East African Journal of Law, Policy and Globalization
Vol. 1. No. 2 (2024), pp: 1-19

Online ISSN: 3057 - 3173
Journal Title Abbreviation: *East Af. JLP&G*

The Legal Framework for Information Security in the Age of Digital Identity in Nigeria

Rebekah Ijeoma Opara,
PhD Candidate,
Department of Jurisprudence and International Law, Faculty of Law,
University of Ibadan, Oyo State, Nigeria.
Email: b89opara@yahoo.com

Abstract:
Governments worldwide, including Nigeria's government, process large volumes of information daily, utilizing both paper-based and digital formats. This encompasses various processing methods including collection, recording, storage, organization, retrieval and dissemination of information. In the legal identity management sector, these information processing activities are rapidly increasing due to various new initiatives. The security of such information is critical for safeguarding the well-being and integrity of citizens, residents and the nation as a whole. This paper employs a doctrinal approach to examine the complexities of the legal framework for information security in Nigeria, specifically in today's age of digital identity. It highlights the unique intricacies, issues and challenges related to information security in Nigeria's digital identity sector, and broader issues relevant to information security across all federal public sectors. The paper is comparative with recourse being had to South Africa's approach towards information security in its public service for insights. The findings reveal that, the legal framework for information security in Nigeria remains inadequate as it fails to sufficiently address critical information security measures. There is thus, an urgent need for increased regulation of information management and information security in Nigeria.

Keywords: Legal identity management, public service, information processing, digital identity, information security

Suggested Citation: R. I. Opara (2024), 'The Legal Framework for Information Security in the Age of Digital Identity in Nigeria,' *East. Af. JLP&G.* Vol. 1. No.2. pp. 1-19

Peer Reviewed

1. INTRODUCTION

Various governmental institutions, including those involved in identity management (IDM) in Nigeria, collect and process the personal information of citizens and residents of Nigeria to fulfil their various statutory mandates. Examples of such agencies include the National Identity Management Commission (NIMC), the National Population Commission (NPC), and the Independent National Electoral Commission (INEC), among others. Recent initiatives being implemented in some of such institutions have resulted in a significant increase in information processing.

Nigeria's National Identity Management System (NIMS) which is anchored on the National Identification Number (NIN) is one such initiative put in place for improved IDM in Nigeria. The NIMS serves as the core infrastructure of the NIMC's activities, connecting the institutional databases of various agencies under a sole platform thus providing a system for the unique verification and authentication of identities of each citizen and legal resident in Nigeria.[1] Registration under the NIN scheme is compulsory for all citizens and some residents of Nigeria. The mass processing of biometric information and other personal information is a key component of the NIMS.

Another recent initiative is the digitalization of the operations of the National Population Commission (NPC) under a public private partnership and the launching of NPC's eCRVS system. The NPC is a foundational institution in Nigeria's legal identity management sector responsible for the registration of births, deaths, marriages and other vital events. Digitalization efforts aim to modernize the operations of the NPC which are largely paper-based, and improve the overall IDM system of the country by increasing the efficiency and effectiveness of the NPC. The digitalization of NPC operations is part of wider digital transformation efforts of the Nigerian government across all government agencies.

The linking of each Subscriber Identification Module (SIM) card in the country to a National Identification Number under the country's 2021 National Identity Policy for SIM Card Registration (NIN-SIM policy) is another significant initiative that increases information processing by cross referencing data sets. This policy aims to among other things, boost the growth of the National Identity Database (NIDB) and contribute to national security through verification of information of mobile subscribers against the NIDB.[2]

[1] Damian Eke and others, 'Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural Concerns' (2022) (11) *Journal of Responsible Technology* 1-9 <https://doi.org/10.1016/j.jrt.2022.100039> accessed 21 June 2024.

[2] Federal Ministry of Communications and Digital Economy, 'Revised National Identity Policy for SIM Card Registration' <https://nimc.gov.ng/docs/revised_national_digital_identity_policy_on_sim.pdf> accessed 21 June 2024.

These and other legal identity management-related initiatives translate to a significant increase in the information processing activities of the Nigerian government, including the mass processing of sensitive, biometric information and personal information of children. Various security concerns arise from such increased information processing activities. For instance, mass personal data processing under the NIMS leads to data protection and cybersecurity concerns; digitalization of the NPC operations is a significant processing activity making the information systems of the NPC more accessible and more vulnerable, raising significant security concerns. Similarly, the NIN-SIM policy creates an increased risk of identity theft and fraud particularly as stolen NINs can be linked to SIM cards to be used for fraudulent activities using identities of unsuspecting victims.[3] Additionally, interconnected datasets increase the vulnerability of both the NIDB, managed by NIMC, and the SIM Database, managed by the Nigerian Communications Commission.

However, despite this significant increase in information processing activities of the government in the legal identity management sector, and in other public sectors, the extant legal framework for information security in the country remains inadequate with insufficient attention being paid to the commensurate legal and regulatory measures necessary to ensure information security. Concerns are heightened due to the lack of a single, robust, legal framework, specifically addressing the security of information and information systems within government agencies in Nigeria.

The signing into law of the country's National Data Protection Act in 2023 marked a significant milestone towards data security and improved IDM in Nigeria as this law provides for data security as a principle of data protection in Nigeria,[4] and also establishes the Nigeria Data Protection Commission as the country's independent data protection authority.[5] While this law significantly contributes to the regulation of information security in Nigeria, robust information governance and information security measures for the country's ID information systems remain inadequate. Nigeria's cyber law, the Cybercrime (Prohibition and Prevention etc.,) Act, 2015 does not adequately address this gap as it focuses mainly on criminalizing cyber offences rather than on information governance and information security measures for government agencies. These and more are discussed in this paper.

Information is the fuel that drives government processes and the government utilizes mass volumes of information in its everyday services and processes. Thus, the regulatory measures put in place for the security of volumes of information processed by the Nigerian government are critical. To provide an examination of information security

[3] Asad Baig, 'Digital Identify Thefts Rampant in Cities of Punjab: Citizens Conned for Their Biometric Prints to Issue Mobile Sims Using their Credentials' *Digital Rights Monitor* (Pakistan, 20 October 2017) <https://digitalrightsmonitor.pk/digital-identify-thefts-rampant-in-cities-of-punjab-citizens-conned-for-their-biometric-prints-to-issue-mobile-sims-using-their-credentials/> accessed 21 April 2024.

[4] Nigeria Data Protection Act 2023, ss 39-40.

[5] Nigeria Data Protection Act 2023, s 4.

measures, particularly within the country's legal identity management sector, this paper seeks to examine the legal framework for information security in Nigeria and its adequacy for legal identity management in the country. South Africa's regulatory framework for information security is used in this paper as a benchmark for regulatory measures that enhance information security. By analysing the legal framework for information security in Nigeria and its adequacy for ensuring the security of information processed within the country's legal identity management sector, this paper aims to make recommendations for increased information security in Nigeria's legal identity management sector and Nigeria's public service as a whole.

2. CONCEPTUAL CLARIFICATION

Information security (InfoSec) is 'the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.'[6] Confidentiality involves ensuring information is protected from unauthorized disclosure and access. Integrity involves ensuring information is accurate, trustworthy and protected from unauthorized modification. While availability is concerned with protecting access to information from unauthorized disruption and ensuring information is available to authorized persons when needed.[7] Confidentiality, integrity and availability are often referred to as the 'CIA triad'. These three principles form the foundation of information security initiatives of various entities that manage information systems. Ensuring these three elements are protected and upheld are the essential goals of information security measures put in place by organizations.

Ensuring the security of the information processed by an organisation requires various safeguards and other measures spanning across managerial, operational and regulatory spheres. According to the South African Centre for Information Security, InfoSec consists of three aspects – '25% of security is technical, 50% is internal organization, and 25% is regulatory and legal'.[8] This paper is concerned with the regulatory and legal aspects.

Oftentimes, information security and cybersecurity are used interchangeably. While they are interrelated concepts, information security is a more encompassing term that is concerned with the security of information and information systems in both analog and digital forms as opposed to cybersecurity which focuses only on the protection of digital information and the security of cyberspace, computer systems and networks.

[6] Celia Paulsen & Patricia Toth, 'Small Business Information Security: The Fundamentals' <https://doi.org/10.6028/nist.ir.7621r1> accessed 22 March 2024.

[7] ibid

[8] South Africa Center for Information Security <https://sacfis.co.za/> accessed 19 March 2024.

Cybersecurity is thus a subset of information security. Noteworthy is that Nigeria's identifying institutions and other government agencies utilize a combination of paper-based and cyber processes for enrolment, credential issuance, verification and authentication and other processing activities. Thus, this paper adopts the broader concept of InfoSec.

Another set of concepts requiring clarification are 'information' and 'data'. Although often used interchangeably, there is a subtle difference between both terms. Data is often used to refer to unprocessed raw facts including letters, numbers, symbols words etc. Such letters, numbers, symbols and words collected for a purpose but stored without additional context are commonly referred to as data. Information on the other hand refers to processed data. Raw data given context and meaning through various processing activities becomes information. Both concepts, 'information' and 'data', are however used interchangeably in this paper.

Information systems on the other hand refer to a network of interconnected components including hardware, software, processes and people that are used to collect, store and process data and to provide information and other digital products. Various public institutions in Nigeria use information systems to carry out their administrative and governance responsibilities. Legal identity refers to the documentation and registration of a person's identity, by a State, which establishes the person as a subject with rights and obligations, entitled to the protection of the State. Legal identity management on the other hand refers to the processes and systems by which legal identity information is collected, shared, verified, authenticated and otherwise processed by the State.

3. OVERVIEW OF INFORMATION SECURITY BREACHES OF LEGAL IDENTITY SYSTEMS IN NIGERIA

Some security breaches affecting the InfoSec of legal identity management systems have occurred in Nigeria. These include the February 2022 downtime of the National Identity Management Commission (NIMC) servers which prevented public and private agencies from using the NIMC National Identification Number Verification Service (NVS) to carry out ID verification and authentication services for over ten days. This significantly affected the third principle of the CIA triad, which is, availability of information systems. Services that were affected by the non-availability of the NVS included Nigeria's Immigration Service passport issuance services, banking services, telecommunication services and more. This downtime caused serious hardship to persons seeking to utilize the compromised services.[9]

[9] Editorial, 'Collapse of NIMC Server' *Daily Trust* (16 February 2022) <https://dailytrust.com/collapse-of-nimc-server/> accessed 23 April 2024.

Another security breach occurred in the previous NIMC mobile software application which was made available on Google Play Store. Reportedly, after downloading the application, persons were in some cases getting encryption errors while others were getting the personal information of strangers. This exposed the personal data of enrolees thus affecting the confidentiality of information systems.[10] This security breach resulted in litigation initiated by a civil society organisation against the NIMC.[11]

The 2015 breach of the website of the Independent National Electoral Commission (INEC) by a group named Team Nigerian Cyber Army, that also claimed to have access to other government services is another notable breach that compromised the integrity and trustworthiness of INEC's systems.[12] More recently, in March 2024, yet another security breach within the NIMC information system was alleged to have occurred which affected the confidentiality and integrity of the National Identity Database (NIDB). According to the Foundation for Investigative Journalism, a privately owned website called XpressVerify allegedly gained unauthorized access to the NIDB and sold access to the private information of enrolees stored in the NIDB to any interested individuals, for a small fee.[13] Following this occurrence, the Nigeria Data Protection Commission launched an investigation into the alleged security breach.[14]

With steps being taken by the Nigerian government towards growing Nigeria's digital economy and improving ID management in the country, the information systems of identifying institutions are increasingly vulnerable to attacks, breaches and other disruptions potentially resulting in ID thefts, denial of services, fraud, financial loss, cyber terrorism and other possible adverse effects. It is thus important to analyse the existing legal framework that governs InfoSec in Nigeria and its adequacy for ensuring the security of various government information systems that manage legal identities.

[10] Olugbenga Adanikin, 'How Presidential Aide Exposed Nigerians to Data Breach Via NIMC Mobile App Registration' *International Centre for Investigative Reporting* (18 August 2020) <https://www.icirnigeria.org/nin-how-presidential-aide-exposed-nigerians-to-data-breach-via-nimc-mobile-app-registration/> accessed 23 April 2024.

[11] See *Incorporated Trustees of Laws and Rights Awareness Initiative v NIMC* (2021) FHC/AB/CS/79/2020 (Unreported).

[12] Wale Odunsi, 'Nigeria Decides: INEC's Website Hacked' *Daily Post Nigeria* (28 March 2015) <https://dailypost.ng/2015/03/28/breaking-nigeria-decides-inecs-website-hacked/ > accessed 23 April 2024.

[13] Joseph Adeiye, 'ALERT: XpressVerify, a Private Website, has Access to Registered Nigerians' Data and is Making Money From it' *Foundation for Investigative Journalism* (16 March 2024) <https://fij.ng/article/alert-xpressverify-a-private-website-has-access-to-details-of-registered-nigerians-and-is-making-money-off-it/> accessed 13 April 2024.

[14] Justice Okamgba, 'Data Breach: NIMC Agents to Face More Scrutiny, Says NDPC' *Punch* (29 March 2024) <https://punchng.com/data-breach-nimc-agents-to-face-more-scrutiny-says-ndpc/#:~:text=The%20Nigeria%20Data%20Protection%20Commission> accessed 13 April 2024.

4. EXTANT LEGAL FRAMEWORK FOR INFORMATION SECURITY IN NIGERIA

Various laws, policies, guidelines and institutional arrangements regulate the protection of information systems managed by government institutions including identifying institutions.

4.1 Nigeria Data Protection Act 2023

The Nigeria Data Protection Act 2023 is Nigeria's data protection law. It provides for the principles of data protection in Nigeria including the principle of data security. The Nigeria Data Protection Act 2023 also covers other measures critical to ensuring the confidentiality, integrity and availability of information systems that process personal information in the country.

The Nigeria Data Protection Act 2023 requires data processors and data controllers to ensure that their processing activities safeguard the security of personal data and protect such personal data from unauthorised and unlawful access and processing as well as loss, damage, destruction and other breaches.[15] The CIA triad of InfoSec is codified in the Act, requiring a controller or processor to ensure that appropriate organisational and technical measures are utilized for safeguarding 'confidentiality, integrity and availability of personal data'.[16] The Act similarly requires data controllers and data processors to implement relevant measures to ensure the confidentiality, security and integrity of personal data.[17] Some possible security measures outlined in the Nigeria Data Protection Act 2023, which can be adopted to uphold InfoSec of information and information assets include:

(a) pseudonymization or other methods of de-identification of personal data;

(b) encryption of personal data;

(c) processes to ensure security, integrity, confidentiality, availability and resilience of processing systems and services;

(d) processes to restore availability of and access to personal data in a timely manner, in the event of a physical or technical incident;

(e) periodic assessments of risks to processing systems and services, including where the processing involves the transmission of data over an electronic communications network;

(f) regular testing, assessing, and evaluation of the effectiveness of the measures implemented against current and evolving risks identified; and,

[15] Nigeria Data Protection Act 2023, s 39(1).

[16] Nigeria Data Protection Act 2023, s 24(2).

[17] Nigeria Data Protection Act 2023, s 39(1).

(g) regular updating of the measures and introduction of new measures to address shortcomings in effectiveness, and accommodate evolving risks.[18]

The National Identity Management Commission's National Identification Number (NIN) tokenization is a pseudonymization technique, a good example of a data security measure adopted by one of the country's identifying institutions which protects data privacy of enrolees by using a coded, encrypted, representation (disguised) version of a person's NIN in place of the actual NIN for everyday transactions. Digital tokens used to substitute the NIN include Virtual NIN, User IDs, verification log details on the NIMC Mobile ID software application and QR codes. These are all methods of tokenization. Using these various tokens, NIMC provides platforms for authorised vendors to carry out verification and authentication of persons' identities against the National Identity Database without ever seeing the actual NIN.

Even though the Nigeria Data Protection Act 2023 explicitly states that its scope of application is to cover 'the processing of personal data, whether by automated means or not',[19] specific physical information security measures addressing security of premises, security in the physical handling of official devices etc, are not provided for in the Act. Additionally, strict InfoSec measures specifically related to the public service, are not contemplated in the Nigeria Data Protection Act, 2023 which is a primary legislation. Rather, such measures specifically related to the public service are provided for in an administrative guideline – the Guidelines for the Processing of Personal data in the Public Service of 2020 – issued by the National Information Technology Development Agency, an administrative agency. This is discussed in more detail, subsequently in this paper.

4.2 Cybercrime (Prohibition, Prevention Etc.) Act, 2015

The Cybercrime (Prohibition, Prevention Etc.) Act 2015 (Cybercrime Act 2015) is another critical legislation making up part of the extant framework for InfoSec being studied. This Act provides for the designation and protection of Critical National Information Infrastructure (CNII) in the country.[20] The Cybercrime Act 2015 also criminalizes certain offenses that could be committed within ID databases and information systems such as identity theft and unlawful access to stored data.[21] Relevant objectives of the Cybercrime Act 2015 are to 'ensure the protection of critical national information infrastructure' and 'to promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights'.[22]

[18] Nigeria Data Protection Act 2023, s 39(2).
[19] Nigeria Data Protection Act 2023, s 2(1).
[20] Cybercrime (Prohibition, Prevention Etc.) Act 2015, s 3.
[21] Cybercrime (Prohibition, Prevention Etc.) Act 2015, ss 22 and 28(3).
[22] Cybercrime (Prohibition, Prevention Etc.) Act 2015, s 1(b) and (c).

Although the Cybercrime Act 2015 does not expressly define Critical National Information Infrastructure, it gives some insight into its meaning when it provides that:

> the President may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, and or networks, whether physical or virtual, and, or the computer programs, computer data and, or traffic data vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure.[23]

Nigeria's legal identity ecosystem is a network of interconnected identity information systems and databases that are foundational in various sectors in the country and are crucial to the country's human, economic and national security. Instances of identity theft, security breaches of legal identity information systems and other fraudulent activities within this ecosystem can adversely affect public health, public trust, law enforcement and safety of persons. Banking and social security services and transactions would be significantly affected if any of these information systems are breached, incapacitated, or destroyed. Such security breaches would also significantly undermine the reputation of the Nigerian government. It is thus the humble opinion of this paper that the country's legal identity ecosystem, which is composed of various legal identity databases and information systems, qualifies as Critical National Information Infrastructure (CNII) under extant law. However, no president has yet officially designated any CNII in the country in a Federal Gazette, pursuant to the Cybercrime Act 2015.

The Presidential designation of CNII is crucial as, under the Cybercrime Act 2015, it could prescribe preservatory and protection measures related to the management of CNII, regulate access to, control, and transfer of data stored in CNII, establish procedural rules to ensure the authenticity and integrity of information stored in the CNII, outline data recovery measures, require audits of CNII by the Office of the National Security Adviser and provide for other related matters necessary for management, control and protection of data in CNII.[24]

The Cybercrime Act 2015 also extensively prescribes punishments for certain offences that could affect legal identity information systems such as unauthorized access to computer systems for fraudulent reasons, obtaining data vital to national security without authorization, unlawfully interfering with information systems, unlawful

[23] Cybercrime (Prohibition, Prevention Etc.) Act 2015, s (3)(1).

[24] Cybercrime (Prohibition, Prevention Etc.) Act 2015, ss 3 and 4.

interception of data, unlawful modification of stored data, cyber terrorism, and identity theft and impersonation.[25]

As the title implies, the Cybercrime (Prohibition, Prevention Etc.) Act, 2015 focuses extensively on the detection, prevention, prohibition, prosecution and punishment of cybercrimes in Nigeria. Certain provisions of the Act criminalize some actions committed specifically by public sector employees in the course of their duties, for instance, manipulating electronic payment devices by public sector employees, with an intent to defraud and to underpay or overpay a public sector employee, is liable to punishment by imprisonment and forfeiture of the stolen item or amount.[26] However, this Act does not specifically address the Nigerian government's vulnerability to cyberattacks, digital and physical security measures for information systems and security of public sector information systems generally.

In addition to the primary legislation discussed above, certain secondary laws also contain relevant provisions for the security of the ID management system in Nigeria.

4.4 Access to Register Information in the National Identity Database Regulations 2017

As Nigeria's national ID management authority, the National Identity Management Commission (NIMC) has set the pace in the country's legal identity management sector through the issuance of regulations that contain relevant security controls for its information systems. The Access to Register Information in the National Identity Database Regulations 2017 provides various access controls regulating the access to information in the National Identity Database (NIDB) by security agencies, licensed private individuals and public agencies. It provides security controls for the platforms provided to such entities to enable access to the NIDB including login credentials for proper auditing, password protection and access level controls in regulations 5(4), 6(4) and 7(4) of the Access to Register Information in the National Identity Database Regulations 2017. However, these standards specifically address the processing activities of the NIMC and do not apply to other federal identifying agencies[27] or other government agencies.

[25] Cybercrime (Prohibition, Prevention Etc.) Act 2015, ss 5-22.

[26] Cybercrime (Prohibition, Prevention Etc.) Act 2015, s 14(4).

[27] There are about 16 federal institutions in Nigeria who process the personal information in Nigeria for various statutory purposes. In addition, various state local government and private organisations are also involved in the processing of personal information for myriad reasons. National Identity Management Commission, 'The Digital Ecosystem' <https://nimc.gov.ng/digital-identity-ecosystem/> accessed 21 July 2024.

4.5 Registration of Persons and Contents of the National Identity Database Regulations 2017

The Registration of Persons and Contents of the National Identity Database Regulations 2017 is also relevant as it directs in its regulation 3(2), that the information stored in the country's NIDB is to be treated as 'classified matter' as defined in the Official Secrets Act 1962, thus granting a higher degree of security to such information. The Official Secrets Act defines 'classified matter' as 'any information or thing which under any system of security classification from time to time in use by or by any branch of the government, is not to be disclosed to the public and of which the disclosure to the public would be prejudicial to the security of Nigeria'.[28] This higher level of legal protection granted to the information stored in the NIDB, by designating such information as classified matter, is not accorded to the at least 14 other federal databases of identifying information containing personal and sensitive information of Nigerians and residents.

4.6 Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020

The Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020 outlines certain InfoSec measures to be put in place by public institutions to foster the confidentiality, integrity, availability and resilience of processed data. Such public agencies are required to demonstrate compliance with international InfoSec standards such as ISO 27001:2013, comply with relevant data privacy laws, conduct Data Protection Impact Assessments and retain Data Protection Compliance Organizations.[29] Sharing of processed personal data with personal identifiers between public agencies is required to be carried out using encrypted formats or other cryptographic methods to protect the personal data from easy access by unauthorized third parties. These Guidelines also prohibit the sharing of databases through hardcopies, emails, and other non-cryptographic formats. Anonymization or pseudonymization of personal data which is to be shared for purposes of intelligence gathering, mapping or predictive analysis is also required.[30]

It should however be noted that unlike the Nigeria Data Protection Act 2023, the Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020 is not a primary law enacted by parliament. It is a secondary guideline issued by an executive agency, the National Information Technology Development Agency (NITDA), in 2020, to serve as a gguideline for the implementation of the Nigeria Data Protection

[28] Official Secrets Act 1962, s 9(1).

[29] Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020, para 2.6.

[30] Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020, para 4.0.

Regulation 2019 (NDPR) within public institutions in the country. The NDPR, issued by the NITDA in 2019, is the predecessor to the Nigeria Data Protection Act 2023, and was the first attempt by the Nigerian government to establish a data protection law for the country. According to section 64(2)(f) of the Nigeria Data Protection Act 2023, provisions of the NDPR remain in force in Nigeria to the extent they do not contradict the provisions of the Nigeria Data Protection Act 2023.

4.7 Revised Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry of 2021 (Revised Regulatory Framework for BVN Operations)

The Revised Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry of 2021 (Revised Regulatory Framework for BVN Operations) is another regulatory instrument emanating from an executive agency, the Central Bank of Nigeria. It is relevant in this paper as it defines key processes related to information security of Nigeria's BVN information system, to protect BVN information from unauthorized access and use, and to ensure confidentiality, integrity, and availability of such information.[31]

One unique provision in this instrument is that it specifically requires a Federal High Court order to be obtained and presented by specific organisations, to gain access to BVN information. Specifically, Pension Fund Administrators, the National Pension Commission, law eenforcement aagencies, and other approved entities require a Federal High Court Order to be given access to BVN information.[32] This provision is unique as such court order is not required for access to other relevant legal identity databases in the country.

Other critical provisions of the Revised Regulatory Framework for BVN Operations clearly outline roles and functions of key stakeholders responsible for InfoSec of the BVN information system. The major stakeholders are the Central Bank of Nigeria, the NNigeria Inter-Bank Settlement System (NIBSS) and banks and other financial institutions. CBN performs regulatory oversight functions, approves eligibility of users for accessing BVN information, monitors entities with an interest in the BVN database, and applies sanctions as necessary for non-compliance with applicable guidelines.

The NIBSS maintains the BVN Database, manages access to the BVN information by approved users, ensures security of BVN information and general seamless operations

[31] The BVN is a digital identifier that is used for the unique identification of persons in Nigeria's banking sector. The BVN is issued by Nigeria's apex bank (the Central Bank of Nigeria), in collaboration with various other banks.

[32] Revised Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry 2021, para 1.8.

of the BVN system, and provides Application Programming Interfaces (APIs) to enable integration of the BVN database with the systems of various eligible institutions for online validation of watch-listed BVNs, among other duties. Various banks and other financial institutions operate with approval from the CBN and ensure accuracy in capture of BVN information and uniformity of customers' details in the BVN database, and across all of such customer's wallets and accounts in the banking industry for integrity of the overall system, among other duties.[33]

4.8 Revised Federal Civil Service Handbook, 2010

Nigeria's Revised Federal Civil Service Handbook, 2010 outlines certain provisions related to data protection in the federal civil service with a focus on automated data processing and the data subject's right to information and right to amendment of personal data held by civil service agencies. The Revised Federal Civil Service Handbook however does not go into details on information management and information security measures within the federal civil service agencies.

As mentioned earlier, information systems managed by various federal identifying institutions in Nigeria utilize both paper-based and digital processes. For instance, Section 9(2)(a) and (b) of the Electoral Act 2022 requires the country's electoral authority, that is the Independent National Electoral Commission (INEC), to keep Nigeria's Register of Voters at the INEC National Headquarters and at other locations selected by INEC, in both '(a) electronic format in its central database; and (b) manual, printed, paper-based record or hard copy format'.

Similarly, the National Population Commission (NPC), the country's population authority, still uses paper-based processes for the collection, storage and transmission of identification information while carrying out its civil registration functions, in the majority of its centres nationwide. However, digitalization efforts of NPC operations are underway. Other relevant identifying institutions like the National Identity Management Commission and the Federal Road Safety Commission also use a combination of both paper-based and digital ID processes in carrying out their legal identity management functions. Thus, the security of physical premises, filing cabinets, network systems and electronically stored data are all critical information security considerations.

The primary and secondary laws discussed above contribute significantly to information security within Nigeria's identity management sector and other governance sectors. However, these laws do not specifically address InfoSec measures for information stored and processed using non-automated means. For instance, the security of physical premises, cabinets, warehouses and other modes of non-digital storage are inadequately, if at all, addressed. Additionally, the security of hand-held devices issued to public service employees and used in storage and other modes of processing of official information

[33] Revised Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry 2021, para 1.5.1-1.5.3

including personal information are not outlined. Clear information governance frameworks, specifically providing for information security officers, officers responsible for incident reporting, staff training on information security and similar, related issues, are also not provided for in the applicable law.

Furthermore, sector-specific laws addressing access to legal identity databases are provided only for the National Identity Management Commission's National Identity Database and the Central Bank of Nigeria's Bank Verification Number Database. However, several other agencies, including about 14 other federal agencies, have identity databases under their control in which they process the personal information, including biometric information, of millions of Nigerians. These include the Voters Register under the control of the Independent National Electoral Commission, the National Social Register under the control of the National Social Safety Net Coordinating Office, and the Central Data Base for drivers and vehicles under the control of the Federal Road Safety Commission.

Access controls for such databases and other InfoSec measures are however not provided for in extant laws. Additionally, only information stored in the National Identity Database is designated as 'classified matter' under the Official Secrets Act, 1962. Such classification is not used for other critical ID databases within Nigeria's digital identity ecosystem, indicating that an appreciation of the need for information security of Nigeria's identity ecosystem as a whole is not contemplated.

5. LESSONS FROM SOUTH AFRICA ON INFORMATION SECURITY OF LEGAL ID SYSTEMS

South Africa presents a more comprehensive framework for InfoSec within its public service than Nigeria. Some relevant legal instruments in South Africa that provide for the management and security of information in the public service, including in government-identifying institutions, are the Public Service Act 1994, Public Service Regulations for South Africa 2016, the Department of Public Service Administration's Directive on Public Service Information Security, and the Protection of Personal Information Act 2013.

South Africa's Public Service Act 1994 designates the power to establish information management standards and norms for South Africa's public service in the office of the Minster for Public Service and Administration (the 'Minster').[34] Additionally, the Public Service Act 1994 vests power to make regulations on the Minister.[35] Pursuant to these powers, the South Africa Public Service Regulations 2016 was issued by the

[34] Republic of South Africa Public Service Act 1994, s 3(1)(f).

[35] Republic of South Africa Public Service Act 1994, s 41.

Minister for Public Service and Administration. The Minister for Public Service and Administration is required by the Public Service Regulations 2016 to issue information security standards for South Africa's public service. Persons working with public service information resources are to comply with the InfoSec standards issued by the Minister according to Regulations 94(1) and (2) of the Public Service Regulations 2016.

Apart from the mandate given to the Minister for setting general InfoSec standards for the public service, the Public Service Regulations 2016 further places governance responsibilities for setting institution-specific standards, regulations, incident reporting and vigilance on various personnel, fostering InfoSec within the public service. Specifically, Regulations 95(1) and (2) of the Public Service Regulations 2016 require that:

> (1) A head of department shall ensure the maintenance of information security vigilance at all times in the department.
>
> (2) When non-compliance with the information security standards referred to in regulation 94(1) comes to the knowledge of an employee of a department, he or she shall report it immediately to the head of department or an employee designated for this purpose by that head.

Furthermore, the Public Service Regulations 2016 require heads of departments to carry out regular incident reporting to requisite authorities – including the 'Director General, State Security Agency, Auditor General and such other authorities as the head considers appropriate' – in cases of non-compliance with established InfoSec standards. Incident reports are also required to include a plan of action for remedying incidents of non-compliance and for the prevention of their reoccurrence.[36]

Such a clear delineation of information security responsibilities is important as they foster accountability as well as transparency of government agencies in their information management responsibilities. By bestowing the responsibility for information security vigilance in the department on the head of department, and by placing the responsibility for incident reporting on employees of departments; who report to heads of departments, and on heads of departments who report to higher authorities, a clear chain of responsibility for monitoring and upholding InfoSec in the public service is established.

In 2020, South Africa's Minister of Public Service and Administration fulfilled the responsibility imposed by Regulation 94(1) of the Public Service Regulations 2016 to set InfoSec standards for the public service, and issued the Directive on Public Service Information Security 2020 (the Directive). This Directive details a broad framework for InfoSec within the South African public service. The overarching purpose of the Directive on Public Service Information Security 2020 as enshrined in its paragraph 2 is to 'provide

[36] Republic of South Africa Public Service Regulations 2016, regs 96(a) and (b).

direction in the public service regarding establishing departmental information security governance, practices, and procedures to protect information and technology assets.'

Under the Directive, a clear information governance structure is established for government departments with heads of departments being responsible for the overall security of information assets in various departments. Such heads of departments are to put in place InfoSec policies aligned with the provisions of the Directive.[37] An official within the various government departments is required by the Directive to be delegated as the Department Information Security Officer (DISO) and is to be accountable to the Government Information Technology Officer for InfoSec related matters. An information communications technology (ICT) steering committee is to be established for the department and is to function as an InfoSec forum.[38]

Further InfoSec guidelines are highlighted in Paragraph 11 of the Directive, which requires heads of departments to train employees on InfoSec, the identification and reporting of InfoSec attacks and threats and the handling of sensitive information among others. Specifically, this provision states that the head of department should ensure that:

(a) The DISO develops and implements a continuous information security awareness program to reduce cybersecurity risks from employees in the department.

(b) The information security awareness program must train employees to recognize & report cyberattacks (phishing, baiting, tailgating, etc) as well as train employees to properly handle (store, transfer, and destroy) sensitive data.

(c) The information security awareness program must include security awareness or skills training targeted for specific roles including system administrators, web application developers, and the helpdesk administrators.

(d) An appropriate summary of the departmental information security policy is included in the HR policies that all employees sign before starting any work in a department.

Another important security measure established in the Directive is the establishment of security awareness programs in government departments. Such programs are established by Department Information Security Officers (DISO) on a continuous basis to train and equip government employees to be able to handle sensitive data, to recognise cyber attacks, and to report such attacks. A summary of the departmental information security policy is required to be included in the human resource policies signed by employees prior to commencing work in any department.[39]

[37] Republic of South Africa Directive on Public Service Information Security 2020, para 6.

[38] Republic of South Africa Directive on Public Service Information Security 2020, para 9(a)-(c).

[39] Republic of South Africa Directive on Public Service Information Security 2020, para 11

Such continuous security awareness and training is invaluable in government offices as it helps to build an information security and data protection culture among employees.

A range of critical physical security InfoSec measures are also outlined in the Directive. This is crucial in South Africa's public service, which, like Nigeria's public service, utilizes digital and manual processes in government information systems including in the information systems of legal identity institutions. Such physical InfoSec measures are required to be ensured safe by the head of department and they include:

1. Physical security measures for departmental information technology (IT) assets such as lockable cabinets, server rooms and restriction of other physical assets from unauthorized access.
2. Measures to be put in place to mitigate against environmental hazards and threats such as fire, theft, water damage.
3. Implementation of access controls at entrances to server rooms and data centres including multifactor authentication and access logins.
4. Suitable security is placed at the entrance of facilities that are used to store ICT infrastructure, including server rooms and data centres among others.
5. The provision of an alternative power supply source such as a generator to provide uninterrupted power supply to power crucial IT systems, and quarterly maintenance of such power source.
6. Putting in place confidentiality agreements and maintenance agreements to foster confidentiality and security of information stored in hardware subject to off-site and 3rd party access.
7. Measures to ensure that all persons assigned devices containing government data or which are connected at any time to the government network, including laptops, smartphones, tablets, etc., do not leave such devices unattended in public places or motor vehicles.
8. The use of 'FollowMe print' for protecting the printing of confidential documents, in the absence of which, sensitive or other restricted documents must be immediately removed from printers when printed.
9. Ensuring that following the departmental loss protocols and procedures, theft or loss of information assets is treated as a security breach and immediately reported.
10. Implementing mobile device management tools to assist with tracking and recovery of government notebooks and laptops.

11. Putting in place procedures, processes and technical controls to manage risks associated with removable media such as data loss, data leaks, malware infection, data sensitivity etc.[40]

Other critical matters addressed in the Directive include but are not limited to human resource security which is to be ensured by the head of department and includes the clear definition of InfoSec responsibilities and roles of employees and third-party users in departments, background and security vetting checks for contractors in line with applicable laws and ethics, and the classification of information being accessed, including the possible risks.[41] Backups are required to be carried out frequently by the head of department, based on sensitivity of various data.[42] Access control management using login privileges, user-access rights, privileged access rights, etc are to be implemented.[43] Password management is also to be implemented by the head of department, utilizing password standards, encryption of stored passwords, multifactor authentication on critical systems among other measures.[44]

6. CONCLUSION AND RECOMMENDATIONS

Information is the fuel of Nigeria's public sector both within identifying institutions and other public institutions. Various security breaches that have been experienced within Nigeria's legal identity sector highlight adverse effects that can arise when information security is threatened or breached. Such effects include non-access to critical services, risks of identity fraud and other types of fraud, loss of confidence in the government, exposure of personal information, endangerment of personal safety and much more. Thus, ensuring the security of information systems and information assets within Nigeria's federal identifying institutions, as well as other public service institutions, is critical for protecting the well-being of Nigerian citizens and the State.

South Africa's regulatory approach towards upholding information in the public service was used in this study as it provides a good case example of robust information security and information governance frameworks in the public service. In light of the foregoing, the study makes the following recommendations.

Firstly, the fact that the vast majority of the country's information security obligations are contained in various laws, executive guidelines, regulations and policies is unsatisfactory. A single regulatory framework is necessary, outlining foundational information management and information security measures for government institutions.

[40] Republic of South Africa Directive on Public Service Information Security 2020, para 15

[41] Republic of South Africa Directive on Public Service Information Security 2020, para 16(1)(a) and (b).

[42] Republic of South Africa Directive on Public Service Information Security 2020, para 17.8.

[43] Republic of South Africa Directive on Public Service Information Security 2020, para 20.

[44] Republic of South Africa Directive on Public Service Information Security 2020, para 21.

This paper recommends that relevant officers including the National Security Adviser, the National Commissioner of the Nigeria Data Protection Commission working with the office of the Head of the Civil Service issues a guideline on public service information security for all officers of the public service including civil service workers.

Borrowing a leaf from South Africa, such a guideline should address information governance and InfoSec responsibilities, placing the office of the Head of the Civil Service of the federation in charge of information governance in Nigeria's civil service, responsible for establishing governance norms and setting standards for management and security of information within the country's civil service. The Head of the Civil Service should also be responsible for regular training of civil servants towards information security of government information systems. The president as the commander in chief of the armed forces, and heads of other institutions falling within the public service but outside the civil service should also be given the responsibility for setting standards towards information management and information security within such institutions.

Responsibilities need to also be placed on the chief executive officers (CEOs) of various government agencies and departments to implement standards set by the Head of Civil Service, the president and other relevant heads. Other managerial staff are to carry out vigilance and incident reporting of InfoSec breaches. Reports of security incidents and breaches should be made to the Chief Executive Officers of government ministries, departments and other agencies, who are then to escalate such reports to designated authorities like the Head of Civil Service, the Nigeria Data Protection Commission, National Computer Emergency Response Team Coordination Center and the Office of the National Security Adviser. Such guidelines should also provide for the appointment of information security officers within government ministries, departments and agencies who are to work with the CEO in establishing information security awareness programs, training on security awareness and the implementation of physical security measures.