NIGERIAN BIOMETRIC STANDARDS REGULATION NO._____, 2016

PURSUANT TO SECTION 5 AND SECTION 31 OF THE NATIONAL IDENTITY MANAGEMENT COMMISSION ACT 2007

DRAFT

NATIONAL IDENTITY MANAGEMENT COMMISSION ACT, 2007

SUBSIDIARY LEGISLATION

List of Subsidiary legislation

Nigerian Biometrics Standards Regulation No. _____, 2016

DRAFT

PREFACE

1. Introduction

Before the National Identity Management Commission (NIMC), there was no centralized National Identity Database and no system of National Identity Management which efficiently linked public and private sector identity schemes in Nigeria. The result has been the creation of several different silos of identification schemes and databases leading to the duplication of an individual's identity data by the various institutions offering services to that person. Further, government agencies also hold a number of databases with no viable integration of access or interoperability to enhance the delivery of services within these government institutions. This is despite the fact that some of these institutions have introduced smart card technology into their schemes. A reliable national system for verification and secure authentication of an individual's identity was thus required.

The National Identity Management Commission (NIMC) Act No. 23, 2007; an Act to provide for the establishment of a National Identity Database; has been setup by the government of Nigeria, with a mandate to issue a Unique National Identification Number (NIN) to all Nigerians and long term residents in the country. The NIMC proposes to create a platform to first collect the identity details and then perform authentication that can be used by several government and commercial service providers because one of the key requirements of NIMC's system is to eliminate duplicate identity.

2. Biometric Standards

In the current Information Technology (IT) world, as interoperability between devices and IT systems becomes a growing concern, the question is not whether to use standards but which standards to use. ANSI, INCITS, CEN, Oasis, ICAO and ISO are just a few of the prominent agencies with published biometric standards. After reviewing the charter of each body and current state of biometrics in Nigeria, the NIMC Biometrics Committee **("the Committee")** selected the ISO standard. Within the ISO body of biometric standards, the Committee proposed the use of data format standards. These standards are widely supported by vendors, and are used extensively. ISO data format standards also contain the minimum empirical information on usage, interoperability and conformance.

There is a way of checking identity, using automated methods and information and communication technologies (ICT) to recognise individuals based on physical or behavioural traits, ranging from fingerprints, iris, photographs, etc. — a field known as biometrics. With the wide acceptance of biometrics for identity verification, especially

DRAFT

in an open network environment, the challenges of privacy, reliability and the security of biometric data become more complicated and demanding. To ensure that biometric authentication systems are reliable, secure, interoperable and easy to use, there is an evident need for the development of international standards.

NIMC as the regulatory authority on identity management in Nigeria has canvassed for the adoption of standardized systems across board. There has to be general uniformity on what biometric traits to measure, & the confidence levels ascribed to the adopted metrics. Standards are also needed to protect biometric data, both to maintain personal privacy and to prevent fraudulent attacks. The underlying objectives of standardization are interoperability, seamlessness, and reliability.

3. Conclusion

NIMC has adopted biometric technology as the primary method for person identity. Standardization of biometric data, processes, and tools/devices within the identity management industry is key for effective service delivery.

This Regulation is therefore to act as a guide to ensure best practices, expected accuracy, interoperability and conformity, to ensure a robust and reliable national system for identity management. It is hoped that the Regulation will fill the necessary gaps in Biometric standards across board.

Engr. Aliyu A. Aziz
Director General and Chief Executive Officer,
National Identity Management Commission (NIMC)

DRAFT

NATIONAL IDENTITY MANAGEMENT COMMISSION ACT, 2007

NIGERIAN BIOMETRICS STANDARDS REGULATION No.: 2016

PREFACE:

ARRANGEMENT OF REGULATIONS

REGULATION:

PART I - POWER OF THE NATIONAL IDENTIFICATION MANAGEMENT COMMISSION (NIMC) TO ENFORCE BIOMETRIC STANDARDS

1. The NIMC Compliance and Inspectorate Division (NIMC-CID) 8

PART II - OBJECTIVES OF THE REGULATION

2. Objectives of the Regulation 8

PART III - APPLICATION OF THE REGULATION

3. Application of the Regulation 9
4. Normative Reference 100

PART IV - BIOMETRICS STANDARDS

5. Standards 110

6. Biometric Basics and Enrolment Standards for the Face 110
7. Biometric Basics and Enrolment Standards for Fingerprint 113
8. Biometric Basics and Enrolment Standards for the Iris 146

PART V - CONTRAVENTIONS AND ENFORCEMENT

9. Acts constituting Contravention 19
10. Enforcement Procedure 19

PART VI - MISCELLANEOUS

DRAFT

11. Abbreviations and Interpretations..... 20

PART VII – SCHEDULES

DRAFT

NATIONAL IDENTITY MANAGEMENT COMMISSION ACT 2007

NIGERIAN BIOMETRICS STANDARDS REGULATION NO.: _____ 2016
[Under Section 31]

[xxxx, *2016*]

[Commencement]

In exercise of the powers conferred upon me by virtue of section 31 of the National Identity Management Commission Act 2007 and all other powers enabling me in that behalf, I,……. .....Director General of the **National Identity Management Commission do hereby make the following Regulations.**

Citation

These Regulations may be cited as the **Nigerian Biometric Standards Regulation No.: _____, 2016.**

DRAFT

PART I - POWER OF THE NATIONAL IDENTITY MANAGEMENT COMMISSION (NIMC) TO ENFORCE THE BIOMETRIC STANDARDS

1. The NIMC Powers to enforce and ensure Compliance with the Regulation

The NIMC shall exercise its powers to enforce the Biometric Standards through the Inspectorate and Enforcement Unit (NIMC-IEU) of the NIMC. The NIMC-IEU shall in addition to the duties assigned by the Regulations have the powers to carry on the following responsibilities:

(1) Inspect the level of Compliance with the recommended Biometric Standards among MDA's, Agencies, Executive Bodies, Institutions and Corporate Organizations who are licensed by the Commission to capture any form of biometric and demographic capture ;

(2) Administer and Co-ordinate the adherence to Biometric Standards by all MDA's and Agencies in Nigeria;

(3) The Unit shall reserve the right to enter in and inspect the level of compliance with these Biometric standards during the issuing of or renewal of identification documents; and

(4) To enter in and confiscate records in circumstances where any Operator is not willing to comply or has shown continuous disregard for adherence to the standards for Biometric capture during the production of means of production of identities not in conformity with the NIMC standards.

(5) The power to enter and confiscate shall only be exercised pursuant to obtaining an Exparte Order/Warrant from the Court of competent jurisdiction.

PART II - OBJECTIVES OF THE REGULATION

2. Objectives

These Regulations shall define the specifics of the National Biometric Standards requirements, formats which enable interoperability of, formats, processes, hardware specifications, with the following guiding objectives and principles:

(1) To enable the standardization of data collection, transmission and storage processes to cover the basic functions of Enrolment, Verification, and Identification; and includes basic standards to allow only

DRAFT

approved/licensed agencies, organisations, and entities to manage and ensure interoperability of their system with the integrated national system;

(2) To ensure consistent, good quality biometric data and reliable interoperability across biometric capture devices, capture software and unique NIN service delivery;
.

(3) To enable the detection and elimination of duplicate identities, and ensure accurate authentication.

(4) To identify applicable biometric standards and recommend best practices to the NIMC on an on-going basis.

PART III- Application of the Regulation

3. These Regulations shall apply to the following categories of persons:

(1) All MDA's, Agencies, Statutory Bodies, Executive Bodies, Corporate Bodies(hereinafter also jointly referred to as "Operators") whose licenses, statutory functions or business functions require Biometric capture and authentication;

(2) Any person or organisation licensed, involved in designing, testing, or implementing the NIN system, NIN compatible systems, or NIN enrolment for the central government, state government, commercial organisations; and

(3) Any and all users of the NIN system.

(4) Any person or organization which the NIMC shall add to this category of persons from time to time

4. Normative Reference

(1) The Provisions of the First Schedule to this Agreement form a part of this Agreement and it shall be the duty of Operator to which these Regulations apply to ensure compliance with the provisions of requirements in the First Schedule herewith as Normative Reference in setting up Biometric data capture modalities;

(2) If the requirements of the First Schedule are not complied with, it shall be the duty of the Operator to ensure and enforce the compliance and make a report of same to the NIMC-IEU

DRAFT

[First Schedule]

PART IV - BIOMETRICS STANDARDS

5. Standards

The ISO standard of Biometric data capture parameters, data format standards, and other standards within the ISO body of biometric standards is hereby adopted as the standard of compliance and shall be adopted by every Operator under these Regulations.

6. Biometric Basics and enrolment standards for the Face

(1) Face Biometrics Basics

The dimensions, proportions and physical attributes of a person's face are unique. Face biometrics involves the use of distinctive facial characteristics such as cheekbones, nose location, eye location, and eye socket outline in order to identify individuals.

There are three generic approaches to human face processing namely component-based methods (separable elements perceived as distinct parts), configural based methods (spatial arrangements), and holistic based methods (face as an unparsed perceptual whole).

ICAO compliant face images shall be captured during enrolment. For verification and identification, the user stands in front of the camera for a few seconds, and the scan is compared with the template previously recorded. To prevent an image/photo of the face or a mask from being used, face biometric systems will require the user to smile, blink, or nod their head. Also, facial thermography can be used to record the heat of the face (which won't be affected by a mask). It is recommended to place the backdrop (a white of off-white background behind the person whose face is to be captured) against an opaque wall/partition.

DRAFT

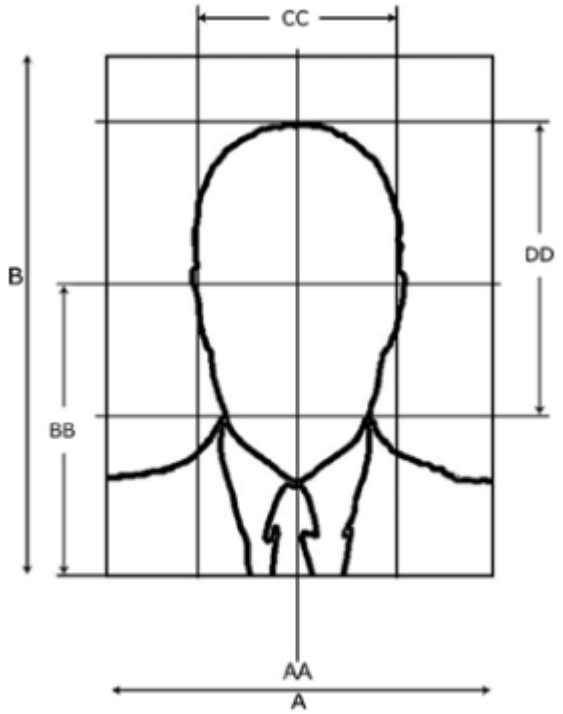

Figure 1: Geometric Characteristics of the Full Frontal Face Image

(2) Face Enrolment standards

(a) Position

Full frontal face image provides sufficient information for both human visual inspection (by an operator) and automatic face recognition algorithms. In order to obtain a good quality image, 24-bit colour images with a minimum of 90 pixels of inter-eye distance are required.

(i) These Standards recommends at least 120 pixels for optimum quality. The image should contain well-focused nose to ear and chin to crown region.

(ii) Assistance may also be provided in special cases, but in no case should the face or body part (hand, arms) of the assisting person or any object appear in the photograph.

(b) Tribal Marks

The face image should be captured with the tribal marks; clearly visible for easy verification purposes.

DRAFT

(c) Digital Photographic Requirements

(i) Face image capture devices may be connected to enrolment workstations and linked to enrolees. The capture device should use auto focus and auto-capture functions if available;

(ii) The output image should not suffer from motion blur, over or under exposure, unnatural colour, uneven lighting, or radial distortion. Interlaced video frames are not allowed;

(iii) Enrolment operators should encourage enrolees to adjust to suitable postures and sitting requirements, and may also adjust capture devices to capture suitable face images.

(d) Expression

Faces should be captured with neutral (non-smiling) expression, mouth closed and both eyes open.

(e) Illumination

Proper and equally distributed lighting mechanism should be used such that there are no shadows over the face, no shadows in eye sockets, and no hot spots.

(f) Glasses

(i) If the person normally wears glasses, it is recommended that the photograph be taken with glasses. However, the glasses should be clear and transparent so that pupils and iris are visible.

(ii) If the glasses are tinted, then direct and background lighting sources should be tuned accordingly.

(g) Accessories

Head coverings such as hats or caps are not permitted. If an applicant wears a head covering for religious purposes (e.g. hijabs) or on medical grounds (e.g. eye patches), a photograph of the applicant wearing it will be accepted provided all facial features from bottom of the chin to top of the forehead (including both edges of the applicant's face) are clearly shown.

(3) Operational Process

(a) Operator Training and Assistance

The single most important factor in obtaining better image quality is the operational process. Operator training and assistance are important for yielding good quality images. Operators' should be trained to obtain the best possible face images that satisfy requirements

DRAFT

(b) Quality check

The quality assessment algorithm should encode parameters like illumination, pose, blur, noise, resolution, inter-eye distance, image height and width, and horizontal and vertical position of the face. The quality assessment algorithm should be used at the time of enrolment to determine the quality score of the captured face image, and the image is stored only if it meets a certain quality threshold.

(c) Storage and Compression

The performance of face recognition algorithms reduce significantly if the compression factor is greater than 10. For preserving the quality of image, only uncompressed images should be stored in the database.

(4.) Face Verification and Authentication Standards

The verification process shall consist of steps similar to enrolment:

(a) Image Capture

Image capture for authentication should also follow standards for enrolment as defined earlier in this Section.

(b) Compression

Images with JPEG 2000 compression ratio of 10 will suffice. As per ISO standards, the image size after compression should not be less than 11 KB.

(c) Number of Images

For both manual and automatic authentication, a single full frontal face image is sufficient. The captured image should conform to the digital/photographic requirements and quality thresholds mentioned above in the enrolment section.

7. Biometrics Basics and Enrolment standards for Fingerprint

(1) Fingerprint Biometrics Basics

A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The points where ridges split (bifurcations) or end (ridge endings) are called minutiae. Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which

DRAFT

cross each other). The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points.

There are five basic fingerprint patterns: arch, tented arch, left loop, right loop and whorl. Statistics show that these compositions vary according to race and ethnic origin.

Fingerprints are usually considered to be unique, with no two fingers having the exact same dermal ridge characteristics. There is a large variation in the quality of fingerprints within the population. The tip of the finger is a small area from which to take measurements, and ridge patterns can be affected by cuts, dirt, or even wear and tear. Acquiring distinct high quality fingerprint data is a complicated task.

(2) Fingerprint Enrolment standards

(a) Plain or rolled capture

The rolled image, common in forensic applications contains twice as much information as the plain image. The plain image is easier to capture and can capture up to four plain fingers in one scan. The rolled image in contrast, must be captured one finger at a time. Rolled images requires operator guiding the rolling of each finger.

(b) Number of fingers

(i) For all Persons, this Regulation recommends capturing prints of all ten (10) fingers. This is because, every additional finger increases accuracy and improves matching speed;

(ii) For persons in the rural areas and due to the nature of strenuous work they do like farming, fishing, hunting, masonary, etc, these Regulations recommends capturing prints of all ten fingers, the maximum possible. In cases where prints cannot be easily captured due to wear and tear, the easily identifiable ones should be captured and other biometric identifiers like face and iris data will be captured also.

(c) Disabilities

Where disability or other circumstances lead to the inability to capture fingerprints, a concerted effort should be made to capture all available fingerprints. If no fingerprints are available, other biometric identifiers like face and iris data will be captured for the disabled person.

DRAFT

(3) Operational Processes

(a) Capture and quality check

Image segmentation and quality checks should be performed after image capture. The enrolee must be asked to retry enrolling if the image quality is poor. The software should assign image quality indices.

Fingerprint quality metrics adopted by the NIMS is based on the internationally recognized National Institute of Standards and Technology (NIST) NFIQ metric. The NFIQ enables the quantification of the quality of fingerprint images. NFIQ generates a single score, in the range of 1-5, to represent the quality of fingerprints; "1" being of the highest quality and "5" being of the lowest quality.

Table 1 below represents the mapping of NFIQ quality grades to other international quality metrics

NFIQ	MINEX 04	800-76-1	MINEX II
1	100	100	100
2	75	80	80
3	50	60	60
4	25	40	40
5	1	20	20

Table 1: NFIQ Mappings to other quality metric

Basic quality checks and image enhancement should be performed after image capture. The enrolee must be asked to retry enrolling if the image quality is poor. The algorithm can assign image quality score. The quality threshold score is an important decision. Images captured with a NIST Fingerprint Image Quality (NFIQ) value of 4 or 5 are considered as poor quality, but should still be captured and stored along with the image quality indices.

(b) Operator Assistance:

Operators need to be trained to assist enrolees during data capture in presenting the correct fingers, finger pressure, finger position/orientation, and so on.

DRAFT

(c) Corrective measures and retries:

Where the initial capture is unsatisfactory, the operator should provide corrective measures such as wiping fingers with a damp cloth or applying lotion. Only after all such measures are exhausted in five attempts will the operator be able to override the quality gate (i.e. force capture).

(d) Storage and Transmission

The data format of storage should be such that other applications can access the data. This includes (but not limited to) WSQ's, ISO/IEC 19794-2, and ANSI INCITS 381-2004 template formats.

(e) Compression

To preserve the quality, these Regulations recommend uncompressed images. Transmission of images may be made in JPEG2000 or WSQlossless compression for legacy or compatibility purposes. Any form of flossy compression is not accepted.

(4) Fingerprint Device Characteristics

a) A minimum optical resolution of 500 DPI is recommended;

b) A minimum FBI IAFIS Appendix F certification is required for enrolment devices;

c) Liveness detection is desirable for capture devices;

(5) Fingerprint Verification and Authentication standards

(a) Number of fingers

A single finger will be sufficient to provide the minimum standard of accuracy requirements. Applications requiring higher levels of accuracy may need additional fingers. These Regulations allow for the scanning of any and every finger. Certain fingers, depending on the condition of the finger, will perform better during authentication.

(b) Retries

During enrolment, the final decision is to take the "best possible" image. The operator can thus "force capture."During authentication, the failure could be because the fingerprints do not match or image capture did not produce sufficient quality image for matching. In both cases, the match score is low enough for the system to declare "nomatch". A timeout will be implemented in service after five (5) attempts.

DRAFT

(c) Transmission format

Bandwidth and data size are two influential factors which will determine the format of data sent online for real time authentication. It is advisable to conduct pre-processing of data at the front-end to reduce the transmitted data size when low bandwidth is experienced.

(i) **Compression**

JPEG2000 compression is recommended. WSQ compression may be acceptable for legacy purposes. A compression of up to 15 is acceptable. While uncompressed images will be accepted, it is not recommended. Compression is not relevant if minutiae data is to be sent for verification.

(ii) **Minutiae format**

Minutiae templates should conform to ISO/IEC 19794-2:2005, ANSI INCITS 381-2004, and the MINEX (I or II) template formats.

8. Biometric basics and Enrolment standards for the Iris

(1) Biometrics Basics for the Iris

The iris is the elastic, pigmented, connective tissue that controls the pupil. The iris is formed in early life in a process called morphogenesis. Once fully formed, the texture is stable throughout life. It is the only internal human organ visible from the outside and is protected by the cornea. The iris of the eye has a unique pattern, from eye to eye and person to person.

An iris scan will analyse over 200 points of the iris, such as rings, furrows, freckles, and the corona. Glasses, contact lenses, and even eye surgery does not change the characteristics of the iris. To prevent an image / photo of the iris being used instead of a real "live" eye, iris scanning systems will vary the light and check that the pupil dilates or contracts. This is referred to as liveness detection.

(2) Iris Enrolment standards

(a) Image

Capturing two eyes simultaneously provides several advantages because the iris pattern of each eye is not correlated, giving two independent biometric feature sets. It assures correct assignment of left and right eyes and allows for more accurate estimation of roll angle.

DRAFT

(b) Capture diameter

In order to obtain good quality templates, the iris image diameter should be a minimum of 140 native pixels. 170 pixels is recommended for optimum quality.

(c) Iris Margins

The margins around the iris portion of the image need to be at least 50% of the iris diameter on the left and right sides of the image, and a least 25% of the iris diameter on the top and bottom of the image. This will retain sufficient image surrounding the iris for adequate segmentation and authentication.

(3) Operational Processes

(a) Device Characteristics

(i) The capture device should be more than 300 mm away from the enrolee to be considered non-intrusive. The capture device should use auto focus and auto-capture functions. In special circumstances where the enrolee has to position him or herself, the capture device should be more than 100mm away but the device should use a visor or other mechanical alignment aid to enable the enrolee to position his or herself. The camera must allow for some variability in the position of the iris centre relative to the camera. For two eye capture devices, the capture volume dimensions for devices without mechanical alignment aids are 19 mm wide, 14 mm high, and 20 mm deep, and for devices with such aids, 19 mm wide, 14 mm high, and 12mm deep. The ability of an iris image capture device to suppress motion blur and to freeze motion, is a function of exposure time. The maximum allowable value for the exposure time is less than 33ms, recommended being 15ms.

(ii) The iris image capture device must be capable of capturing light in the range of 700 to 900 nanometres. The camera's near infrared illuminator(s) must have a controlled spectral content, such that the overall spectral imaging sensitivity, including the sensor characteristics, transfers at least 35%of the power per any 100 nm-wide sub-band of the 700 to 900 nm range. The iris image capture sensor shall use progressive scanning. In order to achieve acceptable time-to-capture and FTA rates, the iris image sampling frequency must be at least 5 frames per second. . Illumination shall be compliant with illumination standard IEC 825-1 and safety specification ISO 60825-1.To achieve acceptable recognition

DRAFT

accuracy, the iris acquisition sensor must achieve a signal-to-noise ratio of at least 36dB.Within the frequency range of interest, 700 to 900 nm, the iris sensor shall generate images with at least 8 bits per pixel.

(b) Operator assistance

The operator and not the enrolee should handle the capture device. The enrolee will be required to sit (or stand) in a fixed position, like taking a portrait photograph; the operator will adjust the camera.

The iris capture device or the connected computer shall be able to measure the iris image quality. The best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process. The device should alert the operator if the captured iris image is of insufficient quality. The iris capture process is sensitive to ambient light. No direct or artificial light should directly reflect off enrolee's eyes.

(c) Quality assessment

The device should take successive 3 to 7 images and use local matching algorithm to match against each other (after feature extraction). The image is considered to be of satisfactory quality if hamming distance of the match is below 0.1.

(d) Compression and storage

The iris images should be stored in ISO standard format using either JPEG 2000 or PNG lossless compression (KIND_VGA).It is expected that each enrolee will require 150 Kbytes of storage space.

(4) Iris Verification and Authentication Standards

(a) Image verification and matching

Any one eye will suffice for 1:1 verification, though application may require higher-level assurance where by both eyes can be verified. Iris verification requires the image to be sent to the server for matching.

(b) Transmission format and storage

The image should be compressed to KIND_CROPPED_AND_MASKED or KIND_CROPPED using JPEG 2000. Resulting image size should be between 2KB to 10 KB. Any of the larger formats specified by the ISO standard area acceptable, though not necessary.

DRAFT

PART V - Contraventions, Compliance and enforcement

9. Acts constituting contravention

Without prejudice to such other enforcement measures as are or may be contained in the NIMC Act or any regulations made there under, any of the following acts or conducts by any Operator shall constitute a contravention under these Regulations, that is:

(1) Any act occasioning harmful interference with the powers of the NIMC-IEU to inspect biometrics databases of an Operator for compliance with these standards and these Regulations ; or

(2) a breach or violation or non-adherence howsoever to these guidelines and standards or any updates made thereto by the Commission, from time to time;

(3) a failure to meet such equipment/ data capturing machine standards as prescribed under these Regulations or as updated or prescribed by the Commission, from time to time.

10. Enforcement procedure

(1) Without prejudice to the provisions of the Act, any Regulations made there under and notwithstanding any provision to the contrary in any license, the Commission may, in addition to the powers to commence civil and criminal proceedings as prescribed under Regulations 8 and 9 of Regulations 2016, seek a Court Order for the temporary suspension of the Operator's statutory right to capture biometrics and demographic details under the following circumstances and procedures, that is—

a) if the Operator refuses for a continuous period of 30 days at any time when non adherence to these Regulations have been expressed, to provide an undertaken to commence procedures for compliance;

b) if within 12 months of the effective date of the commencement of these Regulations, the Agency has not commenced standardization of its biometrics capturing process and equipment to the satisfaction of the Commission.

(2) Provided that the Commission shall give prior notice to the Agency specifying the details of the default by the Agency and requiring that remedial steps be taken within 30 days of such notice.

DRAFT

(3) The Commission may seize and detain any equipment or biometric and demographic capturing device in the following circumstances, that is—

(a) where such Equipment/ biometric device is still in use for capturing and storing biometric or demographic details that contravene the standards and guidelines set in these Regulations and is still in use despite a notification to this effect; or

(b) where such item mentioned in paragraph (3)(a) above is relevant and required for the prosecution in court of a person under the NIMC Act or any regulations made there under ; or

(4) In seizing and detaining of any Equipment/ machine as specified in paragraph (3) (a) of this regulation, the Commission shall:

(a) obtain a warrant from a Judge of a court of competent jurisdiction;

(b) provide to the owner or his agent, a written inventory in evidence of the seizure of the seized equipment, facility, book, record, document or other information storage system except that there shall be no need for the issuance of such receipt where the item is sealed off and remains in the custody of the owner or agent.

PART VI - MISCELLANEOUS

11. ABBREVIATIONS AND INTERPRETATIONS

DPI	Dot Per Inch
ICAO	International Civil Aviation Authority
ICT	Information and Communications Technology
ID	Identity
IEC	International Electrotechnical Commission
IEU	Inspectorate and Enforcement Unit
ISO	International Standards Organization
NIMC	National Identity Management Commission
NIMS	National Identity Management System
NIN	National Identification Number
NIMC-IEU	National Identity Management Commission - Inspectorate Enforcement Unit
UNID	Unique National Identity
WSQ	Wavelet/Scalar Quantization

DRAFT

PART VII – SCHEDULES

[First Schedule]

Normative Reference for Biometric Data Capture Modalities

a. July 2007 Privacy Impact Assessment (PIA) &Harmonization Study for National Identity Management Commission (NIMC)
b. IAFIS-IC-0110 (V3), WSQ Gray-scale Fingerprint Image Compression Specification 1997
c. ISO/IEC 15444 (all parts), Information technology – JPEG2000 image coding system
d. ISO/IEC 19785-1:2006. Common biometric exchange formats framework – Part 1: Data elements specifications
e. ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data
f. ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data
g. ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data
h. ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data
i. ISO/IEC CD 19794-6.3. Biometric data interchange formats– Part 6: Iris Image data working group draft.
j. ANSI/NIST-ITL 1-2000 – Standard Data Format for the Interchange of Fingerprint, Facial & Scar. Mark &Tattoo (SMT) Information

DRAFT

[Second Schedule]
Summary of Face Biometric Standards

Key Decisions	Summary of Decision
Enrolment	
Face Image Capture Tribal Marks	• Full frontal 24bit colour images. • Well focused eye / nose / mouth / forehead / chin region. • Capture of tribal marks.
Digital/Photographic Requirement	Auto forms and auto-capture functions for capture device.
Expression	• Neutral face expression. • Mouth closed. • Eyes open.
Illumination	• Sufficient illumination. • Equally distributed illumination. • No shadows.
Eye Glasses	If glasses are worn, it should be clear and transparent so that pupils and iris are visible.
Accessories	• Head attire is strongly discouraged. • Religious accessories may be permitted (e.g. hijabs). • Medical accessories may be permitted (e.g. eye patches). • All facial features from bottom of the chin to top of the forehead (including both edges of the applicant's face) are clearly shown
Operational	Operators would be trained to obtain the best possible face image that satisfies requirements.
Quality Check	The quality assessment algorithms should encode parameters like illumination, pose, blur, nose, resolution, inter-eye distance, image height and

DRAFT

	width and horizontal vertical position of the face.
Storage and Compression	Uncompressed images should be stored in database to preserve the quality.
Authentication	
Image Capture	Same as enrolment
Compression	JPEG 2000 compression ratio should not be less than 11KB.
Number of images	For both manual and authentication, a single full frontal face image is sufficient.

Summary of Fingerprint Biometric Standards

Key Decisions	Summary of Decision
Enrolment	
Image Capture Plain or Rolled	Plain, Live Scan.
Number of Fingers, Fingerprint in Rural Areas,& Disabilities	Ten. Absence of fingers and presence of worn out fingerprints. Capture other biometric identifiers.
Device Characteristics	In covering scan resolution pixel depth and dynamic range, the biometric sample captured during enrolment needs to be the best sample possible.
Quality Check	Yes-Specified as best practice
Operational	Operator Assistance, Corrective Measure, and 5 retries.
Storage and Transmission	
Compression	Uncompressed images strongly recommended.
Authentication	
Image Capture	Same as enrolment
Number of Fingers	No minimum or maximum. A single finger will be sufficient to provide the minimum standard of accuracy requirements.
Any Finger option	Any finger.
Retry	A timeout will be implemented in service after five (5) attempts.
Device Characteristics	A standard will be defined for the scanners used in the authentication process.

DRAFT

Transmission Format	Offline: Match on Card (MOC) shall be conducted in the National Identity Card. Online: The captured image shall be sent to the NIMS for matching in real time.
Compression	JPEG 2000 compression recommended compression ratio to be less than 15:1.
Minutiae Format	ISO/IEC 19794-2:2005, ANSI INCITS 381-2004, and the MINEX (I or II)

Summary of Iris Biometric Standards

Decision	Summary of Decision
Enrolment	
Image	Two eyes, minimum 140 pixel image diameter (170 pixel preferred),image margin 50% left and right,25% top and button of iris diameter.
Device characteristics	Tethered, auto focus, continuous image capture, expose< 33millisecond,distance 7300mm for Operator control, >100mmenrolee control.
Operational	Operator controlled strongly preferred No direct natural or artificial light reflection in the eye, indoor.
Segmentation	Non linear segmentation algorithm.
Quality Assessment	Per IREX11 recommendation
Compression and Storage	150 19794-6(2010) data format standard JPEG 2000 or PNG lossless compression.
Authentication	Same as enrolment except one or two eyes JPEG 2000.

DRAFT