Appendix 1

THE GOVERNMENT OF JAMAICA

NATIONAL IDENTIFICATION AND REGISTRATION POLICY FOR JAMAICA.

April 2020

'One Person; One Identity'

LIST OF ACRONYMS

AML/CFT	Anti-Money Laundering & Countering the Financing of Terrorism
BOJ	Bank of Jamaica
e-Gov	e-Gov Jamaica Limited
e-ID	Electronic Identification
EOJ	Electoral Office of Jamaica
EU	European Union
GDPR	General Data Protection Regulations
GoJ	Government of Jamaica
ID	Identification
KYC	Know Your Client/ Know your Customer
LAC	Latin America and the Caribbean
MDA	Ministries Departments and Agencies
M&E	Monitoring and Evaluation
MLSS	Ministry of Labour and Social Security
MNS	Ministry of National Security
MOU	Memoranda of Understanding
MSET	Ministry of Science Energy and Technology
NIA	National Identification Agency
NIC	National Identification Card
NID	National /Identification Database
NI Data	National Identification Data
NIDS	National Identification System
NIN	National Identification Number
NIRA	National Identification Registration Authority
OPM	Office of the Prime Minister
PATH	Programme of Advancement Through Health and Education
PICA	Passport Immigration and Citizenship Agency
RGD	Registrar General's Department
SLA	Service Level Agreement
TRN	Taxpayer Registration Number
Voter's ID	Voter's Identification

ACKNOWLEDGEMENTS

The Permanent Secretary of the Office of the Prime Minister (OPM) would like to thank the National Identification System Policy Review Committee (NIDSPRC) for its role in revising the NIDS Policy. The Permanent Secretary also acknowledges and thanks the members of the NIDS Project Executing Unit and the Ministry of Justice who provided oversight and guidance in the process.

Special mention must be made of the participation of the various Ministries, Departments and Agencies (MDAs), some of which were represented on the NIDSPRC. These include:

- The Office of the Prime Minister
- The Cabinet Office
- The Ministry of Economic Growth and Job Creation
- The Office of the Parliamentary Counsel
- The Ministry of Justice, Legal Reform Department
- The Bank of Jamaica
- The Ministry of Finance and the Public Service
- The Ministry of Justice
- The Registrar General's Department
- eGov Jamaica Limited
- Tax Administration Jamaica
- The Passport, Immigration and Citizenship Agency
- The Planning Institute of Jamaica
- The Ministry of Labour and Social Security.

Additionally, the Permanent Secretary would like to thank the Attorney General's Chambers for the independent legal guidance provided.

Table of Contents

PREFACE

This policy sets out the background, motivation and principles which underpin the development of a National Identification System for Jamaica, the necessary legislative and other changes to make this a reality and the system for overseeing the implementation of the policy once developed.

EXECUTIVE SUMMARY

1. A secure national identification system for Jamaica has the potential to positively transform the efficiency and transparency of interactions between the state and the citizens and residents with significant additional positive effects for private businesses. The National Identification System (NIDS), when implemented, will provide a safe, convenient and reliable means for persons to prove their identity while aiding in the furtherance of the digitalisation of Government, which is expected to reduce bureaucracy and encourage efficiency and accountability in the public sector. Additionally, when government and private sector transactions are based on a secure National Identification Number (NIN), supported by a National Identification Card (NIC); crimes such as identity theft, fraud, trafficking in persons [1][2]and other crimes related to identity and property will be significantly reduced.
2. Identity theft and fraud is a growing problem in the global economy, and a NIC will provide an avenue for greater security and privacy of personal information when carrying out electronic and paper-based transactions.
3. The use of minimum biometric data (fingerprints, facial image and manual signature) in identity verifications guarantees that a person will have only one identity and will prove to be a more effective method of securely and accurately assigning a unique number to that person.

[1] National Taskforce Against Trafficking in Persons reported that between 2010 and 2016 only 62 victims were rescued. https://jis.gov.jm/information/get-the-facts/get-the-facts-trafficking-in-persons/

[2] The Office of the Children's Advocate reported that there were 33 reported cases of Child Trafficking received by the OCR between 2007 -2012. (information culled from OCA Annual Reports 2012-2013 and 2009-2010). http://www.welcome.oca.gov.jm/resources/

4. Enrolment in the National Identification System will be **voluntary** and will be supported by the rollout of a robust public education campaign to encourage take-up by all eligible persons.
5. It is proposed that NICs should be available to eligible persons from the age of six (6) years and that the NIN should be available to eligible persons from birth.
6. The assignment of a NIN will be done at enrolment.
7. The key to ensuring a successful system will be the security of the Government held identity databases and strong regulatory oversight.
8. The ability of every eligible person to apply for, and obtain from the state, a secure and verifiable NIN and NIC that will be a secure form of identification that would bring to fruition the vision of '**One Person; One Identity**'.

INTRODUCTION

1. Identification is routinely required by the Government as well as the private sector to facilitate the carrying out of transactions, such as accessing financial services or applying for government benefits.
2. Traditionally in Jamaica, identity has been verified through functional identity documents such as passports, Taxpayer Registration Numbers, Voter Identification Cards, School Identification Cards and Driver's Licences although these forms of identification were not issued for a multiplicity of purposes. In many instances, such as when opening a bank account, at least two such documents are required to prove identity. This is a time consuming and inefficient way of verifying identity, which relies on persons being able to provide multiple identity documents.
3. The National ID will remove the need for persons to provide two forms of ID as part of the KYC requirements.
4. The NIDS will increase the possibility for persons to complete e-commerce transactions securely and efficiently in Jamaica.
5. This policy highlights the benefits to be derived from a National Identification System by individuals, businesses, and Government in facilitating secure commerce in a digital economy, enabling e-government services, and improving security for online transactions.
6. The establishment of a NIDS will contribute to the achievement of crucial 'Vision 2030' goals including adequate social protection, security and safety, effective governance, an enabling business environment, a technology-enabled society and improved national competitiveness.
7. At present, the Electronic Transactions Act provides the framework for the conduct of electronic transactions, and it is anticipated that such transactions will grow exponentially given the advent of the NIC and an Electronic-ID System, which will facilitate ease and security of doing real-time/online transactions with the use of electronic signatures.

OVERALL SITUATIONAL ANALYSIS

1. Jamaica is lagging significantly in terms of its adoption of electronic government applications.[3] [4] Jamaican citizens spend many hours of productive time conducting business transactions with the private sector and the Government[5]. Very few government transactions can be completed in one visit to a government office and even if the transaction is completed in one visit, the wait time is often significant[6]. Time spent conducting business in Jamaica is the time that is taken away from work and private life and thus negatively affects both labour productivity and quality of life.
2. Digital transactions lessen wait times, reduce the opportunities for corruption and are much cheaper to conduct than paper-based transactions. At present, only a limited number of government transactions can be started and finished online[7]. It is envisaged that a robust National Identification System will be the cornerstone for Jamaica to advance significantly in delivering more efficient services, reducing transactional bureaucracy and improving the quality of public services.
3. The occurrence of identity theft and financial crimes is on the increase in Jamaica. The PICA reported that a total of 2499 passport fraud cases were detected and prosecuted during the period 2009-2019. The data shows the movement from 228 occurrences in the

[3] While the TAJ has introduced the Virtual Tax Office which allows Jamaican the ease and convenience to pay and file certain taxes online for example business related taxes, Consumption Taxes, Property Taxes and Traffic Tickets the person using this service must have a valid credit card, an email address and TRN https://www.jamaicatax.gov.jm/documents/10181/106828/paying_and_filing_online_09052016.pdf/1ac0f0a9-54b8-4f94-8bcc-ab53098ac03f

[4] The RGD currently offers many online services for example Birth, Death or Marriage Certificate, Application for Genealogy Research, Application for Entry Number and Application Status the payment for these services are done via valid credit card with local customers being required to visit the RGD to collect Birth, Death or Marriage certificate. These certificates are sent by UPS to foreign customers. The result for the other searches is sent to the applicant via email.

[5] A study undertaken by the Inter-American Bank indicates "that the average time to complete one government transaction in Jamaica was 4.1 hours"- Wait No More- Citizens, Red Tape and Digital Government Caribbean Edition 2019 page 15.

[6] "In Jamaica, just 11 percent of all transactions were completed in one visit, and more than 45 percent of all transactions required three or more visits to a public office to be completed"- pages 17-19 supra.

[7] It was reported that in Jamaica only 16.8% of government transactions can be started and completed online- page 30 supra.

year 2009 to 317 in the year 2019.[8] The MNS reported that a total of 417 cases involving identity theft were reported to the anti-fraud squad between 2008 and 2019, most of which were related to the use of the TRN[9]. The RGD reported that 1,072 cases of forged birth certificates were detected by the agency between 2010 and 2018.[10]

The MSET reported that in 2017 alone there were 474 cybercrime reports filed in Jamaica, up from 432 in 2016, 154 in 2015 and 103 in 2013, showing a significant upward trend[11].

4. (a) This data further indicates that the risk of identity theft and financial crimes is significant in Jamaica and that the existing identity documents are vulnerable to falsification, theft and abuse. A secure national ID tied to a person's biometrics would be the cornerstone of a strategy aimed at countering identity theft and financial crimes and reducing their impact on persons.

(b) The Voter's ID has two low level biometric input and one high-level biometric input, these are photographs and signature, and fingerprints, respectively. However, the Voter's ID does not capture the entire population, as persons below 18 years of age are excluded from registration. The TRN has a sequential randomised number but has no supporting biometrics. The Jamaican drivers' licence and passport have two low-level biometrics that are photograph and signature.[12] These are functional identifications in that they were created by legislation for specific purposes. While anyone can apply for a passport, the drivers' licence is only accessible to persons seventeen years and older. Additionally, while there are costs associated with the drivers' licence and the passport, the national identification card will be offered by the state and will be accessible to persons upon enrollment.

(c) The national identification card supports strong authentication through the use of digital certificates, biometrics as digital credentials, cardholder consent and full onboarding for digital services. Therefore, biometrics are crucial to minimise the risks of

[8] Source; Government of Jamaica. Passport, Immigration & Citizenship Agency (PICA)- Appendix II
[9] Source: Government of Jamaica. Ministry of National Security -Appendix III
[10] Source; Government of Jamaica. Registrar General's Department- Appendix IV
[11] Source: Government of Jamaica. Ministry of Science Energy and Technology- Appendix V
[12] Source: Government of Jamaica. National Identification Policy October 2016 page 8

duplicate identities. In other words, biometrics guarantee the uniqueness of the registration of identity in the National Identity Database. Biometrics allow persons to authenticate based on **who they are** instead of using something they have, such as a PIN or password.

(d) These are the same reasons why the EOJ and PICA are using biometrics to eliminate voter fraud and fraudulent passport, respectively. This is also the standard used by the International Civil Aviation Organization (ICAO) and most countries around the world to secure identity documents.

(e) Additionally, the introduction of a National Public Key Infrastructure as the core security backbone for the new digital identification will be the core security that differentiates the National ID from existing IDs. Additionally, introducing the requirement for persons always to authenticate based on who they are, is an additional layer of security.

5. The biometrics and rationale for its collection are:

a) Fingerprints:

(i) are universal, in the sense that virtually everybody has them;

(ii) are unique in the sense that it is highly probable that a person will have the same fingerprint as another. Also, since each fingerprint is independent of the other, when two, three or ten fingerprints are considered, the uniqueness becomes complete, and therefore affords for reliable identification (this is important if a fingerprint deteriorates or is permanently damaged);

(iii) are permanent and don't change by time. The only situation in which a person changes their fingerprints is when the fingerprint is severely damaged (for example when exposed to abrasives), or by finger or arm amputation;

(iv) are relatively easy to measure with the correct devices;

(v) are easily scanned, and the comparison is fast enough for more practical applications;

(vi) are a very mature technology;

vii) are widely used as the primary trait in most civil identification systems in the world; and

(vii) there is already an existing legislative framework for the taking of fingerprints.

b) Facial image:

(i) Each individual can be recognized by their face;

(ii) Although a face is a distinctive trait, it changes over time. However, coupled with the use of fingerprints, it can be safely and accurately used for identity verification;

(iii) Facial images can be easily obtained with the use of a camera;

(iv) An important feature of facial image is that it can be compared without the need for any special device or system;

(vi) Facial images are routinely used for functional identification documents (for example, passport and driver's licence).

c) Manual signature:

The manual signature forms a part of determining the identity of a person, for example, signature on official documents. The NIDS will support persons operating in the digital world (using a digital signature) and manual transactions (using a manual signature). The manual signature of a person for a basic transaction can be authenticated by examining the signature affixed to the identity document. The manual signature can also be used as a low-level authentication if the system is offline in a national disaster.

6. In this context, a NIDS will facilitate:

- Eliminating the need for enrolled individuals to provide multiple documents to establish identity to conduct business transactions, thus promoting the speed and volume of transactions completed.

- Reducing the need for enrolled individuals to register multiple times with MDAs for each service, benefit and/or obligation for example, payment of property taxes or applying for a funeral grant or PATH benefit. This will simplify government processes and reduce the cost to and time spent by, members of the public who interact with the Government.

a. Minimising the opportunities for an individual to assume multiple identities, which contributes to the proliferation of crime and illegal activities such as money laundering, tax evasion, credit card fraud and 'lotto' scamming. According to the Governor of the BOJ "a single form of identification would help the country with its Anti-Money Laundering and Countering the Financing of Terrorism, AML/CFT initiatives".[13]

b. Enroling in a National Identification System will promote economic and social inclusion by:

(i) Assisting Government to more accurately plan and provide for the total health, well-being and overall needs of the population.

(ii) Improving transparency and accountability in the use of identity information in the public sector by making government transactions easier to verify and reconstruct.

(iii) Providing persons below the age of eighteen (18) years with a free government issued form of identification.

(iv) Reducing the transactional cost associated with identity verification for individuals to access, and providers to deliver, services both in the private and public sectors. .

(v) Fostering a system of accountability as a person's consent will be required before the authentication of their data is carried out, thereby empowering them to have control over their data.

[13] Source: Nationwideradiojm.com/Jamaica-would-be-further-ahead-with-nids-boj-govenor

c. A combination of guiding principles will provide a platform for the public and private sectors to develop a wide array of innovative and productivity-enhancing services online that require 'one's identity', or an aspect of 'one's identity' for secure authentication and the improvement of privacy, transparency and security.

d. While individuals can use traditional forms of identification in face-to-face transactions, these forms of identification are less useful for conducting business on the Internet. To address this challenge, many governments[14] are creating national electronic identification (e-ID) systems with digital signatures—a collection of technologies and policies that enable individuals to electronically prove their identity, or an attribute about their identity to an information system.

e. The opportunity to create an innovation-driven approach to a national e-ID system that balances competing interests improves privacy and security for users and combines the strengths of both the public and private sectors are opportunities worth embracing.

7. Proof of legal identity is defined by the United Nations as "a credential, such as birth certificate, identity card or digital identity credential that is recognised as proof of legal identity under national law and in accordance with emerging international norms and principles".[15] Every person is therefore entitled to be able to quickly establish their identity by way of a trusted means. However, Jamaica does not currently operate a trusted, secure and universal system to support national identification.

8. The use of biometric information in identity verification guarantees that one person will have only one identity and will prove to be a more effective method of securely and accurately assigning a unique number to that person.

[14] Countries with electronic biometric identification cards include Estonia, India, Israel and Nigeria.
[15] https://unstats.un.org/legal-identity-agenda/

9. Many countries, particularly within the EU, enjoy the benefits of Government administered biometric identification card schemes that increase citizens security and deliver interoperable secure digital services.

VISION

The vision can succinctly be set out as "one person, one identity."

MISSION

To facilitate the establishment of a secure national identification system that supports reliable and robust identity verification and authentication for every enrolled citizen and person ordinarily resident in Jamaica, thereby allowing for the strengthening of identity security, cyber-security and the simplification of bureaucracy.

GOALS

1. ENROLMENT

The long-term goal is to encourage every Jamaican, and persons ordinarily resident in Jamaica, to enrol in the National Identification System.

2. DATA COLLECTION

The data to be collected will be adequate, relevant and limited to what is needed for the purposes for which the data is being processed. In order to support the National Identification System, the Government shall establish databases which will contain information on the personal identity of each enrolled citizen and persons ordinarily resident in Jamaica. This personal identity information will consist of the biometric and biographical data as prescribed.

(a) **Biometric data collection**

Biometric data will be taken from each enrolled individual over the age of six (6) years. The biometric data shall be obtained from the individual to complement the biographical data so that it is possible to identify an individual with more certainty and thereby eliminating duplicate identities.

(b) **Biographic data collection**

An individual seeking to be registered will be asked to provide biographical data as prescribed.

3. DATA SECURITY

As the identity information security of every enrolled citizen and person ordinarily resident in Jamaica is the core feature of the national identification system and processes, the Government will provide a robust and coherent legislative framework for the protection, security and privacy of the identity information of enrolled individuals stored in the databases. The legislative framework will also provide for enforcement and strong oversight.

The personal data stored in the databases shall be protected by security safeguards against risks such as loss, damage and unauthorised access, use, modification or disclosure of data.

3. DATA ACCESS

The data stored in the databases shall be used specifically for the purposes for which the data was collected and limited for use only by those persons who are so authorised. There will be no disclosure of information contained in the databases about an enrolled individual to a third party or public entity unless so specified in the governing legislation.

GUIDING PRINCIPLES

In keeping with the need for a lawful, just and fair National Identification System (NIDS), the following principles underpin the NIDS Policy:

1. Protecting the identity information of every person is a shared responsibility between the Government, citizens and residents.
2. Identity information is the property of the person, and their consent is required for its use subject to the exceptions set out in existing laws and the proposed NIDS law.
3. The types of data to be collected, the purposes for which personal data is collected and its subsequent use shall be limited to fulfilling the purposes set out in law.
4. Only the prescribed biographic and minimum biometric data will be taken.
5. The security of the identity information of every enrolled individual shall be a core feature of the National Identification System and processes.
6. The collection, storage and retention of the identity information of every enrolled individual shall adhere to the highest standard and best practices in data protection.
7. The identity data held within the databases will be verifiable, accurate and kept up to date.

STRATEGIES

The key strategies are outlined below:

1. Fundamental to the policy is the linkage between a National Identification Number and the relevant biometric data held. As biometric data is the most reliable means by which the identity of a person can be verified, only the prescribed biometric data will be collected. The biometric data to be collected from persons who enrol will be their fingerprints, facial image and manual signature.
2. Under the NIDS, for security reasons, the biometric data will be encrypted and stored separately from the biographic data. The only prescribed biographic data that will be collected is the full name, date of birth, address, marital status. This "security by design" feature is essential for minimisation of risks: even if an unauthorised individual managed to gain access to the biometric data, no biographic data could be obtained from it, and it would

not be possible to link the data to a specific person. Furthermore, biometric data will not be accessible online.

3. Data separation and reliance on templates are among the most critical security features of the system. As per industry standards, biometric systems work with a template of each biometric trait. A "fingerprint" template is not a picture of the fingerprint but a simplified, schematic version of it. This template can be used to validate a fingerprint but will not reconstruct the fingerprint. Therefore, there is no need to keep any biometric data online for the NIDS to work.
4. A protocol and a policy for access to the database and the use of the information will be designed and incorporated in the principal and subsidiary legislation. This will be modelled on international data protection standards, such as those strategies relating to the collection, processing, use and protection of personal data in the EU under the General Data Protection Regulations (GDPR), and ultimately by any data protection legislation in force in Jamaica. The Data Protection Bill is before the Parliament with a view to enactment in the near future.
5. A statutory body (the Authority) is to be established that will be responsible for civil registration, the national identification system, the enrolment of eligible persons and other related matters.
6. High-level security clearance procedures will be implemented to regulate access to the databases by the Authority's staff. Only security vetted and cleared staff will manage the NIDS databases. All access to these databases will be securely logged and the events shared with the data owners. Electronic monitoring will be implemented at all points of access to the databases.
7. Verification and authentication will be strictly regulated by the Authority.
8. The Authority will provide mechanisms for the verification and authentication of identity information as needed by enrolled individuals in their interaction with third parties. Third parties will be required to be accredited by the Authority in order to receive such validation information. It is to be noted that the verification and authentication process will not involve the disclosure of any information stored in the National Identity Databases. The accreditation process will be based on the standard due diligence processes to satisfy the bona fide nature of the third party requesting the information.

9. Data contained in the National Identity Databases will generally only be accessible for verification and authentication purposes during the lifetime of the enrolled individual. Provision will, however, be made for information about a deceased individual to be made available on the request of a third party (for example, for the purpose of the deceased's estate or by court order).

10. A person will be required to surrender their National Identification Card upon the renunciation of their citizenship, or if they are no longer ordinarily resident in Jamaica. The data contained in the NIDS databases will be accessible for verification and authentication purposes.

11. Only minimal information about an enrolled individual and the issuing authority will be exhibited on their National Identification Card. For example, the Identification Card will contain:

    (a) On the front: The National Identification Number (NIN), the card issuing authority, the cardholder's name, date of birth, photograph and signature.

    (b) On the back: Parish/Place of Enrolment, Date of Issuance, Date of Expiry, Control Number, Card Type (minor, citizen, resident);

    (c) digital certificates incorporated in the body of the card.

12. Once assigned, the National Identification Number will be linked to the enrolled individual even after death and will never be reassigned.

13. If a person's birth was never registered, then enrolment for a National Identification Number and National Identification Card will allow for a "first registration" of that individual.

14. The establishment of an oversight body to monitor compliance with and standards of performance of the Authority and other related matters.

POLICY IMPLEMENTATION

1. The implementation of a NIDS will be spearheaded by the OPM, with support from key public sector entities. The Registrar General's Department will be placed under the umbrella of the Authority and has already been placed under the auspices of the OPM to facilitate this process.

2. The following steps have been identified as part of the NIDS Implementation Plan:

A. Complete a Feasibility Study and Risk Assessment
B. Complete and promulgate the revised NIDS Policy;
C. Implement a new Public Education Programme;
D. Promulgate new NIDS Legislation;
E. Incorporate the RGD into the Authority;
F. Implement a modern Identity Management System;
G. Complete setting up of the facilities to host the Identity Management System and the centralised NIDS databases;
H. Develop competence and expertise in the use and management of the NIDS Identity Management System;
I. Complete preparations for the deployment of the NIDS Identity Management System;
J. Conduct pilot testing of the NIDS Identity Management System;
K. Implement inter-operability/inter-connectedness across the NIDS ecosystem; and
L. Effect full rollout of the NIDS.

3. Funding has already been acquired through a US $68.05m loan from the Inter-American Development Bank to strengthen enabling infrastructure and the implementation of a national identification system.

LEGISLATIVE FRAMEWORK

Effective legislation will be at the heart of the National Identification System.

The NIDS will require an appropriate legal and regulatory framework to support its establishment and operation. The creation of this framework will be underpinned by careful review and amendment of several pieces of related legislation, to provide for the acceptance and use of the NIC and the NIN alongside existing identification programmes, and lawful verification and authentication of personal, biometric and demographic information among relevant public entities.

1. The legislation will contain:
    a. The establishment of the Authority, its functions, its powers and related matters;
    b. The scheme for the enrolment of individuals and for the establishment of databases to store their information;
    c. Sanctions comprising of both fines and custodial sentences for breach of provisions of the Act or any other relevant enactment;
    d. The oversight mechanism for regulation and control of the Authority and the information in the Databases;
    e. The information which can be collected, stored and retained in the Databases;
    f. Procedures for the generation and issue of a national identification number and a national identification card;
    g. Provisions for the non-disclosure of identity information except in prescribed circumstances. This would include but not limited to disclosure pursuant to an individual's request whose information is being disclosed or pursuant to a Court Order , or in the interest of national security, or where there is a public emergency, or to facilitate an investigation under the Proceeds or Crime Act;
    h. Provisions that will ensure harmony with Data Protection legislation and other laws;
    i. Provisions for subsidiary legislation where necessary (e.g. forms, procedures, penalties); and
    j. The processes for identification, authentication and verification.

Promulgation of a National Identification and Registration Act

1. The National Identification and Registration Act will provide for the following, inter alia :

A. Registration of citizens and persons ordinarily resident in Jamaica;
B. Generation and assignment of a NIN;
C. Issue of identification cards;
D. Establishment of National Civil and Biometric Databases;
E. Security of the data stored and retained in the National Civil and Biometric Databases;
F. Protocols for restricted access to the data;
G. Data storage and management;

H. Sanctions for breach of provisions of the Act; .

I. Appropriate measures to safeguard the privacy of enrolled persons; and

J. Institutional arrangements.

2. Enrolment will be open to all citizens of Jamaica and persons ordinarily resident in Jamaica.

Amendment of Laws and Related Regulations

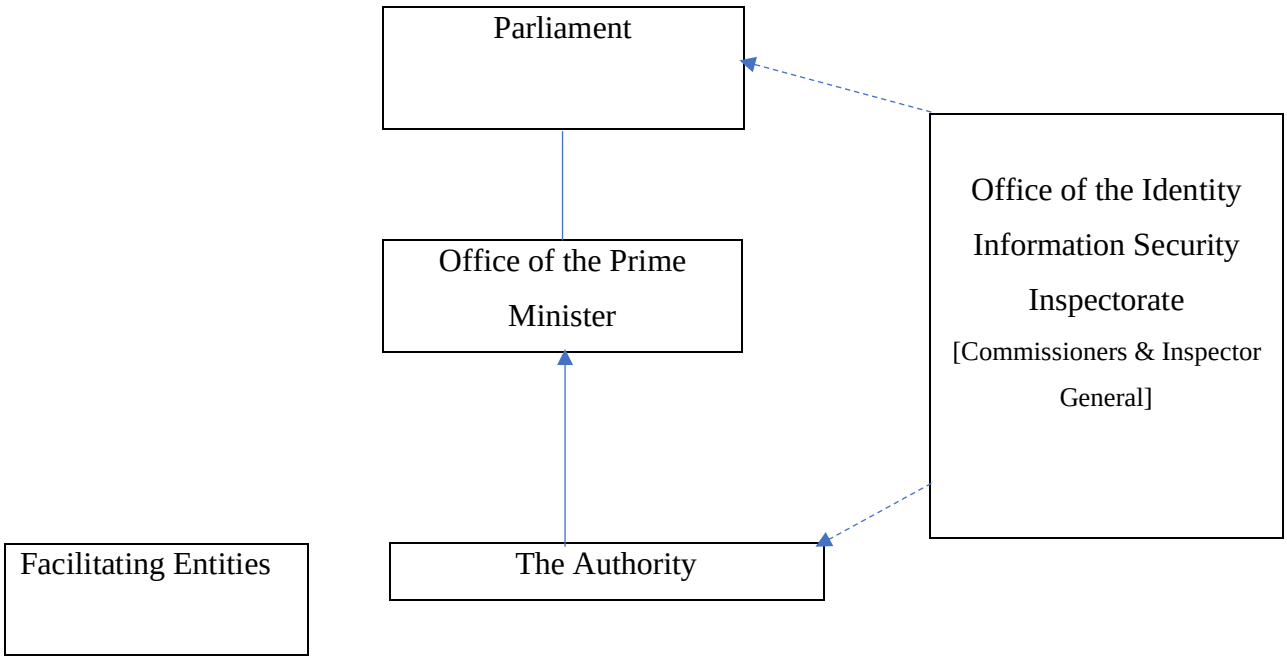
1. Implementation of the NIDS Policy will require amendments to existing laws and related regulations to provide for the acceptance and use of the national identification card and national identification number. The legislation to be amended include:
    I. The Registration (Births and Deaths) Act
    II. The Marriage Act
    III. The Forgery Act
    IV. The Passport Act
    V. The Immigration Restriction (Commonwealth Citizens) Act
    VI. The Jamaican Nationality Act
    VII. The Representation of the People Act
    VIII. The Revenue Administration Act
    IX. The Access to Information Act
    X. The Electronic Transactions Act
    XI. Cybercrimes Act
    XII. Aliens Act
    XIII. Children (Adoption of) Act
    XIV. Justice Protection Act

2. The amendments are being proposed in order to facilitate recognition and use of the NIC and the NIN alongside existing identification programmes.

Institutional Framework

1. A statutory body to be known as the Authority will have responsibility for civil registration and civil identification functions. The Authority will not only undertake all civil registration and other functions currently performed by the Registrar General but will also be responsible for the enrolment of eligible persons as well as the collection of data as prescribed by the proposed legislation.
2. The Authority will provide reports on its activities directly to the responsible Minister who will lay the reports on the Table of the Houses of Parliament.
3. An independent oversight body to be called the Office of the Identity Information Security Inspectorate (Identity Inspectorate) will be mandated to monitor the 'Authority's compliance with the NIDS law as well as the Data Protection Law when it is enacted. The Identity Inspectorate will also be empowered to take action independently or bring to the attention of the appropriate regulatory/disciplinary body where it is found that the Authority or its employees have violated the enabling legislation. In addition, the Authority will be required to comply with the Data Protection Law when it comes into force.
4. Before being appointed to the Identity Inspectorate, the Commissioners, Inspector General and employees shall undergo a security vetting.

Figure 1 below shows the governance and reporting relationships for crucial institutions supporting the implementation and operationalisation of the Authority.



Role and Responsibilities of Facilitating Entities

1. Facilitating entities are existing Ministries, Departments and Agencies (MDAs) whose resources such as physical facilities, human resources, technical expertise and specialised equipment will be leveraged to execute the NIDS business processes. This will be executed through Memoranda of Understanding (MOUs) and Service Level Agreements (SLAs) within the context of relevant legislation.

2. In varying degrees, some of these entities will also have the authority to authenticate specific NIDS data fields to verify records in their database. Capacity building of facilitating entities will be undertaken to ensure that each organisation is NIDS ready. The main facilitating MDAs identified are e-Gov Jamaica Limited, PICA, Jamaica Post, and RGD. All other MDAs will be required to accept the NIDS verification and authentication services.

Figure 2 below denotes the role and responsibilities of the Facilitating Entities

Entity	Role and responsibility
e-Gov Jamaica Limited	e-Gov host the national identification system and databases. Harmonise ICT infrastructure systems across the public sector. Drive the development and use of technology solutions in the public sector. Promote the use of e-Government services. Develop standards for the procurement of ICT hardware and software in the public sector.
Passport Immigration and Citizenship Agency	PICA will provide the information for persons who satisfy the conditions for citizenship. Implement ePassport and border control systems.
Jamaica Post	Jamaica Post will provide agreed locations in their island-wide postal network that will be used as enrolment and distribution sites as well as a designated area in their Central Sorting Office as the Production Centre of the National Identification Cards.
Registrar General's Department	Provide the authentication of birth certificates and civil registry information. Register and issue birth certificates to undocumented Jamaicans.
Ministry of Finance and the Public Service	Approval of budgets for the implementation of the National Identification programme.
Ministry of Justice	Provide legislative support
Ministry of National Security	Administer Cyber Crime Legislation
Ministry of Science, Energy and Technology	Provide legislative support for data protection, data sharing and the use of digital certificates and signatures.
All Ministries, Departments and Agencies	Review existing laws and policies that are required to drive the adoption of digital services. Implementation of digital services

FINANCING OF THE POLICY

1. The Government of Jamaica signed an investment loan on February 26, 2018, with the Inter-American Development Bank in the amount of Sixty-Eight Million and Fifty Thousand United States Dollars (US$68.05M) to finance the implementation of the policy.
2. The institutional framework design for the Authority will include a financial model conducive to the sustainability of a National Identification System.

PUBLIC EDUCATION PROGRAMME

1. A robust public education programme will be implemented to promote the tenets of the revised policy.
2. This programme will be broad-based, multi-level and tailored to meet specific communication requirements for the implementation of the NIDS. The programme will build awareness, sensitize and inform stakeholders about the NIDS. Thereafter, the programme will encourage enrolment in the system.

MONITORING AND EVALUATION

1. A monitoring and evaluation (M&E) framework will be designed and implemented to ensure the proper evaluation of the policy. The OPM will initially have overall responsibility for the development and implementation of the policy; however, on the establishment of the Office of the Identity Information Security Inspectorate, that body will assume the role of oversight while the Authority will have responsibility for execution, buildout and reporting on the framework.
2. Performance reporting will be conducted in keeping with the governing laws, policies and guidelines of the Government. An Annual Progress Report will be compiled each year by the Authority which will be tabled in Parliament. An Evaluation of the policy will be conducted five (5) years after implementation.

ISSUES FOR MAINSTREAMING

1. First, it has been noted that young people under 18 years of age are disproportionately and negatively impacted by the limited number of means (for example, only a passport) to prove their identity. This lack of identification makes it difficult for them to access social and other services.

2. Special arrangements will be developed and implemented to ensure inclusiveness of the elderly, the homeless and the physically and mentally disabled (who may need to access Government services).

LINKAGES WITH OTHER POLICIES

The implementation of a NIDS is guided by the National Development Plan- Vision 2030 Jamaica, which aims to have Jamaica developed country status by 2030. The establishment of a NIDS will contribute to the achievement of key 'Vision 2030' goals, including effective social protection, security and safety effective governance, an enabling business environment and a technological- enabled society and improved national competitiveness.

The NIDS policy, therefore, directly supports four goals and nine outcomes of the National Development Plan- Vision 2030 Jamaica, namely:

Goal 1: Jamaicans are empowered to achieve their full potential

- National Outcome #1: A Healthy and Stable Population
- National Outcome #2: World-Class Education and Training
- National Outcome #3: Effective Social Protection

Goal 2: The Jamaican Society is secure, cohesive and just

- National Outcome # 5: Security and Safety
- National Outcome # 6: Effective Governance

Goal 3: Jamaica's economy is prosperous.

- National Outcome #8: An Enabling Business Environment
- National Outcome # 11: A Technology-Enabled Society

- National Outcome # 12: Internationally Competitive Industry Structures

Goal 4: Jamaica has a healthy natural environment

- National Outcome # 15: Sustainable Urban and Rural Development

1. NIDS must exist in a complementary fashion with related policies and legislation, particularly those dealing with data protection access to information and cybersecurity.
2. While significant resources are spent on poverty reduction programmes which are facilitated under the **National Poverty Reduction Policy**, these programmes remain fragmented, and there are inadequate provisions of service and resource wastage. The NIDS will enhance the Government's ability to administer its poverty reduction and social development programmes by the accurate authentication, identification and verification of beneficiaries through a trusted integrated identity management system.
3. The **National Security Policy** cohesively integrates the country's major security policies, goal, responsibilities and action into an overall master strategy for the fulfilment of the vision for national security for Jamaica. Therefore, the integration of a biometrically verifiable identity through a trusted integrated identity management system will help to address national challenges relating to illegal immigration, border control, trafficking in persons, public safety and national security.

CONCLUSIONS

The important policy with wide-ranging implications across Government is commended to Cabinet.

A NIDS is expected to improve the efficiency in establishing and verifying identity, thereby improving business processes and service delivery, enhance the Government's ability to implement a coherent e-government strategy and support national security.

The establishment of a verifiable identity through a NIDS will more effectively support the identification of potential beneficiaries and the determination of benefit eligibility thereby ensuring a more fair and equitable administration of social benefits,

APPENDICES

Appendix I:

DEFINITION OF KEY TERMS

The following key terms are defined to provide for clarifying in respect of the policy.

a. "The National Identity System" - is the Jamaican system for capturing, storing by way of secure databases, and use of 'citizens' minimum biometric data to create reliable identity;
b. "Biographic Data"- details about an individual, who they are, where they came from and what they have done
c. "Biometric Data" – "Any representation of behavioural or biological characteristics of an individual
d. "Digital Certificate"- An attachment to an electronic message used for security purposes to verify that a user sending a message is who he or she claims to be.
e. "National Identity Number" – a unique number attributed by the Government to represent the unique identity of a citizen who applies for an identification number, secured to their biometric data;
f. "National Identity Databases" –Government-controlled databases which links each National Identity Number to the relevant biometric data;
g. "National Identity Authority" - the statutory body which will be responsible for the efficient operation of the National Identity System and the security of the National Identity Databases;
h. "Identity Inspectorate" - the independent body which will be responsible for the oversight of the National Identity Authority.
i. "Inline Transactions" - services that are offered to customers face to face at MDAs.

Appendix II -

The table depicts the Number of Passport cases detected and prosecuted for the period January 1, 2009, to October 25, 2019, from Passport, Immigration and Citizenship Agency (PICA)

Offences				
Year	**Forgery Act**	**Conspiracy to Deceive**	**Unlawful Possession**	**Total**
2009	207	14	7	228
2010	258	09	2	269
2011	202	33	Nil	235
2012	140	08	Nil	148
2013	126	20	Nil	146
2014	127	32	Nil	159
2015	129	27	Nil	156
2016	201	14	Nil	215
2017	328	06	Nil	334
2018	284	08	Nil	292
2019	310	07	Nil	317
Grand Total				**2499**

Appendix III-

The table depicts Statistics on reported cases involving Identity Theft from Counter-Terrorism and Organized Crime Branch- Ministry of National Security

Year	**No. Reports**	**Percentage**
2019	**7**	**1.7%**
2018	**16**	**3.8%**
2017	**22**	**5.3%**
2016	**20**	**4.8%**
2015	**36**	**8.6%**
2014	**52**	**12.5%**
***2013**	**70**	**16.8%**
2012	**39**	**9.4%**
2011	**37**	**8.9%**
2010	**51**	**12.2%**
2009	**46**	**11.0%**
2008	**21**	**5.0%**
Total	**417**	**100%**

About 95% of the figures in the table represent forgery of Taxpayer Registration Number (TRN)

The data represents the theft of the identity of unsuspecting individuals by imposters (i.e. family members, friends, associates, etc.) who acquired the personal and/or private information of another person in the form of their birth certificates(mainly) and use same on the applications for TRN, passport and to do other businesses.

The records were not capturing the offence as; identity theft or Possession of identity information due to the fact that the law did not recognise such offence until 2013 with the passage of the Law Reform (Fraudulent Transactions) (Special Provisions) Act, 2013. In essence, similar offences were previously being captured as forgery, uttering forged documents and other like offences.

Appendix IV -

The table depicts a total of fraudulent certificates that were confiscated from customers at the Registrar General's Department

Year	Fraudulent certificates that were confiscated from customers
2010	172
2011	154
2012	122
2013	117
2014	110
2015	126
2016	97
2017	89
2018	85
Total	**1,072**

Appendix V –

Tables depict Cybercrime Offences from the Ministry of Science, Energy and Technology

Cybercrime Reports 2016

Offences	Total	Ongoing	Disposed	Court	Convictions
Facilitating the Commission	11	0	1	10	1
Access with intent	2	2	0	0	0
Malicious Communication	19	15	1	3	0
Obscene Publication	6	6	0	0	0
Possession of Forged Device	1	0	0	1	0
Unauthorized access/Simple Larceny	387	367	4	16	0
Unauthorized Interruption	1	1	0	0	0
Unauthorized Modification	2	2	0	0	0
Unauthorized Obstruction	3	3	0	0	0
Total	**432**	**396**	**6**	**30**	**1**

Cybercrime Reports 2016

Offences	Total	Ongoing	Disposed	Court	Convictions
Facilitating the Commission	1	0	0	1	0
Malicious Communication	48	42	2	4	0
Obscene Publication	4	4	0	0	0
Unauthorized access to Computer Data	421	379	0	42	0
Total	**474**	**425**	**2**	**47**	**0**

Cybercrime Offences 2013-2017

Status	2013	2014	2015	2016	2017
Under Investigation	75	122	150	396	425
At Court	19	20	2	30	47
Disposed of	9	16	2	6	2
Total Reports	103	158	154	432	474
Disposed of	**2013**	**2014**	**2015**	**2016**	**2017**
Dismissed	2	5	0	3	0
No Order/Evidence	0	0	0	2	2
Convictions	7	11	2	1	0
Reports	**2013**	**2014**	**2015**	**2016**	**2017**
Reports	103	158	154	432	474

Appendix VI

Table depicts data regarding bank related frauds from Bank of Jamaica (BOJ)

No.	Request	Response
1	In relation to your request for data on the number of bank fraud cases due to identity theft over the past 10 years.	We should point out the following: 1. The data collected does not specify which bank fraud cases are due to identity theft. 2. The regime for receiving and analysing such information as part o the statistical data collated by the BOJ came into operational effect in 2018. As such, we are only able to provide data on the aggregate amount of bank-related frauds for 2018. In this regard, during 2018, there were 5, 139 occurrences on bank-

		related fraud.
2	In relation to the request for data on the cost of identity theft to financial institutions over the past ten (10) years.	Please note the following: 1. The data collected does not specify which bank fraud cases are due to identity theft. 2. The regime for receiving and analysing such information as part o the statistical data collated by the BOJ came into operational effect in 2018. As such, we are only able to provide data on the aggregate losses arising from all bank related frauds for 2018. In this regard, the total losses arising from the bank related fraud during 2018 amounted to JMD$620.5 million.**
**	We wish to note that losses arising from all frauds during 2018 represented a very small fraction of the capital base of DTIs, (less than 1%) indicating their capacity to absorb such losses.	
3	In relation to the query on the number of unbanked Jamaicans (persons who are unable to get a bank account because of KYC and AML requirements).	Please note that the data which ties the number of adults without a bank account and the reason for an adult not having a bank account in Jamaica is currently not available. However, according to the 2014 Global Findex, 78 per cent of Jamaicans have bank accounts.