BIOMETRICS
TASK FORCE

Biometric Collection, Transmission and Storage Standards

Technical Reference

24 July 2006
Version 1.1

Department of the Army
Biometrics Task Force
Executive Agent for Biometrics

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
24 JUL 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Biometric Collection, Transmission and Storage Standards	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of the Army Biometrics Task Force Executive Agent for Biometrics Arlington, VA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**29**	

Document History

Version	Date	Document Status	Participants/Comments
0.1	25 Apr 2006	Working Draft	Internal Reviews
0.2	23 May 2006	Working Draft	Presented to BSWG; editorial changes
0.3	26 May 2006	Working Draft	Editorial changes
0.4	05 Jun 2006	Working Draft	Editorial changes and additional comments from peer review integrated
0.5	06 Jun 2006	Working Draft	CBEFF concerns resolved, sent to technical editor
0.6	07 Jun 2006	Working Draft	Distributed to BSWG for two-week review; technical edits integrated
1.0	21 Jul 2006	Working Draft	Incorporated comments from BSWG based on the approved disposition of comments
1.1	24 Jul 2006	Released version	Edition includes comments from BTF technical editor

Contact Information

For comments or questions, please contact:

Dale Hapeman, DoD Biometrics Task Force Standards Team, 304-326-3029
James B. Hutchinson, DoD Biometrics Task Force Standards Team, 703-984-0430

Executive Summary

This document provides a comprehensive technical reference that lists published biometric standards and describes their applicability to the biometric functions described in the Capstone Concept of Operations (CONOPS) for Department of Defense (DoD) Biometrics in Support of Identity Superiority. It was prepared by the DoD Biometrics Standards Working Group (BSWG) to assist in the development of future system-specific policy and technical documents, such as standard operating procedures, architecture technical views, and application profiles. This document provides support for a number of biometric modalities, including: fingerprints, face images, iris images, signature/sign data, hand geometry, and palm prints. It also describes the status of biometric standards in the DoD Information Technology Standards Registry. The appendices of this document contain a brief overview of the criteria for DoD adoption of standards and information on the collection of non-standardized biometric data, including DNA and voice recording samples. The DoD BSWG will update this document on a regular basis as new biometric standards emerge and to maintain consistency with the CONOPS.

Table of Contents

1 Introduction

1.1 Authority

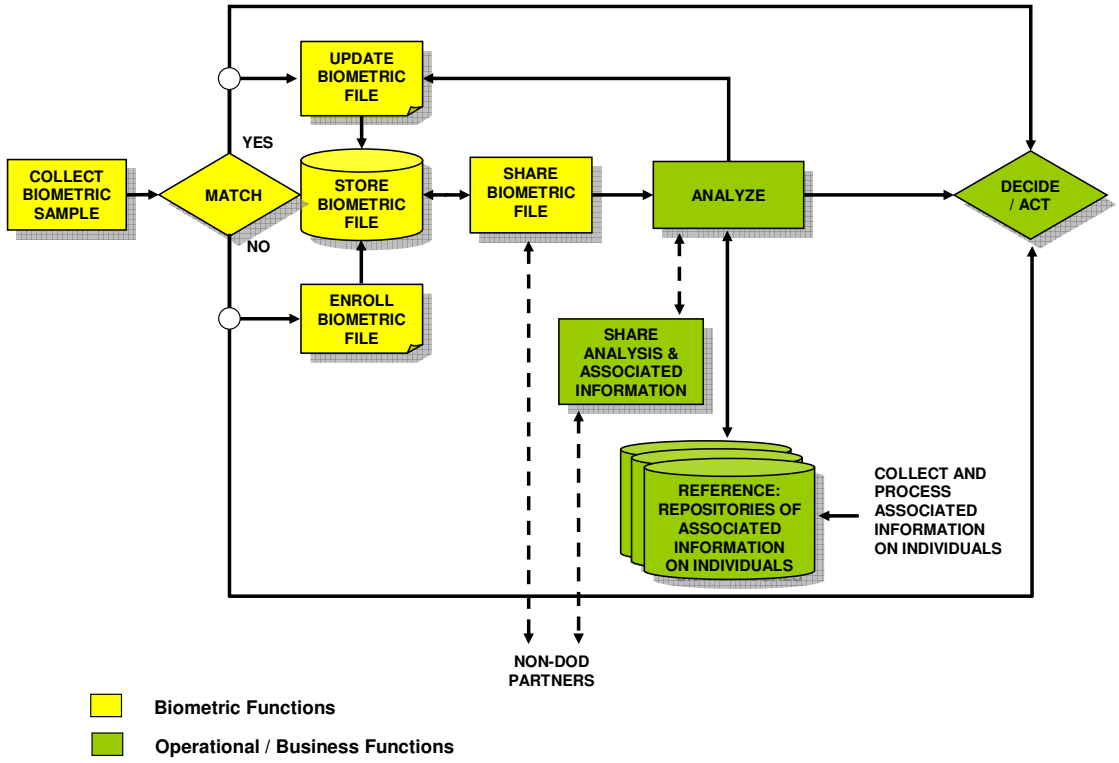
This document is developed by the DoD Biometric Standards Working Group (BSWG). The BSWG is chartered to champion the development of biometric standards at the national and international levels, to coordinate and advocate DoD interests, and to build a consensus on standards development, evaluation, adoption, and implementation issues across the DoD and in coordination with other federal agencies. Members of this working group include:

U.S. Army
U.S. Air Force
Department of the Navy
DoD Biometrics Task Force
DoD Program Manager, Biometrics
Defense Manpower Data Center
Defense Information Systems Agency
Defense Information Technology Standards Registry Information Assurance Technical Working Group
Office of the Assistant Secretary of Defense for Networks & Information Integration
National Institute of Standards and Technology
National Biometrics Security Project
Intelligence Community
Department of Transportation
Federal Aviation Administration
Federal Bureau of Investigation
Department of Homeland Security
U.S. Coast Guard
West Virginia University

1.2 Scope and Purpose

This document serves as a technical reference that lists published biometric standards and describes their applicability to the "Collect," "Store," and "Share" functions defined in the CONOPS document. It also describes the status of biometric standards in the DoD Information Technology Standards Registry (DISR). This document follows the CONOPS capabilities-based approach and does not address any specific system, application, or platform. Figure 1 depicts the Biometric Process defined in the CONOPS.

Figure 1: Biometric Process



1.3 Document Structure

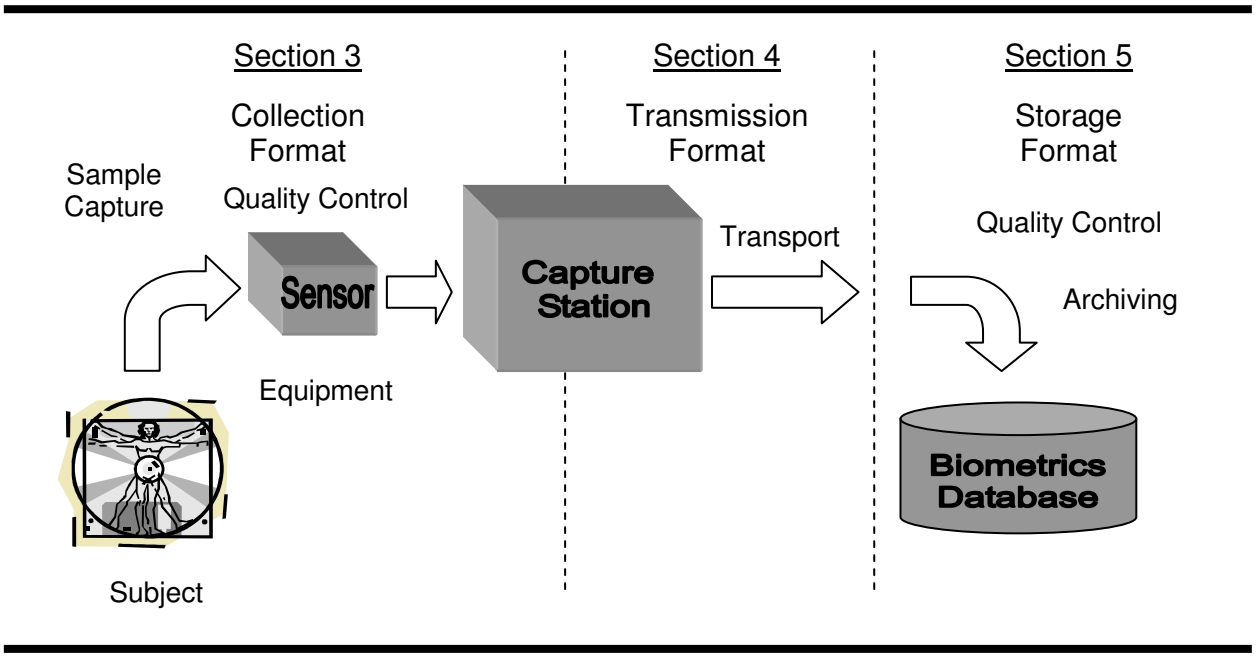
The remainder of Section 1 describes this document's structure and its intended use. Section 2 lists the meanings of acronyms and terms used in this document. Section 3 lists published standards and specifications for collecting biometric data, including any requirements pertaining to that collection. The biometric modalities included in Section 3 are:

- Fingerprints
- Face Images
- Iris Images
- Signature/Sign Data
- Hand Geometry
- Palm Prints

For each modality, a subsection describes related equipment, image or sample capture, quality control (where applicable), and formatting. Section 4 addresses standards and specifications for the transmission of biometrics and related data between systems and organizations. Standards concerning the storage and archival of biometric data are listed in Section 5.

This document is structured to correspond to a generic collection, transmission, and storage process as illustrated in Figure 2.

Figure 2: Biometric Collection, Transmission, and Storage Process



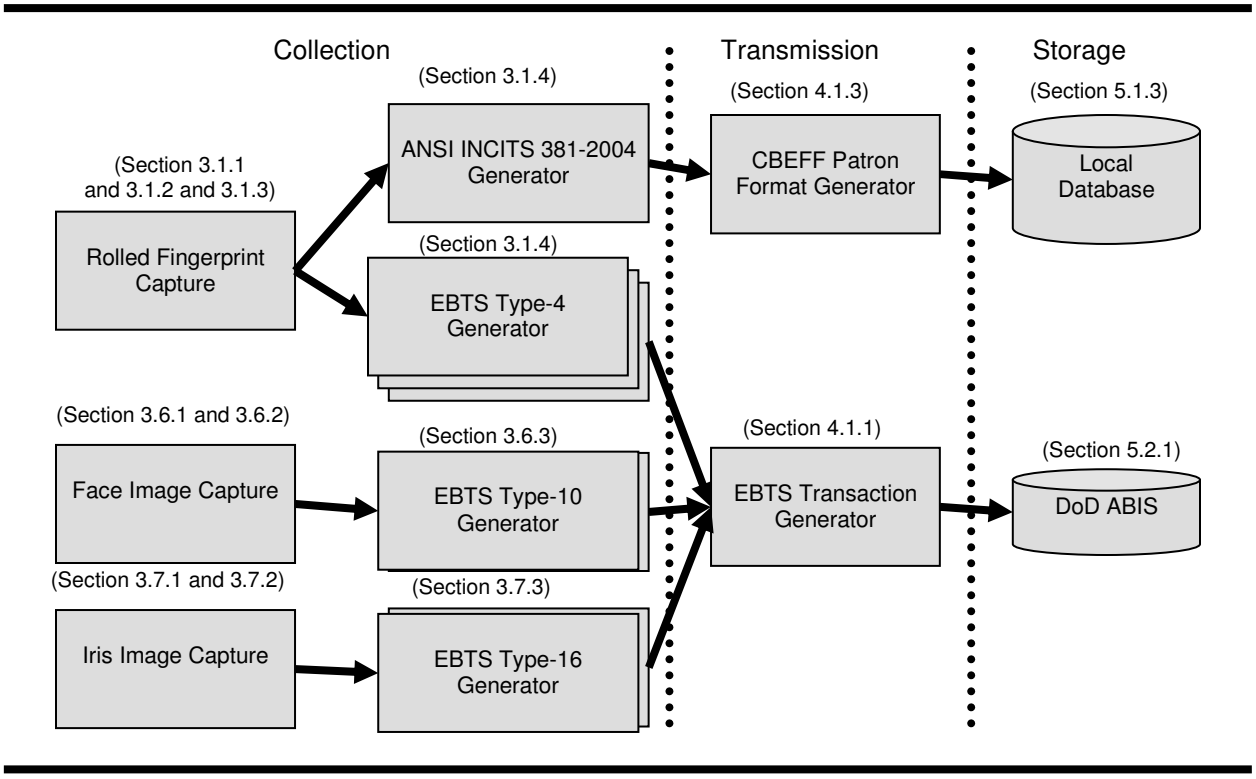
1.4 Intended Use of Document

This document should be used as a reference to assist in the development of future system-specific policy and technical documents, such as standard operating procedures, architecture technical views, and application profiles. The selection of appropriate biometric standards for a particular biometric system implementation is based on the unique circumstances of the system, including the business need, system requirements, and applicable DoD system interfaces.

For example, an application may be required to collect 10 rolled fingerprints, face, and iris samples. The application may also be required to store the fingerprint data in a local database but transmit all biometric data to a remote database, such as DoD Automated Biometric Identification System (ABIS). Figure 3 demonstrates how various sections of this document may

be applied to identify standards that may be implemented to support the collection, transmission, and storage functions of the application.

Figure 3: Example Application



1.5 Published Biometric Standards and DISR Status

In 2004, the DISR officially replaced the Joint Technical Architecture in compliance with the 2004 *Memorandum for DoD Executive Agent for Information Technology Standards* and in accordance with DoD Directives 4350.5 and 5101.7. The DISR serves as a central repository for DoD-approved information technology standards, including biometric standards. Use of the DISR is mandated for the development and acquisition of new or modified fielded IT and National Security Systems throughout the DoD.

The following Table 1 contains descriptions of published biometric standards and their status in DISR. More information about standards adoption criteria and process can be found in Appendix A.

Table 1: Published Biometric Standards and DISR Status

Category of Standards	Standard Name	Description	DISR Status
Fingerprint Image	ANSI/NIST ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information	This standard defines the content, format, and units of measurement for the exchange of fingerprint, palm print, facial/mug shot, and SMT full-image information that may be useful in identifying a subject.	Mandated
	ANSI INCITS 381-2004 Finger Image-Based Data Interchange Format	This standard specifies an interchange format for the exchange of image-based fingerprint and palm print recognition data. It defines the content, format, and units of measurement for such information. This standard is intended for those identification and verification applications that require the use of raw or processed image data containing detailed pixel information.	Pending (Change Request (CR) Submitted as Mandated Standard)
	ISO/IEC 19794-4 Biometric Data Interchange Formats – Part 4: Finger Image Data	This standard specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within an ISO/IEC 19785-1 Common Biometric Exchange Formats Framework (CBEFF) data structure. This can be used for the exchange and comparison of finger image data.	Pending (CR Submitted as Emerging Standard)
Fingerprint Template	ANSI INCITS 378-2004 Finger Minutiae Format for Data Interchange	This standard defines a method of representing fingerprint information using the concept of minutiae. It defines the placement of the minutiae on a fingerprint, a record format for containing the minutiae data, and optional extensions for ridge count and core and delta information.	Pending (CR Submitted as Mandated Standard)
	ANSI INCITS 377-2004 Finger Pattern-Based Interchange Format	This standard specifies an interchange format for the exchange of pattern-based fingerprint recognition data. It describes the conversion of a raw fingerprint image to a cropped and down-sampled finger pattern followed by the cellular representation of the finger pattern image to create the finger pattern interchange data.	Pending (CR Submitted as Mandated Standard)
	ISO/IEC 19794-2 Biometric Data Interchange Formats – Part 2: Finger Minutiae Data	This standard specifies a concept and data formats for representation of fingerprints using the fundamental notion of minutiae. It is generic in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. ISO/IEC 19794-2:2005 contains definitions of relevant terms, a description of how minutiae shall be determined, data formats for containing the data for both general use and for use with cards, and conformance information.	Pending (CR Submitted as Emerging Standard)

Category of Standards	Standard Name	Description	DISR Status
Face	ANSI INCITS 385-2004 Face Recognition Format for Data Interchange	This standard specifies definitions of photographic environment, subject pose, focus, digital image attributes, and a face interchange format for relevant applications, including human examination and computer-automated face recognition.	Pending (CR Submitted as Mandated Standard)
	ISO/IEC 19794-5 Biometric Data Interchange Formats – Part 5: Face Image Data	This standard specifies scene, photographic, digitization, and format requirements for images of faces to be used in the context of both human verification and computer automated recognition. The format is designed to allow for the specification of visible information discernible by an observer pertaining to the face, such as gender, pose, and eye color.	Pending (CR Submitted as Emerging Standard)
Iris	ANSI INCITS 379-2004 Iris Image Interchange Format	This standard describes a format for the exchange of iris image information. It contains a definition of attributes, a data record format, sample records, and conformance criteria. Two alternative formats for iris image data are described—one based on a Cartesian coordinate system and the other on a polar coordinate system.	Mandated Standard
	ISO/IEC 19794-6 Biometric Data Interchange Formats – Part 6: Iris Image Data	This standard specifies two alternative image interchange formats for biometric authentication systems that use iris recognition. The first is based on a rectilinear image storage format and the second is based on a polar image specification.	Pending (CR Submitted as Emerging Standard)
Other Modalities	ANSI INCITS 396-2005 Hand Geometry Format for Data Interchange	This standard specifies an interchange format for the exchange of hand geometry data in a silhouette format. It defines the content, format, and units of measurement for such information. This standard is intended for those identification and verification applications that require the use of an interoperable hand geometry template.	Pending (CR Submitted as Mandated Standard)
Signature Sign Data	ANSI INCITS 395-2005 Biometric Data Interchange Formats – Signature/Sign Data	This Standard specifies a data interchange format for representation of digitized sign or signature data, for the purposes of biometric enrollment, verification, or identification through the use of Raw Signature/Sign Sample Data or Common Feature Data. The data interchange format is generic in that it may be applied and used in a wide range of application areas where electronic signs or signatures are involved. No application-specific requirements or features are addressed in this standard.	N/A

Category of Standards	Standard Name	Description	DISR Status
Transmission	Electronic Fingerprint Transmission Specification (EFTS) (v7.1)	The purpose of this document is to specify certain requirements to which agencies must adhere to communicate electronically with the FBI's Integrated Automated Fingerprint Identification System (IAFIS). This specification is based on ANSI/NIST ITL 1-2000 and covers the IAFIS electronic transmissions involving fingerprints.	N/A
	Electronic Biometric Transmission Specification (EBTS) (v1.1)	This specification describes customizations of EFTS transactions that are necessary to use the DoD ABIS.	Pending (CR Submitted as Mandated Standard)
Technical Interfaces	ANSI INCITS 358-2002 BioAPI Specification (v1.1)	This standard provides a high-level generic biometric authentication model suited for any form of biometric technology. It covers the basic functions of enrollment, verification, and identification and includes a database interface to allow a biometric service provider to manage the identification population for optimum performance.	Mandated Standard
	ANSI INCITS 398-2005 [NISTIR 6529-A] Common Biometric Exchange Formats Framework (CBEFF)	This standard describes a set of data elements necessary to support biometric technologies in a common way. These data elements can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange.	Mandated Standard
	OASIS (Organization for the Advancement of Structured Information Standards) eXtensible Markup Language (XML) Common Biometric Format 1.1	This specification defines a common set of secure XML encodings for the patron formats specified in CBEFF (NISTIR 6529). Much of the information included in this standard has been incorporated into a more recent standard, ANSI X9.84-2003.	Emerging Standard
Application Profiles	NIST Special Publication 800-76 – Biometric Data Specification for Personal Identity Verification	Special Publication 800-76 (SP 800-76) is a companion document to Federal Information Processing Standard 201. It describes technical acquisition and formatting specifications for the biometric credentials of the Personal Identity Verification (PIV) system, including the PIV card itself. The primary design objective behind these particular specifications is high performance universal interoperability.	Pending (CR Submitted as Mandated Standard)

2 Terms and Acronyms

2.1 Terms

The following terms are used in this document as indicated.

- Application Profile – a document that identifies a set of two or more existing prerequisite biometric standards and identifies the classes, subsets, options, and parameters of those base standards that are necessary for accomplishing a particular function.
- Collection Personnel – the DoD-authorized individual collecting biometric data from another person.
- Electronic Fingerprint Sensors – also referred to as live scan devices.
- Person – the individual from whom biometric data are being collected.

2.2 Acronyms

ABIS – DoD Automated Biometric Identification System
ANSI – American National Standards Institute
BioAPI – Biometrics Application Programming Interface
BIR – Biometric Identification Record
BTF – U.S. Army Biometrics Task Force
BSWG – Biometric Standards Working Group
CBEFF – Common Biometric Exchange Formats Framework
CJIS – Criminal Justice Information Services
CONOPS – Concept of Operations
DISR – Defense Information Technology Standards Registry
DNA – deoxyribonucleic acid
DoD – Department of Defense
EBTS – Electronic Biometric Transmission Specification
EFTS – Electronic Fingerprint Transmission Specification
ESP – Encapsulating Security Payload
FBI – Federal Bureau of Investigation
FIQM – Finger Image Quality Measurement
IAFIS – Integrated Automated Fingerprint Identification System
IEC – International Electrotechnical Commission
IETF – Internet Engineering Task Force
IKE – Internet Key Exchange
INCITS – International Committee for Information Technology Standards
IP – Internet Protocol
IPSEC – Internet Protocol Security
ISO – International Organization for Standardization
ITL – Information Technology Laboratory
NFIQ – NIST Finger Image Quality
NIST – National Institute of Standards and Technology
NISTIR – NIST Interagency Reports
OASIS – Organization for the Advancement of Structured Information Standards
PIV – Personal Identity Verification
ppi – pixels per inch

SMT – Scar, Mark, & Tattoo
S/MIME – Secure/Multipurpose Internet Mail Extensions
SOP – Standard Operating Procedure
SSH – Secure Shell
TLS – Transport Layer Security
VPN – Virtual Private Network
XML – eXtensible Markup Language

3 Collection

3.1 Rolled Live Scan Fingerprints

3.1.1 Equipment

- All electronic fingerprint sensors, commonly known as live scan devices, shall be certified by the FBI to conform to Appendix F of the EFTS (Reference a) and shall appear on the FBI-certified devices list (Reference b).

3.1.2 Image Capture

- Collection of samples from each person shall include the following images:
  - 10 separately rolled fingers.
  - Combined plain impression of the four fingers on the right hand (no thumb).
  - Combined plain impression of the four fingers on the left hand (no thumb).
  - Left thumb plain impression.
  - Right thumb plain impression.
- Rolled impressions shall be rolled from one side of the fingernail to the other.
- Images shall be captured at a resolution of either 500 or 1,000 pixels per inch (ppi).

3.1.3 Quality Control

- Rolled live scan fingerprint images shall be evaluated with an automated tool that implements one of the following DoD-approved quality algorithms:
  - National Institute of Standards and Technology (NIST) Finger Image Quality (NFIQ) Tool (Reference q).
  - DoD Finger Image Quality Measurement (FIQM) Tool (Reference r).

3.1.4 Formatting

- Rolled live scan fingerprint images shall be formatted in, and in conformance with, one of the following formats:
  - EBTS Type-4 logical records (Reference k). Only 500-ppi images shall be stored in Type-4 records. Note that EBTS Type-4 records are identical to EFTS and American National Standards Institute (ANSI)/NIST Type-4 records.
  - EBTS Type-14 logical records (Reference k). 500-ppi and 1,000-ppi images may be stored in Type-14 records. Note that EBTS Type-14 records are identical to EFTS and ANSI/NIST Information Technology Laboratory (ITL) 1-2000 Type-14 records.
  - ANSI International Committee for Information Technology Standards (INCITS) 381-2004 Finger Image standard (Reference d).
  - ANSI INCITS 378-2004 Finger Minutiae standard (Reference h).
  - ANSI INCITS 377-2004 Finger Pattern standard (Reference i).

  - International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19794-4 Biometric Data Interchange Formats – Part 4: Finger Image Data (Reference hh).
  - ISO/IEC 19794-2 Biometric Data Interchange Formats – Part 2: Finger Minutiae Data (Reference ii).
- ANSI INCITS- and ISO/IEC-formatted rolled live scan fingerprint data shall be embedded in a CBEFF Patron Format (Reference j).
- EBTS-formatted rolled live scan fingerprint data may be embedded in a CBEFF Patron Format (Reference j).
- Rolled live scan fingerprint data embedded in a CBEFF Patron Format should make use of one of the CBEFF Patron Formats that are being commonly used or are required by the specific application. Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the Biometrics Application Programming Interface (BioAPI) 1.1 storage format (Format C – The BioAPI Biometric Identification Record (BIR)) specified in Annex C of CBEFF (Reference j).

3.2 Plain Live Scan Fingerprints

3.2.1 Equipment

- All electronic plain scan fingerprint sensors shall be certified by the FBI to conform to Appendix F of the EFTS (Reference a) and shall appear on the FBI-certified devices list (Reference b).

3.2.2 Image Capture

- Plain live scan fingerprints may be either "segmented" or "unsegmented."
- Collection of segmented plain live scan finger samples shall include the following 14 images:
  - 10 individual plain impressions of separate fingers.
  - Combined plain impression of the four fingers on the right hand (no thumb).
  - Combined plain impression of the four fingers on the left hand (no thumb).
  - Left thumb plain impression.
  - Right thumb plain impression.
- Collection of unsegmented plain live scan finger samples shall include the following three images:
  - Combined plain impression of the four fingers on the right hand (no thumb).
  - Combined plain impression of the four fingers on the left hand (no thumb).
  - Combined plain impression of the two thumbs.
- Images shall be captured at a resolution of either 500 or 1,000 ppi. Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

3.2.3 Quality Control

- Plain live scan fingerprint images shall be evaluated with an automated tool that implements one of the following DoD-approved quality algorithms:
  - NFIQ Tool (Reference q).

- DoD FIQM Tool (Reference r).

3.2.4 Formatting

- Plain live scan fingerprint images shall be formatted in and in conformance with one of the following formats:
  - EBTS Type-4 logical records (Reference k). Only 500-ppi images shall be stored in Type-4 records. Note that EBTS Type-4 records are identical to EFTS and ANSI/NIST Type-4 records.
  - EBTS Type-14 logical records (Reference k). 500-ppi and 1,000-ppi images may be stored in Type-14 records. Note that EBTS Type-14 records are identical to EFTS and ANSI/NIST ITL 1-2000 Type-14 records.
  - ANSI INCITS 381-2004 Finger Image standard (Reference d).
  - ANSI INCITS 378-2004 Finger Minutiae standard (Reference h).
  - ANSI INCITS 377-2004 Finger Pattern standard (Reference i).
  - ISO/IEC 19794-4 Biometric Data Interchange Formats – Part 4: Finger Image Data (Reference hh).
  - ISO/IEC 19794-2 Biometric Data Interchange Formats – Part 2: Finger Minutiae Data (Reference ii).
- All ANSI INCITS- and ISO/IEC-formatted plain live scan fingerprint data shall be embedded in a CBEFF Patron Format (Reference j).
- All EBTS-formatted plain live scan fingerprint data may be embedded in a CBEFF Patron Format (Reference j).
- Plain live scan fingerprint data embedded in a CBEFF Patron Format should make use of one of the CBEFF Patron Formats that are being commonly used or are required by the specific application. Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

3.3 Single Fingerprints

3.3.1 Equipment

- All electronic single-fingerprint sensors shall implement a software interface that complies with BioAPI 1.1 (Reference c).

3.3.2 Image Capture

- Image capture requirements shall be stated using the "Image Acquisition Settings Levels" in Table 1 of Clause 6, "Image Acquisition Requirements," of ANSI INCITS 381-2004, "Finger Image-Based Data Interchange Format" (Reference d).

3.3.3 Quality Control

- Rolled live scan fingerprint images shall be evaluated with an automated tool that implements one of the following DoD-approved quality algorithms:
  - NFIQ Tool (Reference q).
  - DoD FIQM Tool (Reference r).

3.3.4 Formatting

- Single fingerprint images shall be formatted in, and in conformance with, one of the

following formats:
  - ANSI INCITS 381-2004 Finger Image standard (Reference d).
  - ANSI INCITS 378-2004 Finger Minutiae standard (Reference h).
  - ANSI INCITS 377-2004 Finger Pattern standard (Reference i).
  - ISO/IEC 19794-4 Biometric Data Interchange Formats – Part 4: Finger Image Data (Reference hh).
  - ISO/IEC 19794-2 Biometric Data Interchange Formats – Part 2: Finger Minutiae Data (Reference ii).
- Single fingerprint images embedded in a CBEFF Patron Format should make use of one of the CBEFF Patron Formats that are being commonly used or are required by the specific application. Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

3.4 Latent Fingerprints

3.4.1 Equipment

There is no further guidance related to equipment.

3.4.2 Image Capture

- It is highly recommended that latent fingerprint images be captured at 1,000-ppi or higher resolution.
- Grayscale digital imaging should be at a minimum of 8 bits per pixel.
- Color digital imaging should be at a minimum of 24 bits per pixel.

3.4.3 Formatting

- Latent fingerprint images shall be formatted in, and in conformance with, one of the following formats:
  - EBTS Type-4 logical records (Reference k). Only 500-ppi images shall be stored in Type-4 records. Note that EBTS Type-4 records are identical to EFTS and ANSI/NIST Type-4 records.
  - EBTS Type-7 logical records (Reference k). 500-ppi and higher resolution images may be stored in Type-7 records. Note that EBTS Type-7 records are identical to EFTS and ANSI/NIST ITL 1-2000 Type-7 records.
  - EBTS Type-9 logical records (Reference k). Note that EBTS Type-9 records are identical to EFTS and ANSI/NIST ITL 1-2000 Type-9 records.

3.5 Rolled Ink-on-Card Fingerprints

3.5.1 Equipment

- Rolled ink fingerprints shall be captured on DoD-acceptable fingerprint cards (examples are FBI Criminal Justice Information Services (CJIS) Forms FD-249 (Criminal Card) and FD-258 (Applicant Card)).
- All electronic fingerprint scanners shall be certified by the FBI to conform to Appendix F of the EFTS (Reference a) and shall appear on the FBI-certified devices list (Reference b).

3.5.2 Image Capture

- Collection of samples from each person shall include the following images:
  - 10 separately rolled fingers.
  - Combined plain impression of the four fingers on the right hand (no thumb).
  - Combined plain impression of the four fingers on the left hand (no thumb).
  - Left thumb plain impression.
  - Right thumb plain impression.
- Rolled impressions shall be rolled from one side of the fingernail to the other.
- Images taken from the fingerprint cards shall be captured at a resolution of either 500 or 1,000 ppi.

3.5.3 Formatting

- Rolled ink-on-card fingerprint images shall be formatted in, and in conformance with, one of the following formats:
  - EBTS Type-4 logical records (Reference k). Only 500-ppi images shall be stored in Type-4 records. Note that EBTS Type-4 records are identical to EFTS and ANSI/NIST Type-4 records.
  - EBTS Type-14 logical records (Reference k). 500-ppi and 1,000-ppi images may be stored in Type-14 records. Note that EBTS Type-14 records are identical to EFTS and ANSI/NIST ITL 1-2000 Type-14 records.

3.6 Face Images

3.6.1 Equipment

- All photographs shall be taken using color cameras.
- All facial image capture equipment shall implement a software interface that complies with BioAPI 1.1 (Reference c).

3.6.2 Image Capture

- The camera lens orientation shall be pointed to the front of the person, aligned approximately in the center of the face, and taken from a distance of approximately five feet.
- The orientation(s) of the person for facial photos shall be taken from the following positions:
  - Frontal view (also known as full-frontal pose).
  - 90 degrees left side.
  - 45 degrees left side.
  - 90 degrees right side.
  - 45 degrees right side.
- When photographed, the person shall not be allowed to wear any glasses, sunglasses, headgear, headdress, or other items obscuring the area photographed. There are no constraints on cosmetics.
- The full frontal pose shall conform to the requirements of ANSI INCITS 385-2004, "Face Recognition Format for Data Interchange" (Reference e), clauses 8.2, 8.3, and 8.4 (The Full Frontal Image Type).

3.6.3 Formatting

- Facial images shall be formatted in, and in conformance with, one of the following formats:
  - EBTS Type-10 logical records (Reference k). Note that EBTS Type-10 records are identical to EFTS and ANSI/NIST Type-10 records.
  - ANSI INCITS 385-2004 Face Recognition Format standard (Reference e).
  - ISO/IEC 19794-5 Biometric Data Interchange Formats – Part 5: Face Image Data (Reference jj).
- ANSI INCITS- and ISO/IEC-formatted facial image data shall be embedded in a CBEFF Patron Format (Reference j).
- EBTS-formatted facial image data may be embedded in a CBEFF Patron Format (Reference j).
- Facial image data embedded in a CBEFF Patron Format should make use of one of the CBEFF Patron Formats that are being commonly used or are required by the specific application. Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

3.7 Iris Images

3.7.1 Equipment

- All iris image capture equipment shall implement a software interface that complies with BioAPI 1.1 (Reference c).
- All iris image capture equipment shall collect separate images of the left and right irises of each person. Note: This does not imply that two images must be collected. The requirement is that, if both the left and right eyes are captured, the process must result in two images.

3.7.2 Image Capture

- Images should be captured in accordance with Annex A, Iris Image Capture Best Practices, of ANSI INCITS 379-2004, the Iris Image Interchange Format (Reference f).

3.7.3 Formatting

- Iris images shall be formatted in, and in conformance with, one of the following formats:
  - EBTS Type-16 logical records (Reference k). Note that there are no EFTS or ANSI/NIST Type-16 records that are equivalent to EBTS Type-16 records.
  - ANSI INCITS 379-2004 Iris Image Format standard (Reference f).
  - ISO/IEC 19794-6 Biometric Data Interchange Formats – Part 6: Iris Image Data (Reference kk).
- ANSI INCITS- and ISO/IEC-formatted iris image data shall be embedded in a CBEFF Patron Format (Reference j).
- EBTS-formatted iris image data may be embedded in a CBEFF Patron Format (Reference j).
- Iris image data embedded in a CBEFF Patron Format should make use of one of the CBEFF Patron Formats that are being commonly used or are required by the specific application. Special consideration should be given to the Patron Format specified in

section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

3.8 Signature/Sign Data

3.8.1 Equipment

- All signature/sign data capture equipment shall implement a software interface that complies with BioAPI 1.1 (Reference c).

3.8.2 Data Capture

There is no further guidance related to data capture.

3.8.3 Formatting

- Signature/sign data shall be formatted in, and in conformance with:
  - ANSI INCITS 395-2005 Biometric Data Interchange Formats – Signature/Sign Data (Reference nn).
- Signature/sign data shall be embedded in a CBEFF Patron Format (Reference j).
- Signature/sign data embedded in a CBEFF Patron Format should make use of one of the CBEFF Patron Formats that are being commonly used or are required by the specific application. Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

3.9 Hand Geometry Samples

3.9.1 Equipment

- All hand geometry capture equipment shall implement a software interface that complies with BioAPI 1.1 (Reference c).

3.9.2 Data Capture

There is no further guidance related to data capture.

3.9.3 Formatting

- Hand geometry data shall be formatted in, and in conformance with:
  - ANSI INCITS 396-2005 Hand Geometry Format standard (Reference n).
- Hand geometry data shall be embedded in a CBEFF Patron Format (Reference j).
- Hand geometry data embedded in a CBEFF Patron Format should make use of one of the CBEFF Patron Formats that are being commonly used or are required by the specific application. Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

3.10 Palm Prints

3.10.1 Equipment

- All palm print capture equipment shall meet the equipment requirements contained in ANSI/NIST ITL 1-2000 Section 22 (Reference p).

3.10.2 Image Capture

- All palm print capture equipment shall meet the image capture requirements contained in ANSI/NIST ITL 1-2000 Section 22 (Reference p).

3.10.3 Formatting

- Palm print images shall be formatted in, and in conformance with:
  - ANSI/NIST ITL 1-2000 Type-15 records.
- ANSI/NIST ITL 1-2000 formatted palm print image data may be embedded in a CBEFF Patron Format (Reference j).
- Palm print data embedded in a CBEFF Patron Format should make use of one of the CBEFF Patron Formats that are being commonly used or are required by the specific application. Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

4 Transmission

4.1 Format

4.1.1 EBTS Transactions

- May be used for transmitting the following:
  - finger images in Type-4 or Type-14 logical records.
  - latent images in Type-7 logical records.
  - finger minutiae in Type-9 logical records.
  - facial images in Type-10 logical records.
  - SMT images in Type-10 logical records.
  - iris images in Type-16 logical records.
- Shall conform to EBTS Version 1.1 (Reference k).
- May be used to transmit to the DoD ABIS.

4.1.2 EFTS Transaction

- May be used for transmitting the following:
  - finger images in Type-4 or Type-14 logical records.
  - latent images in Type-7 logical records.
  - finger minutiae in Type-9 logical records.
  - facial images in Type-10 logical records.
  - SMT images in Type-10 logical records.
- Shall conform to EFTS (Reference a).
- May be used to transmit to DoD ABIS and FBI IAFIS.

4.1.3 CBEFF Patron Format

- Any CBEFF Patron Format may be used for transmitting any biometric data that have a Format Type value assigned by a registered Format Owner (see CBEFF, Section 6.3 (Reference j)).
- CBEFF-formatted data should make use of one of the CBEFF Patron Formats, preferably one of those that are being commonly used or are required by the specific application.

Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

4.2 Transport

4.2.1 Transport to DoD ABIS

- Accepts transactions submitted via:
  - E-mail on NIPRNet.
  - E-mail on SIPRNet.
  - FTP on NIPRNet.
  - Computer media (CD-ROM, DVD).

4.2.2 Transport to FBI IAFIS

- Accepts transactions submitted via:
  - E-mail on the CJIS Wide Area Network

4.3 Protection

4.3.1 File Security

- CBEFF
  - X9.84 specifies the minimum security requirements for effective management of biometric data (Reference gg). The application profile will detail the specific implementation of X9.84 to avoid possible incompatibility with CBEFF.
  - PIV Patron Format (Reference l).
- Data Protection
  - Cryptographic Message Syntax (1999) – Internet Engineering Task Force (IETF) Request for Comments (RFC) 2630 (Reference t).
  - Cryptographic Message Syntax (2004) – IETF RFC 3852 (Reference u).

4.3.2 Message Security

- Secure e-mail
  - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3, Message Specification – IETF RFC 2633 (Reference v).
  - S/MIME Version 3.1 Message Specification – IETF RFC 3851 (Reference w).

4.3.3 Transport Security

- Secure Socket
  - Transport Layer Security (TLS) Protocol Version 1.0 – IETF RFC 2246 (Reference x).
  - TLS Protocol Version 1.1 – IETF RFC 4346 (Reference y).
- Secure File Transfer
  - File Transfer Protocol (FTP) Security Extensions – IETF RFC 2228 (Reference z).
  - Secure Shell (SSH) File Transfer Protocol - IETF Internet Draft (Reference mm).

- Virtual Private Network (VPN)
  - Internet Protocol Security (IPSec) with Internet Key Exchange (IKE) (1998).

- Internet Protocol (IP) Authentication Header – IETF RFC 2402 (Reference aa).
- IP Encapsulating Security Payload (ESP) – IETF 2406 (Reference cc).
- The IKE – IETF RFC 2409 (Reference ee).

o IPSec with IKE (2005)

- IP Authentication Header – IETF RFC 4302 (Reference bb).
- ESP – IETF 4303 (Reference dd).
- IKE v2 Protocol – IETF RFC 4306 (Reference ff).

5 Storage

5.1 Format

5.1.1 PIV Card

- The storage format for data on the PIV card is in NIST Special Publication 800-76 (Reference l).

5.1.2 PIV Enrollment Agency

- The storage format for data saved by the agency executing a PIV card enrollment is in NIST Special Publication 800-76 (Reference l).

5.1.3 Other Biometric Repository

- The internal storage format of biometric data in a repository should be specified based on system requirements. However, the biometric repository shall be capable of constructing at least one of the standardized data interchange and transmission formats listed in this document. This construction capability shall enable the system to format biometric files according to the standards listed in this document for the purpose of successfully sharing those files with other standardized DoD-recognized systems. Each biometric modality listed in this document contains published standardized formats for performing successful transmissions.

5.2 Archiving

5.2.1 DoD ABIS

- Data transmitted to the DoD ABIS may indicate that data be retained or not retained.

5.2.2 FBI IAFIS

- Data transmitted to the IAFIS may indicate that data be retained or not retained.

5.3 Protection

5.3.1 File Security

- CBEFF
  - X9.84 specifies the minimum security requirements for effective management of biometric data (Reference gg). The application profile will detail the specific implementation of X9.84 to avoid possible incompatibility with CBEFF.
  - PIV Patron Format (Reference l).
- Data Protection
  - Cryptographic Message Syntax (1999) – IETF RFC 2630 (Reference t).
  - Cryptographic Message Syntax (2004) – IETF RFC 3852 (Reference u).

Appendix A: Adoption of Biometric Standards

Published standards should be adopted and used whenever possible to permit the development of open systems and avoid use of vendor-specific, proprietary solutions. Standards provide structure and a framework by which development, interoperability, interchange, and functionality may be achieved.

Adoption is a process by which an organization expresses formal acceptance of a standard for use in direct procurement, as a reference in another document, or as guidance in its design, manufacturing, testing, or support activities. Adoption of biometric standards is a crucial component of a successful implementation of biometric technologies. Common biometric standards should be used throughout DoD to facilitate interoperability and data sharing within DoD, the federal government, and foreign partners. As new standards are published, these standards must be evaluated and possibly adopted by DoD.

A.1 DoD DISR Overview

In 2004, the DISR officially replaced the Joint Technical Architecture in compliance with the 2004 *Memorandum for DoD Executive Agent for Information Technology Standards* and in accordance with DoD Directives 4350.5 and 5101.7. The DISR serves as a central repository for DoD-approved information technology standards, including biometric standards. Use of the DISR is mandated for the development and acquisition of new or modified fielded IT and National Security Systems throughout the DoD.

To support the adoption of biometric standards, the BSWG selects published standards based on priorities identified by the DoD Biometrics Community of Interest and submits formal Change Requests to the DISR.

A.2 Criteria for Submission of Standards to the DISR

Standards must successfully satisfy the following criteria for submission and acceptance into the DISR: net-centricity, interoperability, technical maturity, implementability, publicly available, consistent with authoritative sources, and applicability to DoD. The standards selection criteria focus on mandating only those items critical to net-centricity and interoperability (Reference s).

- **Net-centric Interoperability** – How does this technology provide users the ability to access applications and services through Web services (an information environment composed of interoperable computing and communication components)?

- **Technical Maturity** – How technically mature and stable is the standard? Does it have strong support in the commercial marketplace? What commercial products exist for this standard? How long has this standard been used? Is a follow-on standard in development? When is its estimated completion date? Should the sunset status be added to the current mandated status?

- **Public Availability** – To what URL can a system developer go to get a copy of the standard? Is a copy of the standard free, or must it be purchased?

- **Implementability** – Who specifically in DoD or the Intelligence Community is using this standard? What specific commercial organizations have developed implementations of this standard?

- **Authoritative** – What standards body developed and now maintains this standard? Is it an international, national, or military standard? What is the process for maintaining and developing this standard? Is the process open or closed?

- **Applicability** – Is the standard applicable to the entire DoD? The standard must have Department-wide applicability since, under the Clinger-Cohen Amendment, the DoD Chief Information Officer has authority to "ensure that information technology and national security systems standards that will apply throughout the Department of Defense are prescribed." This would preclude mandates for Component-unique standards or duplicate standards for the same capability that are not interoperable.

Each standard accepted to the DISR is assigned a status, which is one of the following:

- **Emerging standards** – candidate standards to help the program manager determine those areas likely to change within three years and to suggest those areas in which "upgradeability" should be a concern. They may be implemented, but shall not be used in lieu of a mandated standard without a waiver. An emerging standard is expected to be elevated to mandatory status within three years. Those that continue in an emerging status for longer than three years will require justification.

- **Mandated standards** – essential for providing interoperability and net-centric services across the DoD enterprise. They are the minimum set of essential standards for implementation in the acquisition of all DoD systems that produce, use, or exchange information and, when implemented, facilitate the flow of information in support of the warfighter. These standards are mandated for the management, development, and acquisition of new or improving systems throughout the DoD.

Appendix B: Data Collection for Non-Standardized Modalities

Currently, there are no published national or international standards for voice or DNA biometric data. The following sub-sections provide recommendations based on the practices existing within the DoD.

B.1 Voice Recording Samples

B.1.1 Equipment

- A dedicated microphone(s) shall be used. Microphones built in to a laptop, personal digital assistant, or similar device shall not be used.
- Voice sample capture equipment should implement a software interface that complies with BioAPI 1.1 (Reference c).

B.1.2 Sample Capture

- Microphone(s) shall be positioned 6 to 12 inches from the person.
- The person shall read a prepared script no less than 30 seconds in length in his native language and speaking style.
- If possible, multiple voice samples should be collected from each person on different days and at differing times of the day (e.g., morning, mid-day, and evening).
- Voice samples shall be collected in an indoor location relatively free of background noise. The room used for voice data collection shall use materials such as carpeting, cubicle walls, blankets, or similar materials to suppress reflective noise and echo effects.

B.1.3 Formatting

- Captured voice files shall be formatted in a .wav file format defined in ISO/IEC 13818 – Generic coding of moving pictures and associated audio information (Reference m).
- Formatted voice files shall be embedded in a CBEFF Patron Format (Reference j).
- Voice files embedded in a CBEFF Patron Format should make use of one of the CBEFF Patron Formats that are being commonly used or are required by the specific application. Special consideration should be given to the Patron Format specified in section 6 of NIST Special Publication 800-76 (Reference l) or to the BioAPI 1.1 storage format (Format C – The BioAPI BIR) specified in Annex C of CBEFF (Reference j).

B.2 DNA Samples

This section describes the requirements for the collection of biological material suitable for transfer, temporary storage, and DNA analysis for use in federal counter-terrorism investigations and operations, to include military support for the Global War on Terrorism. These samples may be tested by short tandem repeat marker systems that include the 13 Combined DNA Index System loci. These samples may also undergo mitochondrial DNA analysis, Y-chromosomal analysis, or other forensic testing as deemed appropriate by the Joint Federal Agencies Antiterrorism DNA Database working group, which consists of members drawn from the DoD and federal law enforcement and intelligence communities. The FBI DNA Advisory Board, "Quality assurance standards for Forensic DNA Testing Laboratories and for Convicted

Offender DNA Databasing Laboratories" (Reference g) provides additional information on requirements and quality assurance metrics for DNA testing.

U.S. military units shall collect two buccal (intra-oral cheek) swabs from each person. Collection Personnel shall collect one swab from the inside of each cheek (right and left). The person must not have consumed food or drink; chewed gum; or chewed, dipped, or smoked tobacco or any other products for at least 15 minutes prior to the DNA sample being collected.

B.2.1 Collection and Labeling

- DoD personnel shall label each container of two swabs with the person's name, the date and location of acquisition, and the name and unit of the individual responsible for the collection. The containers must be labeled using a permanent marker or pen.
- DoD personnel shall collect DNA samples using a sterile cotton-tipped applicator for the buccal swabs. Briskly rub the inside of the person's inner cheek up and down 10 times with the buccal swab, concentrating on scraping cells from the oral mucosa, (inner cheek) not just collecting saliva.
- The two swabs should be air dried for at least thirty minutes when possible prior to repackaging and transport. DoD personnel shall place the dried oral swabs in a properly labeled paper envelope or paper box (never plastic) and seal with evidence tape. Gloves should be worn when packaging the swabs.

B.2.2 Transfer to Laboratory

- U.S. military units shall maintain a chain of custody for each pair of swabs using appropriate documentation and procedures or similar document.
- It is important that all individuals handling the DNA samples use gloves and avoid direct skin, hair, or breath contact that might contaminate the samples.
- Combatant Commands shall establish written procedures to transfer persons' swabs to the FBI. DoD and the federal law enforcement and intelligence communities cooperatively process the swabs.
- The DoD shall maintain DNA profiles in a joint database that shall be traceable to the person's other biometric information.

Appendix C: References

a. Electronic Fingerprint Transmission Specification (EFTS), version 7.1, May 2, 2005, http://www.fbi.gov/hq/cjisd/iafis/efts71/efts71.pdf.
b. "Products certified for compliance with the FBI Integrated Automated Fingerprint Identification System image quality specifications," http://www.fbi.gov/hq/cjisd/iafis/cert.htm.
c. ANSI INCITS 358-2002, "BioAPI Specification (Version 1.1)."
d. ANSI INCITS 381-2004, "Finger Image Based Data Interchange Format" (This standard is copyrighted, and licensed copies are available from the Biometrics Task Foce (BTF)).
e. ANSI INCITS 385-2004, "Face Recognition Format for Data Interchange" (This standard is copyrighted, and licensed copies are available from the BTF).
f. ANSI INCITS 379-2004, "Iris Image Interchange Format" (This standard is copyrighted, and licensed copies are available from the BTF).
g. Federal Bureau of Investigation DNA Advisory Board, "Quality assurance standards for Forensic DNA Testing Laboratories and for Convicted Offender DNA Databasing Laboratories," Jul 00, http://www.fbi.gov/hq/lab/fsc/backissu/july2000/codispre.htm.
h. ANSI INCITS 378-2004, "Finger Minutiae Format for Data Interchange."
i. ANSI INCITS 377-2004, "Finger Pattern Data Interchange Format."
j. ANSI INCITS 398-2005/NISTIR 6529-A, "Common Biometric Exchange Framework Format (CBEFF)."
k. DoD Electronic Biometric Transmission Specification (EBTS), version 1.1, 23 Aug 05, http://www.biometrics.dod.mil/Documents/DoD_ABIS_EBTS.pdf.
l. NIST Special Publication 800-76, http://csrc.nist.gov/publications/nistpubs/800-76/sp800-76.pdf.
m. ISO/IEC 13818, "Generic Coding Method of Moving Pictures and of Associated Sound" for various applications such as digital storage media, television broadcasting, and communication.
n. ANSI INCITS 396-2005, "Hand Geometry Format for Data Interchange."
o. "Capstone Concept of Operations For DoD Biometrics In Support Of Identity Superiority," (version 1.0).
p. ANSI/NIST ITL 1-2000, American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST), "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information," Sep 00, ftp://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf.
q. NIST Finger Image Quality (NFIQ) Tool, NISTIR 7151, "Fingerprint Image Quality," Aug 04, by Elham Tabassi, Charles L. Wilson, and Craig I. Watson.
r. DoD Finger Image Quality Measurement (FIQM) Tool, "Fingerprint Image Quality Measurement Algorithm," Jan 06, by Dr. Joseph Guzman and Robert Yen.
s. Department of Defense, "Standard Operating Procedures for the Information Technology Standards Committee (ITSC) and Its Technical Working Groups (TWGs)," Dec 04.
t. IETF RFC 2630 Cryptographic Message Syntax, R. Housley, June 1999.
u. IETF RFC 3852 Cryptographic Message Syntax (CMS), R. Housley, July 2004.
v. IETF RFC 2633 S/MIME Version 3 Message Specification, B. Ramsdell, Ed., June 1999.
w. IETF RFC 3851 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification, B. Ramsdell, Ed., July 2004.
x. IETF RFC 2246 The TLS Protocol Version 1.0. T. Dierks, C. Allen, January 1999.
y. IETF RFC 4346 The Transport Layer Security (TLS) Protocol Version 1.1, T. Dierks, E. Rescorla, April 2006.
z. IETF RFC 2228 FTP Security Extensions, M. Horowitz, S. Lunt, October 1997.

aa. IETF RFC 2402 IP Authentication Header, S. Kent, R. Atkinson, November 1998.
bb. IETF RFC 4302 IP Authentication Header, S. Kent, December 2005.
cc. IETF RFC 2406 IP Encapsulating Security Payload (ESP), S. Kent, R. Atkinson, November 1998.
dd. IETF RFC 4303 IP Encapsulating Security Payload (ESP), S. Kent, December 2005.
ee. IETF RFC 2409 The Internet Key Exchange (IKE), D. Harkins, D. Carrel, November 1998.
ff. IETF RFC 4306 Internet Key Exchange (IKEv2) Protocol, C. Kaufman, Ed., December 2005.
gg. ANSI X9.84-2003, "Biometric Information Management and Security for the Financial Services Industry"
hh. ISO/IEC 19794-4 "Biometric Data Interchange Formats – Part 4: Finger Image Data"
ii. ISO/IEC 19794-2 "Biometric Data Interchange Formats – Part 2: Finger Minutiae Data"
jj. ISO/IEC 19794-5 "Biometric Data Interchange Formats – Part 5: Face Image Data"
kk. ISO/IEC 19794-6 "Biometric Data Interchange Formats – Part 6: Iris Image Data"
ll. "National Science and Technology Council (NSTC) Biometrics Standards (BS) Interagency Coordination Plan (ICP)," Current copies of this document are obtained by request at the discretion of the Director of the BTF.
mm. T. Ylonen and S. Lehtinen, SSH File Transfer Protocol, draft-ietf-secsh-filexfer-00.txt, January 2001, work in progress material.
nn. ANSI INCITS 395-2005 "Biometric Data Interchange Formats - Signature/Sign Data"