The Presidency
NATIONAL IDENTITY MANAGEMENT COMMISSION

Privacy Impact Assessment Report

Executive Summary

EXECUTIVE SUMMARY
1.0   INTRODUCTION
1.1   Background to the Project
The Federal Government of Nigeria (FGN), in implementing the National Identity Management Systems (NIMS) for Nigeria seeks to establish a reliable, secure and scalable Identity Management System that utilizes advanced biometric technologies to uniquely identify every individual in the country. In its quest to implement this strategy, the National Identity Management Commission (NIMC) commissioned contracts for conducting Privacy Impact Assessment (PIA) studies to identify the potential effects that the proposed system may have upon personal privacy; and to examine how any such detrimental effects on privacy might be reduced.

In this regard, the National Identity Management Commission (NIMC) engaged the services of six reputable consulting firms to assist the Commission in conducting Privacy Impact Assessment studies on the proposed National identity Management System in the six geo-political zones of the Federation. The expectation was that the PIA would identify the impacts of the NIMS system on individuals' right to privacy and ways of mitigating these impacts to avoid any adverse effects.

1.2   What is "Privacy"?
In a simple sense, privacy refers to "the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively". It also relates to the wish or desire by an individual or group to be anonymous, unnoticed or unidentified in the public realm (http://en.wikipedia.org/wiki/privacy).

1.3   Reasons for Privacy
People may not want certain personal information about themselves to be made public for various reasons, including the desire to avoid discrimination (e.g. privacy about health status, for instance HIV status) or political orientation, or sexual orientation. Privacy may also be desired in order to avoid personal embarrassment or to avoid exposure to security risks (e.g. information about income, bank account or financial transactions). This is important in order to avoid fraud or identity theft.

Although there are various forms of privacy (including physical privacy, information privacy, etc.) concern in the context of this work is about information privacy. This relates to the expectation by the public of privacy in the collection, storage and sharing of information about a person.

1.4   Terms of Reference (TOR) for the Privacy Impact Assessment (PIA)
The Terms of Reference (TOR) for the Privacy Impact Assessment (PIA) for the consultants were as follows:

    a.   Conduct, coordinate and supervise PIA studies on the proposed Identity Management System in the South-West geo-political zone.

    b.   Be responsible for organizing study enumerators, data gathering and research analysis and reporting templates as well as survey instruments, etc.

c. Design and develop the study methodology, including standard data analysis and reporting templates as well as survey instruments, etc.

d. Oversee and supervise the various activities of the proposed team members for the assignment.

e. Monitor and evaluate the zonal conduct of the study in each state of the South-West zone.

f. Design, develop and implement quality assurance and control mechanisms for consistency in the conduct of the study.

g. Document all collected information, analyze and report the study outcomes.

h. Based on the outcome of the study in the zone, identify elements of a privacy policy document on the project.

i. Write a single NIMS PIA study report for the zone

1.5   Objectives of the Privacy Impact Assessment (PIA)

The objectives of the Privacy Impact Assessment as enumerated by the National Identity Management Commission are to:

i. Identify privacy issues of concern to the public and how this might be dealt with early enough to be taken into consideration in the final design and planning of the data capture, enrollment and access to the national identity database;

ii. Systematically analyze issues that may arise from the implementation of this project to provide a clear understanding that is based on credible information;

iii. Assess technological issues as they concern the core personal information involved in the project, especially in terms of the Public Key Infrastructure (PKI) and the potential abuse;

iv. Provide an opportunity for ensuring that cost-effective solutions and approaches are adopted through the early introduction of appropriate security and other measures to hedge against perceived risks especially as they concern established consensus on privacy concerns;

v. Evaluate extant laws, practices and procedures involved in personal information management and how they impact the privacy of individuals; and

vi. Develop a Privacy Policy to guide the Commission in the discharge of its (other) functions.

2.0   RESEARCH DESIGN
2.1   The Study Area and Population

The Privacy Impact Assessment Study was designed to cover the entire country. For effective coverage, the existing geo-political zoning system was used for delineating the

country. This consists of six geo-political zones, namely: North Central Zone, North East Zone, North West Zone, South East Zone, South South Zone and South West Zone.

2.2   Research Design
A combination of qualitative and quantitative research techniques (including Focus Group Discussions, individual interviews and Key Informant/In-Depth Interviews) was used for the collection of research information. Three major target groups were identified for the purpose of the study, namely: Individuals, Strategic Office Holders (End Users) and NIMC Employees). Special categories of people among the study population (including physically challenged persons, inmates of hospitals, homes for mentally impaired, and old people's homes, inmates of other institutions such as remand homes, and prisons, long distance drivers, women in purdah, residents of *sabon gari* (exclusive residential area for non-indigenes), nomadic people, etc.) were also targeted specially for inclusion. Research information was collected from the target groups through the use of Interview Schedules for the three target groups and FGD Guide for selected groups.

2.3   Research Instruments
Four instruments were developed for the survey to collect privacy impact assessment information, namely: Individual Interview Schedule; Interview Schedule for Strategic Office Holders; Interview Schedule for Senior Employees of NIMC; and Focus Group Discussion Guide. All the research instruments were subjected to intensive in-house scrutiny among the consultants, and were pre-tested before the actual field work.

2.4   Sampling
The Privacy Impact Assessment targeted a sample of 15,002 individual respondents drawn proportionally from all the states in the six geo-political zones of the federation, using the multi-stage random sampling method. Quotas were allocated to the states in proportional to the population of the states, based on the 2006 national population census figures.

2.5   Training of Trainers
A Training of Trainers Workshop was organized for all the Consultants in Lagos on 14th November, 2008, followed by zonal level training for the research teams.

2.6   Fieldwork
The fieldwork was conducted in all the zones in the month of December, 2008, spanning a period of about three weeks.

2.7   Data Capture, Processing and Analysis
The SPSS software was used to enter and analyze the quantitative data, while qualitative data from key informant interviews were processed manually and used to complement survey data.

3.0   FIELD EXPERIENCES
The fieldwork went reasonably well, although there were a few challenges. On the positive side is the general cooperation received from the respondents, with many of them expressing excitement about the prospects of the proposed national identity card scheme enhancing individual identification and reducing crime and fraud through better identification systems.

Publicity and awareness was created for the exercise prior to the commencement of fieldwork through several advertisements both by the National Identity Management Commission (NIMC) and the various zonal consultants in various media. In addition, direct mobilization was made in various communities through contacts with community leaders. The branded T-shirts and face caps (with NIMC logo) that were made for the project also facilitated the fieldwork by creating awareness in the communities and enhancing easy identification of the field personnel.

4.0 FINDINGS

4.1 Achieved Samples

The Privacy Impact Assessment covered a sample of 15,057 individual respondents, with varying proportions from the six geo-political zones of the country was achieved. One hundred and thirty-seven respondents were interviewed for the special groups category, comprising: hospital in-patients, prison in-mates, lame/amputees, leprosy victims, women in purdah, beggars/destitute, housewives, and visually impaired. Four hundred and seventy-one (471) end-user respondents were also interviewed, comprising senior staff of relevant organizations.

Furthermore, senior NIMC employees including State Coordinators, Chief Technical Officers, Administrative Officers, Data Entry officers, Computer Engineering staff, and Field officers were interviewed.

4.2 Knowledge/awareness of the existing national identity card programme

The Privacy Impact Assessment indicated widespread awareness about the existing (2003) national identity card programme among both the individual respondents and the Special Group respondents. The relatively high level of awareness is believed to be good for the proposed national Identity Card scheme.

Further analysis revealed that knowledge of the existing national identity card programme was high across the six geo-political zones, although awareness was shown to be higher in urban areas than in rural areas. The level of awareness was also shown to be higher among males than females.

4.3 Awareness of the proposed national identity card management programme

However, awareness of the proposed National Identity Card scheme was relatively low, with only 11.8% of the respondents and 7.3% of the Special Group respondents affirming awareness of the proposed scheme. This points to the need for intensive enlightenment campaigns about the proposed national identity card scheme in all communities.

4.4 Participation in the last (2003) national identity card exercise

About three-quarters of the respondents said they participated in the 2003 National Identity Card exercise. Again, this shows a fairly high participation rate in the last exercise. The participation rate increases to about 89 per cent if we consider the fact that about 15 per cent of the respondents were not eligible to register in 2003 because of age. Given this relatively high participation rate in the 2003 exercise (the first of its type in Nigeria), there is high hope that the proposed exercise can build on this success rate to achieve greater success. However, a much lower proportion (59.9%) of the special group respondents participated in the last national identity card exercise.

Variations were noted in the participation rates across the zones, being highest in the North East zone (83.9%), and lowest in the North West zone (67.4%). There were also disparities between rural and urban areas, with the report of higher participation rate among respondents in the urban areas than respondents in the rural areas. Participation rate was also higher among males than females.

4.5   Possession of the national identity card among individual respondents
Only about three-fifth of the individual respondents and two-fifth of the special group respondents possessed the 2003 National Identity Card. Zonal analysis showed that the South South zone had the highest proportion of respondents who had the Identity Card, while South East zone had the lowest proportion. In terms of gender, a slightly higher proportion of males than females had the 2003 National Identity Card.

Non-possession of the 2003 National Identity Card by the respondents was attributed to various reasons, with the most commonly given reason being told that the cards were not ready, did not know where to collect the cards, collected card but lost, and being asked to pay some money in order to collect the cards.

4.6   Willingness to provide personally identifiable information
The success of the proposed National Identity Management Scheme depends on the willingness of the citizens to provide the required Personally Identifiable Information (PII) (such as date of birth, place of birth, place of origin, names, height, sex, religion, ethnic background, blood group, place of residence/address, languages spoken, languages they can read/ write, occupation, names of next of kin, addresses of next of kin, finger prints, photographs, biometrics (colour of their eye, hair, facial dimensions, etc.), native language, father's name, mother's name, and mother's maiden name) for inclusion in the Identity Database. The findings of this study showed a generally high expression of willingness by respondents to provide necessary personal information, ranging from 94.6 for biometrics to 97.5% for sex.

4.7   Cultural religious and political reasons why people may not be willing to provide personal information for identification purposes
The study further probed into the existence of cultural reasons why people may not be willing to provide personal information for the purpose of identification. Only 6.4% of the respondents said there were cultural reasons why people may not provide personal information for identification purpose. The reference to cultural inhibitions to the provision of personal information was highest in the North West zone and lowest in the South South zone.

Furthermore, only 6.1% said there were some religious reasons why people may not be willing to provide some personal information. Again, allusion to religious reasons that may inhibit the provision of some personal information required for registration purpose was highest in the North West zone, and lowest in the South South zone.

Moreover, only 6.4% of the respondents said there were some political reasons which may inhibit the provision of some personal information. The allusion to political reasons why people may not provide some personal information was highest in the South East zone and lowest in the South South zone.

4.8   Willingness to remove glasses for registration
The study showed that majority of the respondents were not opposed to the removal of glasses for registration purposes. However, further analysis showed that opposition to the removal of eye glasses for the purpose of registration was highest in the North West zone and lowest in the South South zone.

A major reason given by those who were unwilling to remove their glasses for the purpose of registration was that it could lead to wrong/false identification (some respondents said the eye glasses were part of their daily make-up and identity).

4.9   Willingness to Remove Veil for Registration Purpose
Opposition to the removal of veil for registration purpose was slightly higher than for the removal of eye glasses, although majority of the respondents were also not opposed to the removal of veil for registration purposes. Again, opposition to the removal of veil was highest in the North West zone and lowest in the South South zone.

Reasons for unwillingness to remove veil include that it is part of the culture or religious life (some respondents noted that Islam forbids women to expose themselves in public), while some respondents mentioned security reasons.

4.10   Useful Personal Information
The largest proportion of the end-user respondents affirmed the usefulness of all the information proposed for collection, namely: names of clients/customers, place of residence (address), date of birth, sex, occupation, photographs, place of origin, place of birth, next of kin's name, next of kin's address, father's name, finger prints, mother's name, birth registration, languages spoken, languages respondents could read and write, religion, mother's maiden name, biometrics, height, death registration native language, ethnic background and blood group.

4.11   Need for third party consent
The study showed that 28.5 percent of the individual respondents would require the permission of some other people before they could take part in the registration exercise. Gender analysis showed that, overall, a higher proportion of females than males would require a third party's permission in order to participate in the ID card registration exercise, suggesting greater freedom for males than for females. Further analysis showed that, generally, a higher proportion of females in the northern zones than in the southern zones said they required a third party's permission to participate in the exercise.

4.12   Awareness of multipurpose use of database
A major advantage of the database for the proposed national identity card scheme is that it can be used for other purposes in addition to identification. More than half of the respondents were aware the database could be used for other purposes. This shows a reasonable level of awareness about the fact that the identity card could be used for other purposes beyond simple identification.

Furthermore, a little more than half of the individual respondents answered in the affirmative when they were asked if they were aware that public institutions such as

the Police, EFCC, FRSC, FIRS, etc may have access to and use/share information in the proposed identity database.

4.13 Fears/concerns about the use of personal information against citizens

The sharing of information by other agencies raises issues about concerns about privacy. There was a relatively high level of concern about the misuse of personal information, with majority of the respondents expressing fears about some of the personal information they provide for the National Identity Card programme being used against them in various ways.

4.14 Objection to the plan to give public institutions access to the database

Given the expressed fears by the respondents, it is surprising that only a few respondents objected to the arrangement that gives some public institutions access to their personal information. The distribution across the zones showed that the highest rate of objection was recorded in the North West zone (23.3%), and the lowest in the North Central zone (6.8%). This relatively low expression of objection is positive for the proposed National Identity Card and Database scheme.

The PIA survey showed that the police and other security agencies were the most frequently mentioned agencies that the respondents did not want to have access to their personal information, followed by hospitals and related health organizations, employers of labour including the civil service and private employing organizations and banks and financial institutions including insurance companies.

4.15 Steps Taken to Validate Identity Information Provided by Members of the Public

The reliability of information in the database is important for the integrity of the database. The study showed that the end-user organization take some steps to validate identity information provided by members of the public, including: screening/vetting of information provided, use of third party confirmation, comparison with data in existence in database, investigation through direct visits to source of data, on-site verification, request for evidence/original papers, and publication in the mass media.

4.16 Privacy Issues Arising from the Use of Data

Privacy issues that arise from the use of data were said to be minimal, but include: abuse of phone numbers, breach of confidentiality, disclosure of information about family members, unauthorized disclosure of information about personal emolument, disclosure of information about religious/ethnic background resulting in victimization, disclosure of other personal information, and mismanagement of information.

4.17 Instances of Misuse of Information by Employees

Misuse of information by employees were minimal, with only one-tenth of the Strategic Office Holders reporting instances when members of their organizations misused information in their database (i.e. using the information for purposes other than what they were meant for or giving the information to other agencies or people without authorization), entailing abuse of listed contact phones, and use of information for ethnic/religious victimization. However, majority of the NIMC officials were not aware of any cases of misuse of information by employees.

4.18   Litigations Emanating from Abuse of Issues of Privacy
Furthermore, only about one-tenth of the end-user respondents said there had been litigations over privacy issues in their organizations, suggesting that litigations arising from the abuse of privacy issues are not many.

4.19   Measures to Protect the Privacy of Information Supplied (End-User Perspective)
Various steps are taken by end-user organizations to protect the privacy of information provided to them, including: oaths of secrecy by staff; emphasis that information provided be treated with utmost confidentiality, unauthorized persons not allowed access to the database, and encryption of information stored so that unauthorized persons cannot decipher the stored information.

4.20   Sharing of Database Information by End-Users
The Privacy Impact Assessment showed that the sharing of database information is not strange to end-user organizations, as many of them said they shared their database information with other institutions. This points at the prospect/viability of information sharing by institutions once the proposed identity card scheme is in place.

Majority of the Strategic Office Holders said their organizations would be favourably disposed to using a database to which other end user organizations have access. This also shows that there is a high potential for the success of the scheme based on the potentiality of sharing of information.

The overwhelming majority of the end-user respondents did not foresee any conflict between the National Identity Card scheme and their organizations' need for and use of information. This again highlights the good prospects for the proposed National Identity Card scheme.

4.21   Possession of Information Technology Facilities to Verify Identity Online
For end-user organizations to make optimum use of the new identification scheme, they need to have standard up-to-date information technology (IT) facilities that can be used for on-line verification of information. However, just 56.1% of the end-user organization respondents answered in the affirmative. This calls attention to the need for the end-user organizations to upgrade their information technology facilities. Further analysis showed that most of the organizations that lacked adequate information technology facilities for on-line verification of personal information were public institutions.

Furthermore, less than half of the end-user organizations said their information technology facilities for online verification of identity were reliable. This again calls attention to the need for end-user organizations to upgrade their information technologies in order to make optimum use of the national identity database system.

Similarly, many of the senior NIMC officials interviewed affirmed the availability of necessary IT facilities, although some of them also said the available facilities were not reliable.

4.22   Measures/Provisions to Protect Officers and Organizations against Legal Action about Violation of Privacy Issues

Various measures were said to be taken by end-users to protect their officers and staff/organizations against legal action for violation of privacy issues, including: adequate training for staff, establishment of a Legal Department to handle and advise on such cases, enforcement of the Civil Service Rules, the Code of Conduct, disciplinary actions against erring officers, inclusion of a Disclaimer Clause, adequate internal control mechanism, limiting access to personal data and information, the provision of an Operational Policy Manual, and protecting the database with passwords/PIN.

4.23   Belief in proper management of identity card programme
Overall, majority of the respondents believed NIMC would manage the information they provide well. Given the generally poor perception of government institutions, this finding shows a relatively high confidence level in NIMC and expression of good will for NIMC.

4.24   Perceived impact of the scheme
People are more likely to support schemes that they believe are likely to be beneficial to them. This is in line with general hedonistic views about human nature. The PIA showed that three-quarters of the individual respondents and four-fifth of the special group respondents thought the scheme would improve the welfare of the citizens. Similarly, majority of the end-users believed the proposed National Identity Management System would improve their current use of data.

4.25   Acceptance of National Identity Card
Overall, two-third of the end-user organizations said they accepted the National Identity Card as a form of identification. This shows that the current national identity card is accepted by many organizations for identification purposes, although, ideally, a good national identity card should have total acceptance by all organizations.

4.26   Shortcomings of Existing National Identity Card
Some of the shortcomings of the existing national Identity Card were said to include: absence of holder's signature and address, poor quality of card, not everybody has it, foreigners have access to it, and irregularities in records.

4.27   Whether the Project Should Be For All Nigerians
More than half of the individual respondents in all the zones and about three-quarters of the special group respondents thought the exercise should be for Nigerians of all ages.

4.28   Willingness to participate in the next national identity card registration exercise
A crucial determinant of the potential success or failure of the project is the willingness of people to participate in the registration exercise. The expressed willingness of people to participate in the scheme lends credence to the view about popular support for the National Identity Card scheme, with a high majority of the individual respondents and the special group respondents expressing willingness to participate in the next exercise.

4.29   Preparedness of the National Identity Management Commission for the next exercise
The result also shows that NIMC officials claimed to have put in place effective

structures such as effective management, recruitment of well trained and disciplined staff and staff have been mandated to abide by rules and regulations guiding the office. Most of the NIMC officials affirmed that the organization was well-prepared for the next registration exercise.

5.0 REPORT OF THE LEGAL ASPECTS OF THE PRIVACY IMPACT ASSESSMENT (PIA) OF THE NATIONAL IDENTITY DATABASE ESTABLISHED BY THE NATIONAL IDENTITY MANAGEMENT COMMISSION ACT NO 23, 2007

The broad objective of the legal component of the Privacy Impact Assessment (PIA) is to identify and assess the level of risks, if any, to privacy in the implementation of the National Identity Database under the National Identity Management Commission Act No. 23 of 2007 in light of the constitutional guarantee of the right to privacy; and to propose remedial measures to mitigate the identified risks.

The Report reviews specific provisions that deal with the content of the National Identity Database, powers of NIMC to obtain, retain, and disclose information in the Database, any safeguards, mandatory use of the Multipurpose Identity Card for certain transactions and penalties for breaches of the NIMC Act, with a view to determining their privacy implications using the elaborate Information Privacy Principles (IPPs) as benchmark.

The Report recognises that the NIMC Act raises potentially three fundamental privacy issues, namely: privacy of the physical person; privacy of personal behaviour; and privacy of personal information and data.

The Report considers the primary question whether the NIMC Act or its implementation particularly in terms of its provisions on collection of personal information and data (including biometric information and data); the retention of the information and data in the National Identity Database and disclosure of such information and data in certain circumstances) violates the right to privacy under Section 37 of the 1999 Constitution of the Federal Republic of Nigeria.

On the issue of collection and retention of fingerprints/other biometric information, the Report concludes that even if the collection and retention of fingerprints/other biometric information under the NIMC Act may be said to involve a level of interference with the privacy rights of citizens, such interference will be justifiable in light of the provisions of Section 45(1) of the 1999 constitution of Nigeria, given the purpose for which the fingerprints and other biometric information are required, as well as the objectives of the Database clearly specified under Section 15 of the Act.

The Report concludes that Sections 17(3); 18(1) (a) & (d); 20; and 31(c) of the NIMC Act increase the potential for breach of privacy rights under the Act and makes recommendations for relevant amendments.

The Report examines the provision of Section 27 of the NIMC Act in relation to the issue whether the requirement for the presentation of the National Identity Number or Multipurpose Identity card as a precondition for the registration of voters in Nigeria is a nullity on the basis that it violates the 1999 Constitution of Nigeria or the rights of citizens under the Electoral Act of 2006. The Report concludes that Section 27(1)(i) of

the NIMC Act violates Sections 11(2) of the Electoral Act and Section 15(e) of Part 1 of the third schedule to the 1999 Constitution and is therefore null and void to the extent that it makes the *"mandatory"* presentation of the National ID Number or Multipurpose Identity Card a precondition to the registration of voters. Neither the National Identity Number nor a Multipurpose Identity Card is a prequalification condition for registration of voters under section 13(1) of the Electoral Act. Similarly, neither the National ID Number nor Multipurpose Identity Card can be validly held as the sole identity document or instrument required to prove the identity, age or nationality of a registration applicant under Section 11(2) of the Electoral Act.

The Report further examines the issue whether the Collection of Biometric Information under the NIMC Act violates Section 34 of the 1999 Constitution on the Dignity of Human Person. It concludes that if the technology deployed will not involve any penetration of the body's surface and adequate care is taken in the process of dealing with individuals who present themselves for registration, then the violation of citizens right under Section 34 of the 1999 Constitution is unlikely to arise. It recognizes however that there could be certain challenges regarding the collection of biometric information of blind and visually impaired individuals as well as persons whose fingerprints cannot be registered due to loss of their fingers or deformity or due to other legitimate factors. Relevant amendment or Regulations to meet these challenges are recommended.

Apart from certain provisions of the NIMC Act which have been identified and recommended for amendment for better assurance or protection of privacy rights, the Report concludes generally that the Act meets the constitutional requirement of being a law that is reasonably justifiable in a democratic society; and that neither the national identity database project nor the NIMC Act constitutes a violation of the right to privacy under the Constitution or any international instrument to which Nigeria is privy.

The Report further examines the provisions of existing laws which require the collection; retention and basis for disclosure of personal information of citizens with a view to determining areas of conflict with NIMC Act – and concludes that in areas of conflict, the provisions of the NIMC Act will prevail by virtue of Section 32(6).

The Report makes the following recommendations:

- The need to adopt a Privacy Act, which elaborates privacy principles and clarifies the meaning, nature and scope of privacy-related rights and obligations, is compelling and urgent.

- It is imperative for Government/NIMC to regulate both public and private databases to which the multipurpose identity card is connected or to which it serves as a gateway.

- In furtherance of its obligations to protect personal information, NIMC should develop its own Codes of Practice and/or in collaboration with other organizations, establish Standards of Practice for Privacy. Documents such as the Canadian Standards Association's *Model for the Protections of Personal Information* (CSA Standard) can provide models.

- Massive public enlightenment, including the use of popular religious figures in Nigeria to enlighten the populace on the importance and advantages of the multipurpose identity card, and to dispel any connection of the National Identity Number and Multipurpose Identity Card with the "Mark of the Beast".

- If it is still intended that the Multipurpose Identity Card or National Identity Number must be presented as a precondition to being registered as voter in Nigeria under Section 27 of the NIMC Act, then Section 11(2) of the Electoral Act of 2006 will need to be amended to make the Multipurpose Identity Card the only document required as proof of identity.

6.0 OBJECTIVE-BASED ANALYSIS
This Privacy Impact Assessment Report includes:

i. Identification of privacy issues of concern to the public and how these might be dealt with early enough to be taken into consideration in the final design and planning of the data capture, enrollment and access to the national identity database;

ii. Systematic analyses of issues that may arise from the implementation of this project to provide a clear understanding that is based on credible information;

iii. Assessment of technological issues as they concern the core personal information involved in the project, especially in terms of the Public Key Infrastructure (PKI) and the potential abuse;

iv. Provision of an opportunity for ensuring that cost-effective solutions and approaches are adopted through the early introduction of appropriate security and other measures to hedge against perceived risks especially as they concern established consensus on privacy concerns;

v. Evaluation of extant laws, practices and procedures involved in personal information management and how they impact the privacy of individuals; and

vi. Development of a Privacy Policy to guide the Commission in the discharge of its (other) functions.

6.1 Privacy issues of concern to the public
From information provided by the respondents in the course of the Privacy Impact Assessment, various privacy issues of concern to the public were identified, including: misuse of personal information, and objection to institutional access.

Based on the views expressed by the respondents, Strategic Officer Holders/End-Users and NIMC officials, as well as literature about other projects, various issues that may arise from the implementation of this project were identified and broadly categorized as follows:

6.2.1 Issues that may arise in the process of information collection/registration

Issues that may arise in the process of information collection/registration relate essentially to unwillingness or inability of people to provide required information, genuine ignorance about some personal information, requirement of third-party consent for registration, removal of eye glasses, removal of veil, cultural, religious and political barriers to provision of personal information, inadequate number of registration centres, inadequate number of registration officials, use of ad-hoc staff, poor remuneration of officials, short supply of registration materials, failure/breakdown of computers and other registration equipment, logistic challenges, limited coverage/inability of many people to register, registration of ineligible persons, shortcomings of the existing national identity card, non-possession/inability to collect the 2003 national identity card, scope/coverage of the National Identity Card exercise (whether the project should be for all Nigerians), and willingness/unwillingness to participate in the proposed registration exercise,

6.2.2   Issues that may arise at the point of processing/using/retrieval of information

Issues that may arise at the point of processing/using of information included: risk of computer fraudsters accessing the database, protecting the privacy of personal information against abuse by employees, inadequate public awareness of the Proposed National Identity Card Scheme, capacity building for responsible officers, doubts about the reliability of personal information collected, lack of required IT facilities for online verification of information, verification of information provided by members of the public, verification of personal information by individuals, and the need for revalidation of personal information.

6.2.3   Issues that may arise in the course of interaction with third party end-users

Issues that may arise in the course of interaction with third party end-users were identified to include: partnership/buy-in/Take-up by end-user organizations, and litigations over privacy issues.

6.3   Technological issues as they concern the core personal information involved in the   project, especially in terms of the Public Key Infrastructure (PKI) and the potential   abuse

Technological issues in terms of public key infrastructure that may affect the proposed national identity card project include: inadequate technological and infrastructural facilities by end-user organizations (especially public institutions and organizations) for on-line verification of personal information; poor internet access (especially for public institutions such as schools, hospitals, security agencies, etc.); limited capacity of staff to operate technological equipment and machines; poor infrastructure, especially in terms of energy (electricity) supply which may affect the efficient operation of equipment and machines; possible breach of privacy/misuse of personal information by employees of NIMC and end-user organizations; misuse/abuse of privacy information by end-user organizations and security agencies; absence of a good privacy law in Nigeria; and absence of guidelines on use of personal information.

6.4   Provision of opportunity for ensuring that cost-effective solutions and approaches   are adopted through the early introduction of appropriate security and other   measures to hedge against perceived risks especially as they concern established consensus on privacy concerns

Some guidelines for ensuring that cost-effective solutions and approaches are adopted through the early introduction of appropriate security and other measures to hedge against perceived risks especially as they concern established consensus on privacy concerns include: accountability, specification of purpose, information limitation, confidentiality, fair treatment of personal information, direct information collection, accurate information collection, adequate safeguards for personal information, individual consent, openness, individual access and provision for challenging compliance.

7.0 RECOMMENDATIONS

Based on the findings of this Privacy Impact Assessment, the following recommendations are made:

7.1 Recommendations for enlightenment and awareness creation

- There should be intensive enlightenment campaigns in all communities, especially in the rural communities, about the proposed national identity card scheme and the need for people to support the scheme by providing required personal information.

- There should be full mobilization and involvement of traditional leaders, community leaders, religious leaders, and opinion leaders in the enlightenment programmes.

- Officials at the three tiers of government should be mobilized for support for the enlightenment campaign all over the country.

- There should be general enlightenment about the need for people to remove their eye glasses or veils as may be necessary for proper identification purpose.

- There should be general enlightenment for the public about eligibility for registration. Appeals should be made to the patriotic spirit of Nigerians to report fraudulent effort to register by non-Nigerians.

- End-user organizations should be mobilized for support and mandated to accept the national identity card for individual identification purposes.

7.2 Recommendations for registration procedures and activities

- Adequate number of registration centres should be provided for various communities, taking into consideration population size, distance between communities and transportation logistics.

- Mobile registration centres should be provided in some communities as may be appropriate to ensure adequate coverage and easy accessibility for the people.

- Adequate number of registration officials should be provided for various communities, taking into consideration population size.

- Ad-hoc staff should be given appropriate training and necessary incentives for effective performance.

- Ad-hoc staff should be recruited from local communities in order to enhance familiarity with local names and social and cultural values.

- Female registration officials should be made to attend to women who wear face veils.

- Booths should be provided at registration centres where women wearing veils can remove their veils outside public view.

- Tape measuring devices should be provided at the registration centres to measure the height of people who do not know their heights.

- Advance notification should be given for people to confirm their blood groups prior to the registration exercise.

- Adequate remuneration should be provided for registration officials, especially the ad-hoc officials, in order to enhance their motivation for good performance.

- Adequate number of registration materials should be provided for various communities, with adequate extra materials, taking into consideration population size.

- Use of good and tested equipment for the registration exercise and adequate arrangement for back-up as may be necessary.

- Use of appropriate technologies for our environment to ensure proper functioning.

- Adequate logistic arrangements should be made for the transportation of registration officials and materials.

- Adequate arrangement should be made for power supply for registration equipment, especially with back-up by electricity generating sets.

- Adequate provision for registration period to enhance greater coverage.

- Special arrangement should be made for the registration of special categories of people such as the physically or mentally challenged, people in institutions such as the prisons, hospitals, welfare homes, etc.

- NIMC should consider the pros and cons of covering all Nigerians, regardless of age, in the scheme.

- Only information that is useful for identification purposes should be collected at the point of registration.

7.3   Recommendations for information access and processing

- Personal information provided by individuals should only be used for legitimate and specified/approved purposes.

- Given the concerns about possible abuse or misuse of information by security agencies, access to information in the database by security agencies should be limited to what they may need for specific purposes at a particular time. The security agencies should also be enjoined to use the information for specified purposes only.

- There should be enlightenment for security personnel about the need to respect the privacy of individuals and not to misuse or abuse the personal information about individuals made available to them.

- There should be a limitation of institutions/agencies that may have access to personally identifiable information in the database.

- Only specified responsible officers should have access to the information database.

- There should be provision for the right of an individual to request for a verification or updating or correction of his or her personal information on the NIMC database. The Commission should respond to such requests in a timely manner, and provide data in a format that is easy to understand.

7.4   Recommendations for ensuring the security of personal information

- There should be adequate protection of database by encrypting the information in the database and protecting the database with password.

- Information in the database should be secured against virus infection through the installation of reliable and up-to-date anti-virus software.

- Personal information in the database should be encrypted and protected with password to limit access.

- The database should be locked and made a "read-only" database.

7.5   Recommendations for guidelines on the activities of end-user organizations and officials

- NIMC should, in collaboration with other stakeholders, establish Standards of Practice for Privacy, with appropriate sanctions for breaches, to guide the operations and activities of all organizations/ institutions and practitioners on privacy matters.

- There is need for Government/NIMC to regulate both public and private databases to which the multipurpose identity card is connected or to which it serves as a gateway.

- NIMC should develop its own Codes of Practice for use by the Commission and its employees.

- There should be adequate training for End-User organizations and officials on privacy issues.

- There should be adequate training and re-training for responsible officers about privacy issues to enable them keep abreast of developments on privacy matters.

- Adequate training for responsible officers and staff about the use of technological equipment and associated privacy issues.

7.6   Recommendations for National Identity Card Issuance and Collection
- There should be provision for holder's signature on the identity card.

- Adequate steps should be taken to facilitate the collection of identity cards by registered persons.

- Adequate information should be provided about where to collect identity cards, and the procedures for collection of identity cards.

- The Public Relations/Affairs unit of the National Identity Management Commission should be mandated to respond promptly to enquiries and complaints from members of the public about difficult in collecting identity cards.

- There should be clear and conspicuous display of information at all NIMC offices that collection of identity cards is free.

- Investigation of reports about demand of gratification by officials before collection of identity cards and appropriate sanctions for erring officials.

- Only officials of NIMC should be used for the distribution of identity cards.

- Adequate steps should be taken to facilitate the collection of identity cards by registered persons.

- Adoption of open, credible and reliable procedures for the collection, storage, retrieval and management of personal information.

- Due consideration should be given to measures for the verification of information provided by citizens.

- There should be appropriate amendment to the NIMC Act and to enact a Privacy Law.

- There should be an enactment of enabling laws to protect the privacy of citizens.

- The NIMC Act should be amended to introduce individual criminal liability for unlawful disclosures done willfully, recklessly or negligently.

- If it is still intended that the Multipurpose Identity Card or National Identity Number must be presented as a precondition to being registered as voter in Nigeria, then Section 11(2) of the Electoral Act of 2006 will need to be amended to make the Multipurpose Identity Card the only document required as proof of identity.

- NIMC should appoint a senior officer, preferably a Director, whose work would, among others, include ensuring best practices and compliance with privacy policies and practices by both the staff of the Commission, as well as end-user organizations.