MANAGING EMERGING CYBERSECURITY AND PRIVACY IN NATIONAL IDENTITY MGMT

CISO NIMC

AGENDA

- WHAT IS IDENTITY
- IDENTITY MANAGEMENT
- CYBER THREATS TO IDENTITY
- PRIVACY THREATS TO IDENTITY
- MITIGATION
- HOW TO DO YOUR PART

What is Identity?

Identity refers to the characteristics or attributes that define an individual or entity and distinguish them from others.

It includes both physical and non-physical attributes, such as name, age, gender, nationality, occupation, biometric data, online identifiers, and more

NIMC IDENTITY MANAGEMENT

The National Identity Management Commission (NIMC) is the agency given the sole responsibility for managing identity in Nigeria.

Our primary function of the NIMC is to create and maintain a centralized national identity database, known as the National Identity Database (NIDB), which contains the biometric and demographic information of all registered citizens and legal residents of Nigeria.

NIMC also collaborates with other government agencies and private sector organizations to ensure the seamless integration of the National Identity Database into various applications and systems for efficient service delivery.

NATIONAL IDENTITY MANAGEMENT

The NIMC manages identity through the following processes:

- REGISTRATION: The NIMC registers individuals by capturing their biometric and demographic information.
- VERIFICATION: The NIMC verifies the identity of individuals by comparing their biometric data against the data in the NIDB to confirm their identity.
- AUTHENTICATION: The NIMC provides a means of authenticating the identity of registered individuals using their unique National Identification Number (NIN), which is issued to each individual upon registration.
- UPDATING RECORDS: The NIMC allows individuals to update their records in the NIDB in case of changes to their personal information or biometric data.

CYBER THREATS AFFECTING IDENTITY MANAGEMENT

1. **DATA BREACHES**: The National Database is a target of malicious actors seeking to steal sensitive data. A data breach could result in identity theft, financial fraud, and other forms of cybercrime.
2. **INSIDER THREATS**: Employees or contractors with access to NIMC's systems and data pose a cybersecurity risk, whether through malicious intent or accidental actions such as falling victim to social engineering tactics.
3. **RELYING TECHNOLOGY**: NIMC relies on technology to manage the National Database, some of these technologies come with inherent risks and requires continuous updates, patches and upgrades. If the technology is not properly managed, a threat actor may be able to exploit.
4. **HUMAN FACTOR**: Attackers may use social engineering tactics, such as phishing or impersonation, to trick employees or stakeholders into revealing sensitive information or compromising the NIMC's systems.

PRIVACY THREATS AFFECTING IDENTITY MANAGEMENT

1. **DATA MISUSE**: The NIMC collects and stores sensitive biometric and personal data about citizens, which could be misused if it falls into the wrong hands or if used for purposes other than what it was originally intended for.
2. **INSUFFICIENT CONSENT**: may be required to provide their biometric and personal data to NIMC without fully understanding the implications of doing so or without giving informed consent.
3. **DATA HARMONIZATION**: The NIMC may share citizens' data with other government agencies or private sector organizations for various purposes, raising concerns about data privacy and security.

MITIGATIONS TO ISSUES

- NIMC certified for the 10th year to ISO 27001:2022 which ensures access controls, strong authentication mechanisms, encryption, and regular software updates and patching
- Employee and contractors are put through training and awareness programs to help prevent insider threats and social engineering attacks.
- NIMC ensures regular security audits and penetration testing to help identify vulnerabilities and ensure that the NIMC's systems and data are adequately protected against cyber threats.
- NIMC relies on special interest groups such as NCS, NG CERT, USCERT to stay abreast of emerging cybersecurity trends

HOW TO DO YOUR PART

- Keep private your PII
- Spread awareness to friends and family
- Report security incidents to NGCERT incident@cert.gov.ng or NIMC info@nimc.gov.ng customercare@nimc.gov.ng in cases of extortion actu@nimc.gov.ng

THANK YOU