Unsolved Identities	149,156	159,423	170,728	182,785	196,436	419,545	321,225	402,756	476,858
Unique SPCF Identities	225,000	375,000	450,000	600,000	1,050,000	1,500,000	1,500,000	1,500,000	1,500,000
Sub-Total Identity (UCN) Capacity	71,174,156	89,634,423	104,354,493	129,806,903	157,452,250	187,471,883	218,094,301	271,528,572	339,407,438
Less: Consolidation of Identities spanning multiple repositories	0	0	0	0	0	0	0	-38,173,572	-42,868,058
Less: Criminal Expungments / Civil Deletions	-413,253	-444,351	-477,858	-513,774	-552,318	-593,928	-2,147,660	-2,192,996	-2,603,665
Total Yearly Identity (UCN) Capacity	**70,760,903**	**89,190,072**	**103,876,635**	**129,293,129**	**156,899,932**	**186,877,955**	**215,946,641**	**231,162,004**	**293,935,714**

4.6.9 Support Rap Back Processing Workload

NGI shall be capable of meeting the estimated yearly Rap Back workloads contained in Table 4-17a.

NGI shall be capable of meeting the estimated average daily Rap Back workloads contained in Table 4-17b.

NGI shall be capable of meeting the estimated average hourly Rap Back workloads contained in Table 4-17c.

The following are the assumptions used to support the development of the Rap Back Workload Estimates depicted in Tables 4-17a, 4-17b, and 4-17c below.

- Rap Back capabilities will not start until FY2009.

- Daily enrollments equal all civil retains (70% civil identification workload) plus 5% of criminal identification workloads.
- Rap Back Subscription Deletions are estimated to be 5% of all Rap Back enrollments.
- Rap Back Subscription updates are estimated to be 5% of all Rap Back enrollments.
- Rap Back renewals are estimated to be 50% of all Rap Back enrollments.
- Rap Back Subscription List Requests are estimated to be 1% of all enrollments.
- Rap Back Notifications are estimated to be 65% of criminal and 75% civil identification workloads.

Table 4-17a Yearly Rap Back Workload Estimates

Yearly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Rap Back Enrollment as part of Fingerprint Enrollment	0	0	0	0	0	0	24,865,850	21,140,841	24,097,586
Information Services									
Rap Back Subscription List Requests	0	0	0	0	0	0	431,159	430,409	532,976
Data Management Services									
Direct Enrollment	0	0	0	0	0	0	18,250,000	21,900,000	29,200,000
Rap Back Subscription Deletions	0	0	0	0	0	0	2,155,793	2,152,043	2,664,880
Rap Back Subscription Updates	0	0	0	0	0	0	862,317	860,817	1,065,952
Rap Back Subscription Renewals	0	0	0	0	0	0	21,557,925	21,520,421	26,648,793
Notification Services									
Rap Back Notifications	0	0	0	0	0	0	5,173,902	5,164,901	6,395,711

Table 4-17b Average Daily Rap Back Workload Estimates

DAILY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Rap Back Enrollment as part of Fingerprint Enrollment	0	0	0	0	0	0	68,126	57,921	66,021
Information Services									
Rap Back Subscription List Requests	0	0	0	0	0	0	1,182	1,180	1,461
Data Management Services									
Direct Rap Back Enrollment	0	0	0	0	0	0	50,000	60,000	80,000
Rap Back Subscription Deletions	0	0	0	0	0	0	5,907	5,897	7,302
Rap Back Subscription Updates	0	0	0	0	0	0	2,363	2,359	2,921
Rap Back Subscription Renewals	0	0	0	0	0	0	59,063	58,961	73,011
Notification Services									
Rap Back Notifications	0	0	0	0	0	0	14,176	14,151	17,523

Table 4-17c Average Hourly Rap Back Workload Estimates

Average Hourly	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Identification Services									
Rap Back Enrollment as part of Fingerprint Enrollment	0	0	0	0	0	0	2,839	2,414	2,751
Information Services									
Rap Back Subscription List Requests	0	0	0	0	0	0	50	50	61
Data Management Services									
Direct Rap Back Enrollment	0	0	0	0	0	0	2,084	2,500	3,334
Rap Back Subscription Deletions	0	0	0	0	0	0	247	246	305
Rap Back Subscription Updates	0	0	0	0	0	0	99	99	122
Rap Back Subscription Renewals	0	0	0	0	0	0	2,461	2,457	3,043
Notification Services									
Rap Back Notifications	0	0	0	0	0	0	591	590	731

NGI shall be capable of meeting the estimated yearly Rap Back capacities contained in Table 4-18.

The following are the assumptions used to support the development of the Yearly Rap Back Estimates depicted in Table 4-18 below.

- Capacity equals new enrollments plus the previous year renewals reduced by Rap Back Subscription Deletion.

Table 4-18 Yearly Rap Back Subscription Capacity Estimates

YEARLY	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Rap Back Subscriptions Capacity	0	0	0	0	0	0	40,960,057	81,848,855	132,481,561

4.6.10 Support Identity History File Processing Workload

NGI shall be capable of processing an average daily volume of 200 Ad Hoc Subject Search inquiries against the Identity History File.

NGI shall be capable of meeting the estimated average daily volume of Identity history requests and searches as specified in Table 4-19.

The following are the assumptions used to support the development of the Daily Identity History Workload Estimates depicted in Table 4-19 below.

- Daily Identity History Inquiries, Requests, and Searches workload based on NGI SRD, September 2006, Table 4-5.
- III Subject History Requests (QH) estimated annual growth rate of 20%.
- III Subject Record Requests (QR) estimated annual growth rate of 10%.
- NCIC Persons Inquiry (QWI) estimated annual growth rate of 20%.
- NICS firearms & explosives background checks estimated annual growth rate of 1.5%.

Table 4-19 Average Daily Identity History Searches and Request Estimates

Average Daily	FY2007	FY2008	FY2009	FY2010	FY2011	FY2012	FY2013	FY2014	FY2015
Information Services									
III Subject Record Request Requests (QR)	68,599	69,689	76,658	84,324	92,756	102,032	112,235	123,458	135,804
Record Status Query (ZRS)									
Record Availability Query (ZR)									
Investigative Services									
III Subject History Requests (QH)	513,726	526,684	632,021	758,425	910,110	1,092,132	1,310,558	1,572,670	1,887,204
NCIC Persons Inquiry (QWI)	3,764	9,796	11,755	14,106	16,927	20,313	24,376	29,251	35,101
FBI Service Provider Subject Searches	10,362	9,641	10,605	11,666	12,832	14,115	15,527	17,080	18,788
Total Subject Inquiries, Requests, and Searches	**596,451**	**615,810**	**731,039**	**868,521**	**1,032,626**	**1,228,592**	**1,462,696**	**1,742,459**	**2,076,897**

4.7 System Characteristics

NGI shall comply with the current CJIS Data Center and Facility Management policies when defining the environment in which NGI is located.

APPENDIX A DESIGN CONCEPTS

A.1 NGI Design/Policy Concepts

The following table contains the User Concept/Stakeholder Requests (STRQ) that fall into two categories: Design Issues and Policy Issues. These STRQs imply a design or require a FBI CJIS policy decision to guide the system design.

The STRQs defined below were determined to represent some concepts at the system requirements level, and were not appropriate for the decomposition at a User Service Requirement or Functional Requirements Level. The STRQs listed are presented to ensure that they are addressed during the system design phase. These requirements must be carried into system design and included in subsequent development documentation. The STRQ ID represents the unique identifier maintained within the Rationale RequisitePro toolset. The User Concept (REQID) represents the original identifers assigned during the NGI user concept / requirements canvass. The STRQs that have a '*' in their User Concept column were captured as part of the NGI System Requirements Review, not the NGI Requirements Canvass, therefore a User Concept (Req ID) does not exist.

Table A-1 NGI Design & Policy Stakeholder Requests

STRQ ID (RVTM)	Stakeholder Request Text	User Concept (REQID)	Issue
STRQ7	IPS shall accommodate very large images (such as 5 megapixels). The system needs larger resolution on the face, e.g. greater face texture.	5	NGI - Design
STRQ8	IAFIS shall support the capability to exchange the EFTS information using XML.	6	NGI - Design
STRQ16	IAFIS shall support the submission of disposition information using an XML interface.	12	NGI - Design
STRQ42	IAFIS shall allow the ORI table to store all ORIs in a state.	35	NGI - Design
STRQ44	IPS shall provide the capability to process high resolution facial photos (1/10 millimeter covering faces 6.7" in width and 9.8" high).	37	NGI - Design
STRQ48	IPS shall be able to store facial depth maps.	41	NGI - Design
STRQ49	IPS shall be capable of processing multiple resolutions for photos, including 1/10 millimeter resolution, legacy 480x640, and about twice 480x640.	42	NGI - Design
STRQ51	IPS shall be capable of processing high resolution SMT photos (1/10 millimeter).	44	NGI - Design

STRQ ID (RVTM)	Stakeholder Request Text	User Concept (REQID)	Issue
STRQ61	IAFIS shall allow a state to use a separate connection to the CJIS WAN with its own IP address for submitting dispositions with the state's permission.	54	Policy
STRQ62	IAFIS shall allow disposition submissions to be submitted using a real time transaction formatted in XML.	55	NGI - Design
STRQ63	IAFIS shall be capable of supporting XML batch submissions.	56	NGI - Design
STRQ64	IAFIS shall be capable of supporting batch disposition submissions using web services protocol.	57	NGI - Design
STRQ66	IAFIS shall store the state unique arrest number so that dispositions could be matched by FBI number and arrest number to do the matching of dispositions to arrest records.	59	NGI - Design
STRQ70	'The NPPS shall allow bulk submission of palmprints using XML.	61	NGI - Design
STRQ91	IAFIS shall allow direct BPPE submissions from local agencies with the state's permission.	81	Policy
STRQ94	IAFIS shall provide an explanation when a submission is rejected that indicates what corrective action is required.	84	NGI - Design
STRQ103	IAFIS shall be able to send all responses (criminal, civil, rap back) directly to originating requestor in addition to responses being sent to SIB	93.1	Policy
STRQ112	NGI shall return the response for palmprint search to the local AFIS (by ORI) workstation, or e-mail, bypassing the states AFIS system	102	Policy
STRQ114	NGI shall provide capability for local agencies to connect to NGI without going through the state to submit and search palmprints with the state's permission.	104	Policy
STRQ125	IAFIS shall provide the ability to make submissions via LEO with the same capabilities as the CJIS WAN. (i.e. Submit ULAC, ULD files through LEO/JABS to NGI and receive ULM files from NGI via LEO/JABS.)	115.1	Policy
STRQ126	IAFIS shall provide the ability to make submissions via LEO with the same capabilities as the CJIS WAN. (i.e., submit ULAC, ULD files through LEO/JABS to NGI and receive ULM files from NGI via LEO/JABS).	115.2	Policy
STRQ129	IAFIS shall provide the ability to pull up an electronic image of the fingerprint card to verify demographic data (e.g. names, DOB, Age) with fingerprints and palmprints.	116.2	NGI - Design
STRQ139	The submission protocol shall include but not be limited to e-mail (such as web based submission).	122	NGI - Design
STRQ140	The submission protocol shall support a header that reveals transaction purpose, routing (multiple), and priority.	123	NGI - Design
STRQ141	The submission protocol shall support a header that reveals transaction purpose, routing (multiple), and priority.	123	NGI - Design

STRQ ID (RVTM)	Stakeholder Request Text	User Concept (REQID)	Issue
STRQ157	The date photo taken shall be mandatory for the submission of a mug shot without an arrest record. The "DATE PHOTO TAKEN" will be appended to the photo as a photo message.	139	NGI - Design
STRQ159	The IPS system shall provide the ability for local agencies to submit photos to the FBI.	141	Policy
STRQ172	IAFIS shall have the ability to load old latent fingerprint cases for storage.	154.1	NGI - Design
STRQ173	IAFIS shall have the ability to load old latent fingerprint cases for searching.	154.2	NGI - Design
STRQ177	IAFIS shall have the capability/protocol for States to permit county Law Enforcement Agencies to submit standard submissions other than tenprint via pass-through systems managed by the state.	157.1	Policy
STRQ178	Any direct access by a county or local law enforcement agency to IAFIS shall require the consent of the state.	157.1	Policy
STRQ179	IAFIS shall have the capability/protocol for States to permit local Law Enforcement Agencies to submit standard submissions other than tenprint via pass-through systems managed by the state.	157.2	Policy
STRQ180	IAFIS shall have the capability/protocol for States to permit county Law Enforcement Agencies to submit standard submissions other than tenprint via direct access to NGI.	157.3	Policy
STRQ181	IAFIS shall have the capability/protocol for States to permit local Law Enforcement Agencies to submit bulk submissions other than tenprint via pass-through systems managed by the state.	157.4	Policy
STRQ182	IAFIS shall have the capability/protocol for States to permit local Law Enforcement Agencies to submit bulk submissions other than tenprint via direct access to NGI.	157.5	Policy
STRQ183	IAFIS shall have the capability/protocol for States to permit county Law Enforcement Agencies to submit bulk submissions other than tenprint via pass-through systems managed by the state.	157.6	Policy
STRQ184	IAFIS shall have the capability/protocol for States to permit county Law Enforcement Agencies to submit bulk submissions other than tenprint via direct access to NGI.	157.7	Policy
STRQ185	IAFIS shall have the capability/protocol for States to permit local Law Enforcement Agencies to submit standard submissions other than tenprint via direct access to NGI.	157.8	Policy
STRQ186	State, county, local and other law enforcement entities shall have systems that are compatible to NGI.	157.9	Policy
STRQ188	IAFIS shall have the capability/protocol for States to permit county Law Enforcement Agencies to conduct searches other than Tenprint of the repositories via pass-through systems managed by the state.	158.1	Policy

STRQ ID (RVTM)	Stakeholder Request Text	User Concept (REQID)	Issue
STRQ189	IAFIS shall have the capability/protocol for States to permit local Law Enforcement Agencies to conduct searches other than Tenprint of the repositories via pass-through systems managed by the state.	158.2	Policy
STRQ190	IAFIS shall have the capability/protocol for States to permit county Law Enforcement Agencies to conduct searches other than Tenprint of the repositories via direct access to NGI.	158.3	Policy
STRQ191	IAFIS shall have the capability/protocol for States to permit local Law Enforcement Agencies to conduct searches other than Tenprint of the repositories via direct access to NGI.	158.4	Policy
STRQ192	State, county, local and other law enforcement entities shall have systems that are compatible to NGI.	158.5	Policy
STRQ193	Direct NGI access by a county law enforcement agency shall be through a system equivalent to the ULW.	158.6	Policy
STRQ194	Direct NGI access by a local law enforcement agency shall be through a system equivalent to the ULW.	158.7	Policy
STRQ195	Direct NGI access by a county law enforcement agency shall require the consent of the state.	158.8	Policy
STRQ196	Direct NGI access by a local law enforcement agency shall require the consent of the state.	158.9	Policy
STRQ197	The latent examiner shall have the choice of searching either fingerprint latents or palmprint latents or both.	163	NGI - Design
STRQ209	IAFIS shall be able to retrieve multiple fingerprint and palmprint images for an FBI number.	172.2	NGI - Design
STRQ221	NGI shall provide specific instructions are available as to what action is to be taken following a hit on the ETIS repository	183	NGI - Design
STRQ241	IAFIS shall send a message, such as "no candidates found" when a name search is negative; currently a negative name search sends back no information or messages.	202	NGI - Design
STRQ261	LPW shall take no longer than 5 seconds to update a screen.	215.1	NGI - Design
STRQ262	LPW shall take no longer than 5 seconds to display a screen.	215.2	NGI - Design
STRQ277	IAFIS shall utilize the palmprint to supplement lights out processing for a fingerprint where the fingerprint quality is poor/insufficient.	226.2	NGI - Design
STRQ280	IAFIS shall update the structure of the ULF to be closer to the structure of the SLC file.	229	NGI - Design
STRQ288	AFIT shall provide searchable knowledge base help indexes.	236.1	Policy
STRQ305	IAFIS shall provide a more interactive method for retrieving rap sheet information, such as can be provided by web services.	252	NGI - Design
STRQ307	IPS shall provide the ability to use XML as the means for interaction with the users through a more interactive	254	NGI - Design

STRQ ID (RVTM)	Stakeholder Request Text	User Concept (REQID)	Issue
	interface.		
STRQ311	When NGI identifies a criminal subject, the system shall generate a NCIC name check for criminal warrants and return the results to the booking agency.	257.1	Policy
STRQ317	IAFIS shall retain fingerprints despite quality.	262	Policy
STRQ335	IAFIS shall provide the ability to perform simultaneous searches against the state and FBI repositories.	279	Policy
STRQ341	IAFIS shall support Global Justice XML Data Model (GJXDM) for all submissions and responses.	283	NGI - Design
STRQ359	IAFIS shall allow latent examiners to retrieve multiple images from the ULF list with all the SIDs and TCNs associated with the candidate FNU.	301	NGI - Design
STRQ370	ETIS shall provide some level of classification of why a person should be held.	313	NGI - Design
STRQ393	IAFIS shall provide standardized internet protocols for routing the messages from NGI back to the ORI.	331	NGI - Design
STRQ394	IAFIS shall optionally provide the SRE response and the rap sheet in XML format.	332	NGI - Design
STRQ398	The ORI tables shall be the same in all the different CJIS systems.	336	Policy
STRQ406	IAFIS shall allow local agencies to connect directly to NGI for submissions other than tenprint, bypassing the state, provided the state gives its permission.	345	Policy
STRQ414	The functionality provided in ULW shall be changed to provide the functionality available in LPW.	359	Policy
STRQ451	Civil submissions that result in a hit against the ETIS shall be reported to the STIC (State Terrorism Information Center)	397	Policy
STRQ477	The images shall be available through the "Imaging" file in NCIC by supplying the FNU. Optional retrieval fields shall include date of arrest, date photo taken, date photo submitted.	449.2	NGI - Design
STRQ530	The NPPS shall be a fully automated service within NGI.	471.5	NGI - Design
STRQ547	IAFIS shall support multiple level and modes of sending and receiving information to external users.	492	NGI - Design
STRQ548	IAFIS shall support multiple level and modes of sending and receiving information to external users.	492	NGI - Design
STRQ549	ULW shall allow the submission of a latent search without ridge counting.	493	Policy
STRQ552	IAFIS shall provide the users with the capability to edit and maintain their information via a web-based solution or thin client.	497	NGI - Design
STRQ568	IAFIS shall provide a method to update photos, palms, fingerprints with a single transaction.	513	NGI - Design

STRQ ID (RVTM)	Stakeholder Request Text	User Concept (REQID)	Issue
STRQ585	IAFIS shall target the compression ratio to no more than 10:1 for JPEG 2000 and WSQ images.	527.3	NGI - Design
STRQ600	'IAFIS shall allow the storage of all friction ridge details.	535.2	NGI - Design
STRQ628	IAFIS shall return more demographic information on the ERRT transactions.	556.1	NGI - Design
STRQ629	IAFIS shall return more demographic information on the SRE transactions.	556.2	NGI - Design
STRQ655	The ULW system shall be able to launch more than one latent search per case at a time.	584	Policy
STRQ657	The ULW shall notify the user when a download has taken place.	586.1	Policy
STRQ658	The ULW shall notify the user when a system update has taken place.	586.2	Policy
STRQ673	IAFIS shall accept less than perfect biometric data.	602.1	Policy
STRQ674	IAFIS shall provide limited search capabilities against less than perfect biometric data.	602.2	Policy
STRQ676	IAFIS shall have the ability to export ETIS data for developing and cleaning up VGTOF such that all data is up to date and accurate in all sources.	604	Policy
STRQ699	IAFIS shall provide the ability to receive dispositions directly from the state courts with the SIB's permission. IAFIS shall send the record if requested by the state.	633	Policy
STRQ716	IAFIS shall expedite the work flow of acceptance, retention, examination and reply for digital latent image searches (palmprints) to latent examiners for a positive identification, back to the requesting office for investigative action.	651.2	Policy
STRQ723	IAFIS shall provide access to FBI Field Offices with the same NGI civil functionality as the state law enforcement agencies.	658.1	Policy
STRQ724	IAFIS shall provide access to FBI Field Offices with the same NGI criminal functionality as the state law enforcement agencies.	658.2	Policy
STRQ725	IAFIS shall provide access to FBI Field Offices with the same NGI latent functionality as the state law enforcement agencies.	658.3	Policy
STRQ728	IAFIS shall allow Federal contributors (e.g. FBI Field Offices) to also bulk submit photos.	661	Policy
STRQ761	IAFIS shall be able to accept transactions and route returns over a VPN over LEO.	689	NGI - Design
STRQ768	IAFIS shall have the ability to search the "meta data" or text based fields on the special photo populations.	695	NGI - Design
STRQ777	IAFIS shall have algorithms that adapt based on the best input of flat prints being submitted, allowing the best flat prints to automatically be kept as a master file on an individual.	702.1	NGI - Design

STRQ ID (RVTM)	Stakeholder Request Text	User Concept (REQID)	Issue
STRQ778	IAFIS shall have algorithms that adapt based on the best input of rolled prints being submitted, allowing the best rolled prints to automatically be kept as a master file on an individual.	702.2	NGI - Design
STRQ783	IAFIS shall allow parallel searching for names and palmprints.	705.2	NGI - Design
STRQ797	IAFIS shall initially use the ULW for AFIT and add features.	717.1	Policy
STRQ798	IAFIS shall initially use the ULW for AFIT and NPPS and add features. In subsequent phases AFIT and NPPS would transition to a new system.	717.2	Policy
STRQ803	The NGI system shall be flexible and include multimodal biometrics by 2010.	722	NGI - Design
STRQ809	The IAFIS shall provide wireless connectivity to CJIS.	729	NGI - Design
STRQ875	IAFIS shall address the official retention periods for all NGI records and plan for migration of the records to maintain authenticity, accessibility, and validity for the life of the records.	795	Policy
STRQ881	IAFIS shall add network and host based intrusion detection systems.	801	NGI - Design
STRQ882	IAFIS shall add real time alerting of security relevant activities.	802	NGI - Design
STRQ883	IAFIS shall improve security controls on existing application code.	803	NGI - Design
STRQ886	IAFIS shall ensure Special Stops Group has the capability of adding a SPF to the Mug Shot Record captured within NGI	806	NGI - Design
STRQ891	IAFIS shall ensure to route any PPR transactions to the Special Stops Log when the image is identified with any Special Stops SPF.	811	NGI - Design
STRQ908	AFIS and NPPS systems shall be integrated.	829	NGI - Design
STRQ912	IAFIS shall provide a Service Oriented Architecture.	834	NGI - Design
STRQ916	IAFIS shall allow IPS to interface with NCIC.	838	NGI - Design
STRQ918	IAFIS shall have multi-modal biometric fusion.	843	NGI - Design
STRQ919	NGI' architecture shall allow a face recognition engine to be easily added.	844	NGI - Design
STRQ921	IAFIS shall provide a scalable, multimodal framework that provides "plug and play" for new biometrics and technologies.	845.1	NGI - Design
STRQ934	IAFIS shall provide a scalable, expandable, flexible framework to support multi-modal biometric search and fusion, that is easily maintained.	860	NGI - Design
STRQ943	IAFIS shall provide standard web services.	867	NGI -

STRQ ID (RVTM)	Stakeholder Request Text	User Concept (REQID)	Issue
			Design
STRQ961	IAFIS shall offer different levels of search that will accept fewer than 10 fingerprints for searching at the cost of increased inaccuracy.	885	NGI - Design
STRQ984	The NGI transaction for estimating the search penetration for the ULW shall be made accurate.	913	Policy
STRQ990	ULW shall provide more meaningful error messages that explain the problem.	919	Policy
STRQ1005	All composite palm records shall note the origin from which each palm segment originated.	935	NGI - Design
STRQ1028	IAFIS shall store Court Case Number when submitting fingerprint-based disposition information to NGI.	959	NGI - Design
STRQ1033	IAFIS shall include source (ORI) of any photos when distributing photos.	964	NGI - Design
STRQ1035	IAFIS shall create linkages between palm and fingerprints such that palmprints that are collected can be linked to 10-prints captured later.	966	NGI - Design
STRQ1085	NGI should be capable of receiving, fingerprint images which do not meet target thresholds for quality.	1032.1	Policy
STRQ1086	NGI should be capable of retaining fingerprint images which do not meet target thresholds for quality.	1032.2	Policy
STRQ1095	IAFIS shall use the NIST fingerprint image quality standard to direct the workflow of a submission.	1043	NGI - Design
STRQ1101	IAFIS shall provide an initial automated minutiae/vector placement and search.	1049	NGI - Design
STRQ1103	IAFIS shall limit the number of latent palmprints that can be submitted at one time.	1051	NGI - Design
STRQ1109	IAFIS shall have the ability to search old latent cases.	1062	NGI - Design
STRQ1144	IAFIS shall provide more detailed information about the digital fingerprint image, such as impression code (livescan, inked, etc.), initial capture resolution (500 or 1000 ppi), stored resolution, or the compression technique or rate, with state's permission.	1133	NGI - Design
STRQ1174	The system shall require that the nationality (Country of Citizenship) field be completed on submissions.	266	NGI - Design
STRQ1177	IAFIS shall increase the number of charges per arrest/court cycle from 40 to unlimited.	*	NGI - Design
STRQ1178	IAFIS shall resolve hanging dispositions created with a default arrest cycle.	*	NGI - Design
STRQ1179	IAFIS shall perform fingerprint identification search requests against all individual event fingerprint features (non-composite) including plain impressions.	*	NGI - Design
STRQ1180	Capability to distinguish criminal justice or non-criminal justice Rap Back for User Fee billing purposes.	*	NGI - Design

A.2 Interoperability Design Requirements

Upon review, these requirements were identified to have immediate design level implications. The Business Requirements included in the following table are jointly held between FBI/CJIS, DHS/US-VISIT, and the Department of State (DOS)/Bureau of Consular Affairs (BCA). The Business Requirement included here are under strict CM control and cannot be changed without concurrence from the Business Requirements leads from FBI/CJIS, DHS/US-VISIT, and DOS/BCA. These requirements are contained in the table below to ensure that they are addressed during system design. These requirements must be carried into system design and included in subsequent development documentation.

The following describe the Table A-2 headings:

- Design Number (L#) - This column is an identifying number for the design issue.
- Requirement Text - This column represents the design issue text.
- Traced-From - This column identifies the source of the requirement.
- Business Requirement Number (BR#) - This column represents the jointly managed business requirements from which the design issue is traced.

Table A-2 Interoperability Design Level Business Requirements

D #	Requirement text	Comment	Traced-from	BR #
D1	The IAFIS shall retain audit records for no less than three years.		FEAT266	BR376
D4	The IAFIS shall accept the following data from IDENT when an individual with an active want is encountered: Encounter ID, Encounter Timestamp, FNU (if available), SID or ARN (if available), Location.		FEAT325	BR435
D5	The IAFIS shall create an Nlets administrative message to the wanting agency containing the following: Date, ICN, FNU, Master Name, DOB, DOA or Encounter, SID or ARN, Name of person wanted, Case Number, NCIC Number.		FEAT326	BR436
D6	The IAFIS shall require all IAFIS input data to be formatted in accordance with the IAFIS Interface Control Document/Message Definition Database.	Specific to IAFIS input data from the IDENT external system.	FEAT347	BR449
D9	The IAFIS shall return data generated by IDENT in the ISS element of the message.		FEAT224	BR335

D #	Requirement text	Comment	Traced-from	BR #
D12	The IAFIS shall accept an ISS of IDENT subject biographic information which includes the enumerator of that individual and the encounter history including: Encounter Event(s) (e.g. Arrival, Extension, Returned), Date of Encounter(s), Location(s) of Encounters, Class(es) of Admission (e.g. Tourist, Student), Admitted Until date(s), Document(s) Used (e.g. Visa, I-94), Approval(s) and Denial(s) of Request to the end user as available.	Returned data items are forwarded with no validation.	FEAT150	BR221
D13	The IAFIS shall be able to provide a report to IDENT on the biometrically-linked enumerated information on an individual.		FEAT289	BR399
D14	The IAFIS shall return any biometrically-linked information on an enumerated individual based on a request from IDENT: Digital Facial photo, - Minimum biographic information- First Name, Last Name, DOB, FNU, ARN, - Social Security, - Physical descriptors, - Sex, - Race, - Height, - Eye Color, POB, - Country of Citizenship, - Additional DOB(s), - SMT, - FBI Rap sheet - Arrest Records (Charges of Crimes), Disposition (Convictions), Federal Wants and Warrants, Supervision or Custody (Flashes), Sexual Registration, KST information.		FEAT31, FEAT56, FEAT57, FEAT58, FEAT59, FEAT150	BR49, BR83, BR84, BR85, BR86, BR221
D15	The IAFIS shall return the following data for a biometrically-linked enumerated individual to IDENT: FBI Rap Sheet - Arrest Records (Charges of Crimes), Disposition (Convictions), Federal Wants and Warrants, Supervision or Custody (Flashes), Sexual Registration, KST Information.		FEAT235, FEAT291	BR346, BR401
D16	The IAFIS shall accept additional biometrically-linked immigration information from IDENT for to international, federal, state, and local law enforcement and authorized non-criminal justice agencies to include the following:- Digital facial photo- Minimum biographic information - First Name, Last Name, DOB, Gender, Associated identity document number (e.g., passport numbers, BCC number), Document Issuing Authority (e.g., country or state)- Enumerator- Other biographic information that currently exists within IDENT - AKA, Associated Number(s), FNU, ARN, Social Security, Visa Number, Additional Number(s) and Sources, Biographic Descriptors, Sex, Race, Skin Tone, Height, Eye Color, POB, Country of Citizenship, Additional DOB(s), SMT, IDENT Administrative Information - Event, Date, Location, Class of Admission, Admitted Until, Document Used - IDENT Criminal Arrests - Arrest		FEAT150	BR221

D #	Requirement text	Comment	Traced-from	BR #
D17	The IAFIS shall provide IDENT biometrically-linked immigration information to international, federal, state, and local law enforcement and authorized non-criminal justice agencies for individuals to include the following:- Digital facial photo- Minimum biographic information - First Name, Last Name, DOB, Gender, Associated identity document number (e.g., passport numbers, BCC number), Document Issuing Authority (e.g., country or state) - Enumerator- Other biographic information that currently exists within IDENT - AKA, Associated Number(s), FNU, ARN, Social Security, Visa Number, Additional Number(s) and Sources, Biographic Descriptors, Sex, Race, Skin Tone, Height, Eye Color, POB, Country of Citizenship, Additional DOB(s), SMT, IDENT Administrative Information - Event, Date, Location, Class of Admission, Admitted Until, Document Used	Provide what IDENT gives us without modifying their response.	FEAT150	BR221
D18	The IAFIS shall return an ISS of IDENT subject biographic information which includes the enumerator of that individual and the encounter history included Encounter Event(s) (e.g. Arrival, Extension, Returned), Date of Encounter(s) , Location(s) of Encounters , Class(es) of Admission (e.g. Tourist, Student), Admitted Until date(s), Document(s) Used (e.g. Visa, I-94), Approval(s) and Denial(s) of Request to the end user as available.	Provide what IDENT gives us without modifying their response.	FEAT150	BR221
D19	The biometrics and associated FNUs of IAFIS Wanted Persons shall be included in the GCDS.		FEAT276	BR386
D20	The biometrics and associated FNUs of IAFIS KST shall be included in the GCDS.		FEAT276	BR386
D21	The biometrics and associated FNUs of NCIC IVF shall be included in the GCDS.		FEAT276	BR386
D22	The IAFIS shall have the ability to receive information linked to the enumerator, such as: Event (e.g. Arrival, Extension, Returned), Date, Location , Class of Admission (e.g. Tourist, Student), Admitted Until, Document Used (e.g. Visa, I-94), Approval/Denial of Request.		FEAT42	BR61
D26	The IAFIS shall store multiple values for citizenship and place of birth information when data sets are available.		FEAT51	BR78
D28	The IAFIS shall provide dedicated communication lines between the IAFIS and IDENT systems.		FEAT109	BR166
D30	The IAFIS shall log the reason a linked record is changed.		FEAT151	BR232

D #	Requirement text	Comment	Traced-from	BR #
D31	The IAFIS shall log modification date, time, and authorized user ID for maintenance activities of a linked record.		FEAT151	BR232
D32	The IAFIS shall log the reason a record modification is made to jointly held biometric information.		FEAT151	BR232
D33	The IAFIS shall provide the ability to report on the number of identifications of IAFIS criminal and civil records with latent prints submitted by DHS authorized agencies.		FEAT89	BR146
D34	The IAFIS shall create an Activity Log of de-linked records.		FEAT279	BR389
D35	The IAFIS shall provide agency-to-agency audit trails for data receipt, maintenance, storage, dissemination, and use of shared data.		FEAT106	BR163
D36	The IAFIS shall provide audit trails for the receipt of the biographic, criminal and immigration history data, from the IDENT system.		FEAT106	BR163
D37	Any audit trail maintained by the IAFIS shall include timestamps of the activities or events being tracked.		FEAT106	BR163
D38	The IAFIS shall provide audit details of transaction history including the following: - Unique Identifier - Date Processed - Time Processed.		FEAT268	BR378
D39	The IAFIS shall provide an audit record of individuals that perform actions in the system.		FEAT269	BR379
D40	The IAFIS shall provide an audit record of the actions that individuals perform in the system.		FEAT270	BR380
D41	The IAFIS shall provide an audit record of the actions performed by the system.		FEAT271	BR381
D42	IAFIS shall provide the ability to report on the length of time it takes to forward a specific query to IDENT.		FEAT345	BR447
D43	IAFIS shall provide the ability to report on the length of time for a response to return to IAFIS after having been forwarded to IDENT.		FEAT345	BR447
D44	IAFIS shall provide the ability to report on the length of time to process a response from IAFIS and IDENT.		FEAT345	BR447
D45	The IAFIS shall provide the ability to report on the time required to respond to search request from DHS authorized agencies.		FEAT102	BR159
D46	The IAFIS shall provide the ability to report on the number of service requests by agency.		FEAT104	BR161
D47	The IAFIS shall provide the ability to report on the number of positive identifications resulting from service requests by agency.		FEAT104	BR161

D #	Requirement text	Comment	Traced-from	BR #
D48	The IAFIS shall provide the ability to report on the number of service requests to IAFIS from IDENT.		FEAT104	BR161
D49	The IAFIS shall provide the ability to report on the number of service requests from IDENT received by IAFIS.		FEAT104	BR161
D50	The IAFIS shall provide the ability to report on the number of positive identifications resulting from IAFIS service requests from IDENT.		FEAT104	BR161
D51	The IAFIS shall provide the ability to report on the number of positive identifications resulting from IDENT service requests from IAFIS.		FEAT104	BR161
D52	The IAFIS shall provide the ability to report on the number of rejected service requests by agency.		FEAT104	BR161
D53	The IAFIS shall provide the ability to report on the number of rejected service requests from IDENT to IAFIS.		FEAT104	BR161
D54	The IAFIS shall provide the ability to report on the number of rejected service requests from IAFIS to IDENT.		FEAT104	BR161
D55	The IAFIS shall report on the number of automatic verification and the number of manual verification for the Tenprint submissions.		FEAT126	BR184
D57	The IAFIS shall provide the ability to report on the IAFIS response time to the IDENT requests.	This is how long it takes IAFIS to process a request from IDENT.	FEAT346	BR448

D #	Requirement text	Comment	Traced-from	BR #
D59	The IAFIS shall return any biometrically-linked information on an enumerated individual to a end-user (DOS consular official): - IDENT data provided (e.g., Digital facial photo - IDENT watchlist and recidivist information - Minimum biographic information - First Name, Last Name, DOB, Gender, Associated Identity Document Number (e.g., passport numbers, BCC number), Document Issuing Authority (e.g., country or state) - Enumerator - Other biographic information that currently exists within IDENT - AKA, Associated Number(s), FNU, ARN, Social Security, Visa Number, Additional Number(s) and Sources, Biographic Descriptors, Sex, Race, Skin Tone, Height, Eye Color, POB, Country of Citizenship, Additional DOB(s), SMT) - FBI Rap Sheet - Arrest Records (Charges of Crimes), Disposition (Convictions), Federal Wants and Warrants, Supervision or Custody (Flashes), Sexual Registration, KST Information		FEAT283	BR393
D60	The IAFIS shall return any biometrically-linked information on an enumerated individual to end-user (POE secondary): IDENT data provided (e.g., - Digital facial photo)- IDENT watchlist and recidivist information- Minimum biographic information - First Name, Last Name, DOB, Gender, Associated Identity Document Number (e.g., passport numbers, BCC number), Document Issuing Authority (e.g., country or state)- Other biographic information that currently exists within IDENT - AKA, Associated Number(s), FNU, ARN, Social Security, Visa Number, Additional Number(s) and Sources, Biographic Descriptors, Sex, Race, Skin Tone, Height, Eye Color, POB, Country of Citizenship, Additional DOB(s), SMT -Crossing History Information (e.g., admission date, class of admission. Data should be sorted by most recent encounter)) - FBI Rap Sheet - Arrest Records (Charges of Crimes), Disposition (Convictions), Federal Wants and Warrants, Supervision or Custody (Flashes), Sexual Registration, KST Information.		FEAT285	BR395

D #	Requirement text	Comment	Traced-from	BR #
D61	The IAFIS shall return any biometrically-linked information on an enumerated individual to an end-user (ICE agent): - IDENT data provided (e.g., Digital facial photo - IDENT watchlist and recidivist information - Minimum biographic information - First Name, Last Name, DOB, Gender, Associated Identity Document Number (e.g., passport numbers, BCC number), Document Issuing Authority (e.g., country or state) - Enumerator - Other biographic information that currently exists within IDENT - AKA, Associated Number(s), FNU, ARN, Social Security, Visa Number, Additional Number(s) and Sources, Biographic Descriptors, Sex, Race, Skin Tone, Height, Eye Color, POB, Country of Citizenship, Additional DOB(s), SMT) - FBI Rap Sheet - Arrest Records (Charges of Crimes), Disposition (Convictions), Federal Wants and Warrants, Supervision or Custody (Flashes), Sexual Registration, KST Information		FEAT286	BR396

D #	Requirement text	Comment	Traced-from	BR #
D62	The IAFIS shall return any biometrically-linked information on an enumerated individual to a end-user (USCIS adjudicator):IDENT data provided (e.g., - Digital facial photo- IDENT watchlist and recidivist information- Minimum biographic information - First Name, Last Name, DOB, Gender, Associated Identity Document Number (e.g., passport numbers, BCC number), Document Issuing Authority (e.g., country or state)- Enumerator- Other biographic information that currently exists within IDENT - AKA, Associated Number(s), FNU, ARN, Social Security, Visa Number, Additional Number(s) and Sources, Biographic Descriptors, Sex, Race, Skin Tone, Height, Eye Color, POB, Country of Citizenship, Additional DOB(s), SMT) - FBI Rap Sheet - Arrest Records (Charges of Crimes), Disposition (Convictions), Federal Wants and Warrants, Supervision or Custody (Flashes), Sexual Registration, KST Information		FEAT287	BR397

D #	Requirement text	Comment	Traced-from	BR #
D63	The IAFIS shall return any biometrically-linked information on an enumerated individual to an end-user (officer who makes decisions regarding registered travelers):IDENT data provided (e.g., - Digital facial photo)- IDENT watchlist and recidivist information- Minimum biographic information - First Name, Last Name, DOB, Gender, Associated Identity Document Number (e.g., passport numbers, BCC number), Document Issuing Authority (e.g., country or state)- Enumerator- Other biographic information that currently exists within IDENT - AKA, Associated Number(s), FNU, ARN, Social Security, Visa Number, Additional Number(s) and Sources, Biographic Descriptors, Sex, Race, Skin Tone, Height, Eye Color, POB, Country of Citizenship, Additional DOB(s), SMT) - FBI Rap Sheet - Arrest Records (Charges of Crimes), Disposition (Convictions), Federal Wants and Warrants, Supervision or Custody (Flashes), Sexual Registration, KST Information		FEAT288	BR398

D #	Requirement text	Comment	Traced-from	BR #
D64	The IAFIS shall return any biometrically-linked information on an enumerated individual to an end-user (DOS consular official): IDENT data provided (e.g., Digital facial photo) IDENT watchlist and recidivist information Minimum biographic information- First Name, Last Name, DOB, Gender, Associated identity Document Number (e.g., passport numbers, BCC number) Document Issuing Authority (e.g., country or state) Enumerator Other biographic information that currently exists within IDENT- AKA, Associated Number(s), FNU, ARN, Social Security, Visa Number, Additional Number(s) and Sources, Biographic Descriptors, Sex, Race, Skin Tone, Height, Eye Color, POB, Country of Citizenship, Additional DOB(s), SMT FBI Rap Sheet - Arrest Records (Charges of Crimes), Disposition (Convictions), Federal Wants and Warrants, Supervision or Custody (Flashes), Sexual Registration, KST Information. IAFIS civil history information.		FEAT52	BR79

D #	Requirement text	Comment	Traced-from	BR #
D65	The IAFIS shall return any biometrically-linked information on an enumerated individual to an end-user (POE officer at secondary): IDENT data provided (e.g., Digital facial photo) IDENT watchlist and recidivist information Minimum biographic information-First Name, Last Name, DOB, Gender, Associated Identity Document Number (e.g., passport numbers, BCC number), Document Issuing Authority (e.g., country or state), Other biographic information that currently exists within IDENT-AKA, Associated Numbers(s), FNU, ARN, Social Security, Visa Number, Additional Number(s) and Sources, Biographic Descriptors, Sex, Race, Skin Tone, Height, Eye Color, POB, Country of Citizenship, Additional DOB(s), SMT) Crossing History Information (e.g; admission date, class of admission. Data should be sorted by most recent encounter). FBI Rap Sheet - Arrest Records (Charges of Crimes), Disposition (Convictions), Federal Wants and Warrants, Supervision or Custody (Flashes), Sexual Registration, KST Information. IAFIS civil history information.		FEAT31, FEAT55	BR49, BR82

APPENDIX B - NGI FUTURE PHASE - CATEGORY 3 STAKEHOLDER REQUESTS

STRQs assigned to category 3 will be considered for implementation as part of NGI Phase II. These STRQs were not decomposed into user or functional requirements in this document. However, Phase I design must not preclude the implementation of these user concepts in Phase II.

User Concept (STRQ ID)	User Concept Text
95	IAFIS shall provide states the capability to query into FBI stored records to get the state's statistical and other information.
111	IAFIS shall be used as a hub to search other state databases for images.
126	The system shall provide a response in a format that supports the capability to consolidate ("federate") responses from parallel searches.
169	IAFIS shall provide expanded latent palm search capability to include latent ridge flows, poreoscopy, and edgeoscopy.
185	IAFIS shall allow identification capability using 2- and/or 4-finger identification with 15 second or less response time
187	IAFIS shall provide a feature to facilitate the exchange of latents, flat prints, and rolled 10-print fingerprints between states, i.e. state fingerprints for offenses that are not sent to the FBI, such as non-criterion misdemeanors
226.1	IAFIS shall utilize the palmprint to supplement lights out processing for a fingerprint where the fingerprint quality is poor/insufficient.

User Concept (STRQ ID)	User Concept Text
230	IAFIS shall provide the capability to conduct a search of a state's repository.
298	IAFIS shall provide a pointer to a higher quality forensic captured photo in a local system.
300	IAFIS shall provide the gateway to DHS, DOS, and DOD databases for extended searches.
306	IPS and NPPS shall provide a pointer to NFF.
310	IAFIS shall organize and provide for data retrieval by state.
364	IAFIS shall utilize ridges in sequence versus minutiae in sequence to conduct search-and-matching.
370	IAFIS shall provide for interoperable minutiae interchange capabilities between IAFIS and existing vendor systems.
371	The CJIS-WAN and LEO shall be enhanced to provide the capability for states to exchange latent print searches with other AFIS systems.
472.3	The NPPS shall provide identification capabilities similar to what is currently available via tenprint.

User Concept (STRQ ID)	User Concept Text
495	IAFIS shall provide the capability to conduct a pattern search of SMT images.
503	The latent workstation shall provide the capability to do a correlation of multiple records when conducting a latent search.
506	IAFIS shall submit a response back to originating agency indicating fingerprint or disposition has been received and accepted for processing, both criminal and civil.
536	IAFIS shall provide the capability to initiate a search of a state's AFIS system with the state's permission.
549	IAFIS shall support an automated notification process for when a state has an arrest without a disposition.
558	IAFIS shall increase the penetration rate to a level above the current 30% while maintaining the current 90-95% accuracy standards.
570	IAFIS shall provide the capability to send latent searches to states so that they (the state) can search their own repository and return the response to the submitting agency.
609	IAFIS shall be interoperable with the Office of Personnel Management (OPM) and perform all transactions electronically.
621.1	IAFIS shall provide an audit trail for all photo inquiries.

User Concept (STRQ ID)	User Concept Text
639	IAFIS shall supply notification to the arresting agency and the case agent when a match is made while searching the Bureau of Prisons (BOP) database for Tenprint submissions.
640	IAFIS shall provide the capability to retain drivers license photos (in IAFIS) from the state through IPS without an FNU.
641	IAFIS shall provide the capability to access drivers license photos (in IAFIS) from the state through IPS without an FNU.
642	IAFIS shall have the capability to retain photos from passports without an FNU to identify Known or Suspected Terrorists (KST).
643	IAFIS shall have the capability to search passport photos without an FNU to identify Known or Suspected Terrorists (KST) using demographic based text searches.
650	The Joint Automated Booking System (JABS) shall be completely interoperable with IAFIS.
652	IAFIS shall allow for access of photos through the Bureau of Prisons (BOP) repository of photos for all states' Law Enforcement Agencies and FBI Field Offices.
659	Tenprint submissions in IAFIS shall initiate an automatic BOP database search.

User Concept (STRQ ID)	User Concept Text
686	Next generation of ITN shall be studied for improvements.
712	IAFIS shall provide the capability for users to do online expungement.
814	IAFIS shall ensure that the applicable federal or state statute for all charges for each arrest cycle per each criminal fingerprint submission be included with the submission.
816	IAFIS shall provide an alternate mechanism for the processing of fingerprint submissions that deviate from the typical submissions processed by the CJIS Divisions.
827.2	IAFIS shall provide a MultiModal framework that will easily support current information sources with future considerations such as iris, palm, flats, and other biometrics to provide fusion from the analysis of multiple biometrics.
831	The IAFIS system shall be able to filter images for best quality.
889	IAFIS shall provide lights out processing for latents.
896	The search time for SMT searches shall be 5 minutes or less.

User Concept (STRQ ID)	User Concept Text
923	IAFIS shall coordinate an III Name search to all State databases for possible matches if no hit in IAFIS.
927	IAFIS shall validate whether the correct photo was received with the submitted fingerprints.
985	The latent workstation shall be able to add an additional characteristic choice of "dot" for characteristics of one or two ridge units.
986	IAFIS shall be able to add an additional characteristic choice of "dot" for characteristics of one or two ridge units for latent searches.
1017	IAFIS shall provide remote access to local agencies with AFIS systems, provided the state gives its permission.
1026	IAFIS shall provide increased lights out processing by fusion with other biometric/demographic matching capabilities.
1046	IAFIS shall apply an image quality metric to photos.

APPENDIX C BIBLIOGRAPHY

1. 5 U.S. Code 552a, Privacy Act of 1974, (Public Law 93-579), December 1974.

2. 40 U.S. Code 759, Computer Security Act of 1987, (Public Law 100-235), January 8, 1988.

3. AAMVA National Standard for the Driver License/Identification Card, American Association of Motor Vehicle Administrators, AAMVA DL/ID-2000, June 30, 2000.

4. American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information Part 1, ANSI/NIST-ITL 1-2007, NIST Special Publication 500-271, April 20, 2007.

5. American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Part 2: XML Version ANSI/NIST-ITL 2-2008, NIST Special Publication 500-275, August 12, 2008.

6. American National Standards Institute (1988), *American National Standard for Forensic Identification - Automated Fingerprint Identification Systems - Glossary of Terms and Acronyms*, ANSI/IAI 2-1988, New York, NY.

7. Assistant Secretary of Defense (1985), *Department of Defense Trusted Computer System Evaluation Criteria*, (TCSEC), DOD 5200.28 STD, Washington, DC.

8. Biometric Data Specification for Personal Identity Verification, NIST Special Publication 800-76, Feb 1, 2006, http://csrc.nist.gov/publications/nistpubs/800-76/sp800-76.pdf.

9. Criminal Justice Information Services Controlled Access Protection Profile (CJISCAPP), Department of Justice, Federal Bureau of Investigation, December 8, 2003.

10. Criminal Justice Information Services (CJIS) Electronic Biometric Transmission Specification, IAFIS-DOC-01078-8.0 Draft, V8.0, 2007.

11. Criminal Justice Information Services (CJIS) Electronic Fingerprint Transmission Specification (EFTS), IAFIS-DOC-01078-7.1, V7.1, May 2, 2005.

12. Department of Defense Computer Security Center (1985), *Department of Defense Password Management*, CSC-STD-002-95, Fort George Meade, MD.

13. Department of Justice Order 2640.2B, *Automated Information Systems Security*, November 16, 1988.

14. Department of Justice Order 2640.3, *Unique Identification and Authentication of Users of Automated Information Systems*, March 30, 1990.

15. Department of Justice (1991), *Code of Federal Regulations Title 28, Part 19*, National Archives and Records Administration, Washington, DC.

16. Federal Bureau of Investigation (2004), *Disposition Submission via Machine Readable Data*, IAFIS-III-DOC-01008-2.0, February 25, 2004.

17. Federal Bureau of Investigation, *Electronic Recordkeeping Certification Manual*, April 30, 2004.

18. Federal Bureau of Investigation (2004), *Expungement Submission via Machine Readable Data*, IAFIS-III-DOC-01007-1.1, October 20, 2003.

19. Federal Bureau of Investigation (FBI), Information Technology Life Cycle Management Directive (IT LCMD) 2.0, November 19, 2004.

20. Federal Bureau of Investigation (2006), *Machine Readable Data (MRD) Name Search Specifications*, IAFIS-DOC-01049-1.2, April 11, 2006.

21. Federal Bureau of Investigation (1979), *The Identification Division of the FBI*, Washington, DC.

22. Federal Bureau of Investigation (FBI), *NCIC 2000 Operating Manual*, December 1999.

23. Federal Bureau of Investigation (1984), *The Science of Fingerprints: Classification and Uses*, Washington, DC.

24. Federal Bureau of Investigation (FBI) Manual of Investigative Operations and Guidelines (MIOG), Part II, Section 35 (FBI ADPT Security Manual), July 26, 1995.

25. ISO/IEC 19794-5:2005, Information technology -- Biometric data interchange formats -- Part 5: Face image data, June 2005.

26. McCabe, R.M., Best Practice Recommendation for the Capture of Mug shots, Version 2.0, Sept 1997, http://www.itl.nist.gov/iad/894.03/face/bpr_mug3.html.

27. Manual of Investigative Operations and Guidelines, Part 2, MIOGP2, July 26, 1995.

28. National Bureau of Standards (1985), NBS Special Publication 500-120, *Security of Personal Computer Systems: A Management Guide*, Washington, DC.

29. National Computer Security Center (1987), *Trusted Network Interpretation*, NCSC-TG-005, Version 1, Fort George Meade, MD.

30. National Technical Information Service (1975), FIPS PUB 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Washington, DC.

31. National Telecommunications and Information Systems Security Committee, National Telecommunications and Information Systems Security Policy, NTISSP No. 200, (1987),

National Policy on Controlled Access Protection, Washington, DC.

32. Next Generation Integrated Automated Fingerprint Identification System – Automated Fingerprint Identification Technology Functional Requirements Document, NGI-DOC-01133-2.0, V2.0, February 2007.

33. Next Generation Integrated Automated Fingerprint Identification System – Biometric Interoperability Program Office Functional Requirements Document, BIO-DOC-01174-2.0, V2.0, February 2007.

34. Next Generation Integrated Automated Fingerprint Identification System – Disposition Reporting Improvements Functional Requirements Document, NGI-DOC-01135-2.0, V2.0, February 2007.

35. Next Generation Integrated Automated Fingerprint Identification System – Enhanced NGI Repository Functional Requirements Document, IAFIS-DOC-01136-2.0, V2.0, February 2007.

36. Next Generation Integrated Automated Fingerprint Identification System – International Terrorist File Shared Services and Data Exchange Functional Requirements Document, NGI-DOC-01184-2.0, V2.0, February 2007.

37. Next Generation Integrated Automated Fingerprint Identification System – Interstate Photo System Functional Requirements Document, NGI-DOC-01131-2.0, V2.0, February 2007.

38. Next Generation Integrated Automated Fingerprint Identification System – National Palmprint System Functional Requirements Document, NGI-DOC-01137-2.0, V2.0, February 2007.

39. Next Generation Integrated Automated Fingerprint Identification System – Quality Check Automation Phase III Functional Requirements Document, NGI-DOC-01134-2.0, V2.0, February 2007.

40. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources,* February 20, 1996.

41. Office of Management and Budget (OMB), Bulletin No. 88-16, *Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information*, Washington, DC., 1988.

42. Office of Management and Budget (1985), Circular No. A-130, Management of Federal Information Resources, Washington, DC.

43. Target Enterprise Architecture, EAPO-DOC-1077-1.1, August 2005.

44. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 65), Guideline for Automatic Data Processing (ADP) Risk Analysis, August 1, 1979.

45. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 73), Guidelines for the Security of Computer Applications, June 30, 1980.

46. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 87), Guidelines for ADP Contingency Planning, March 27, 1981.

47. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 31), Guidelines for Automatic Data Processing Physical Security and Risk Management, June 1974.

48. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 112), Password Usage, May 30, 1985.

APPENDIX D ACRONYMS AND GLOSSARY

See the NGI Acronym List Glossary (NGI-DOC-09064)

APPENDIX E RISC CANDIDATE EVALUATION

Table E-1 RISC Color Indicators

(A) AFIS Match Level of highest ranked candidate	(B) Tier Level of highest ranked candidate	(C) Candidates within corresponding AFIS Match Level	(D) Tier Level(s) within AFIS Match Level	(E) SRF Response	(F) Notify Record Owner (s)
High (Red)	1	Single	Same (1)	Red	Yes
High (Red)	1	Multiple	Same / Mixed	Red[4]	Yes
High (Red)	2	Single	Same (2)	Red	Yes
High (Red)	2	Multiple	Same / Mixed	Red	Yes
High (Red)	3	Single	Same (3)	Green	Yes
High (Red)	3	Multiple	Mixed	Red[5]	Yes
High (Red)	3	Multiple	all 3's	Green	Yes

[4] The UCN of the highest ranked candidate is returned in the 2.014-FBI field. The 2.071-ACN field will contain: other tier one / tier two UCNs above the high confidence threshold, a caveat that these UCNs are possible consolidations, the corresponding record type of each high confidence UCN and any related tier two contact information. When requested, the 2.075-ERS field will contain the UCN and corresponding criminal history information for all tier one UCNs above the high confidence threshold.

[5]When the highest ranked candidate is a tier three record, the next highest non tier three UCN will be returned in the 2.014-FBI field. The 2.071-ACN and 2.075-ERS fields will follow the same rules described in footnote one above.

(A) AFIS Match Level of highest ranked candidate	(B) Tier Level of highest ranked candidate	(C) Candidates within corresponding AFIS Match Level	(D) Tier Level(s) within AFIS Match Level	(E) SRF Response	(F) Notify Record Owner (s)
Middle (Yellow)	1	Single	Same (1)	Yellow	No
Middle (Yellow)	1	Multiple	Same / Mixed	Yellow	No
Middle (Yellow)	2	Single	Same (2)	Yellow	No
Middle (Yellow)	2	Multiple	Same / Mixed	Yellow	No
Middle (Yellow)	3	Single	Same (3)	Green	No
Middle (Yellow)	3	Multiple	Mixed	Yellow	No
Middle (Yellow)	3	Multiple	all 3's	Green	No
Low (Green)	1, 2 or 3	Single / Multiple	Same / Mixed	Green	No

When multiple agencies enter the same UCN into RISC, a "Red" light response's tier level should be based on the least restrictive tier level. However, all agencies should be notified. The record type returned in the response should be based on a configurable priority list. See the following chart for an example of multiple agencies entering a record with the same UCN into RISC.

Table E-2 RISC color example

Agency	Tier Level	Record Type
1	3	KST
2	**1**	**W&W**
3	2	KST
4	1	SOR
5	3	KST

In the above example, an AFIS match with only this UCN above the high confidence threshold would result in a Tier 1 "Red" light with a record type of W&W (assumes W&W is the highest priority in the record type priority list) being returned in the response while all five entering agencies would receive a notification that this record had been hit upon.

APPENDIX F REQUIREMENTS VERB USAGE

The following are brief descriptions of the verbs used in the functional requirements within this document. While the usage of these verbs is in harmony with their dictionary definitions, these descriptions provide a more relevant explanation of their use within the context of the requirements.

Accept

These requirements refer to NGI receiving a message from an Authorized Contributor (e.g., accept...from) or allowing a piece of information within a message (e.g., accept...as part of). When accept is used in reference to a piece of information, it is generally true that the information is allowed, but not required.

Advise

These requirements describe passing specific information to an end-user, where a dedicated notification message is not used. Although design is not dictated, the information may be part of a broader user response or, in the case of an FBI Service Provider, may be provided on-screen or through the use of workflow queues.

Allow

This is used to indicate that NGI is giving a capability to an end-user. Allow almost exclusively applies to FBI Service Providers, with the "accept...from" model being used for Authorized Contributors; however, there are requirements that give a specific capability within a function that use allow in reference to Authorized Contributors. (e.g., NGI shall allow an Authorized Contributor to add supplemental biographic identifiers as part of a III Record Maintenance request.)

Apply

This is used solely in conjunction with dissemination rules, and indicates that the rules will be considered before providing responses or notifications to end users.

Assign

In general, these requirements indicate that NGI is either giving a data item a default value, or using a user-supplied value.

Associate

These requirements indicate the creation of a logical relationship among individual data elements or groups of elements. No database design is inferred or precluded, but rather there is a functional need for the relationship.

Calculate

These requirements indicate some form of mathematical computation, which is necessary to fulfill subsequent functional requirements.

Collect

These Administration and Control requirements indicate information that will be gathered, either in real-time or offline, and brought together in a manner that will facilitate status and reporting functionality.

Combine

These requirements refer to the joining of response information from external sources with NGI' own Identity information to form a single NGI response. The response data may be merged or appended as appropriate.

Compare

These requirements are solely to indicate a one to one comparison of fingerprint features performed by NGI.

Comply

These requirements will reference standards, policies, laws, requirements or rules that are external to NGI. These requirements indicate adherence to the stated external reference.

Create

These requirements indicate the ability for NGI to generate and/or store information.

Delete

These requirements indicate that a data item or group of data items should be removed from NGI. This does not infer a permanent database deletion, nor does it preclude the retention of the data in a manner that renders it un-accessible by end-users should there be such a system need.

Determine

These requirements indicate that NGI will come to a decision by applying business rules or performing calculations before continuing with the current operation.

Eliminate

These requirements are associated with a specific NGI candidate list and indicate that the candidate(s) that meet defined criteria should be removed from further consideration as they relate to the named candidate list.

Enroll

These requirements indicate the addition of new data into NGI. This could include data added to one of the main repositories as well as any associated information.

Extract

These requirements indicate that a feature extraction algorithm will be applied to fingerprint images. The features are necessary to support subsequent requirements.

Filter

These requirements indicate a process of removing a subset of a search population from consideration based upon defined criteria.

Forward

These requirements indicate that a response received from an external source is going to be passed along to the original requestor.

Include

These requirements are associated with a specific piece of information that must be made a part of the request/response. When preceded by "optionally", this indicates that a specific piece of information will be made a part of the request/response when a prior condition has been met.

Indicate

These requirements are associated with the ability to provide specific information in a request/response related to a condition or selection.

Maintain

This indicates NGI creating/updating/or deleting information.

Manage

This refers to the supervision of a transaction as it is processed through NGI. These requirements imply the functional need for NGI workflow management.

Mark

These requirements reflect a functional need for an indicator to be associated with a data item or group of items, or an NGI transaction. Subsequent functional requirements will refer to the specific data item as marked or unmarked when applicable.

Modify

This indicates the carrying out of an end-user's request to modify the status of their Latent Searches.

Perform

These requirements indicate an action to be taken by NGI.

Prioritize

These requirements state a functional need for requests to have varying priorities, based on established or specified criteria, and to be processed according to those priorities.

Provide

Provide is used in many different contexts; "Provide the capability" defines functionality required by NGI to satisfy an end-user need or subsequent system need. Provide is also used to indicate a response being supplied to an end-user, or to state the inclusion of specific data items in a response.

Re-associate

This implies a previous association between data items or groups of items. These requirements indicate that the previous association will be removed and a new association will be created using one or all of the data items.

Record

These requirements indicate that a data item or message will be stored within NGI, for the purpose of satisfying a subsequent user or system need. Examples are biometric decisions and disseminations.

Reject

This is used primarily to indicate an automated reject by the NGI system. A "when" or "if" in the requirement will generally indicate the cause of the reject. Reject is also used to indicate that enrollment of supplementary information (e.g., biometrics, rap back subscriptions) should not occur when the containing transaction is rejected.

Replace

This indicates the complete substitution of one data item or a group of items with another.

Report

These requirements indicate information regarding system or communications status that will be provided to System Administrators.

Require

These requirements indicate that a particular data item is mandatory in order for NGI to process a message, or that a specific step in a process is mandatory.

Restore

These requirements refer to returning Identity History data to a previous state.

Retain

This indicates the preservation of transaction, performance, and/or administrative data for the purpose of historical reporting.

Retrieve

These requirements indicate the obtaining of information from NGI repositories, usually to support subsequent requirements which include this information on a user response.

Search

Search indicates the carrying out of a user or system request to search NGI repositories. This refers to the actual biometric or biographic search process at the lowest functional level.

Send

This indicates NGI initiating a request to an external system or providing a notification to an end-user or system.

Support

These are Administrative and Control requirements used to indicate system functionality that is necessary to provide all user services.

Update

These requirements indicate a change to previously stored data items or groups of items.

Validate

This is to indicate that NGI will confirm that specific conditions exist prior to carrying out a user request.

Write