SUBMISSION TO THE JOINT SELECT COMMITTEE OF PARLIAMENT REVIEWING THE NATIONAL IDENTIFICATION AND REGISTRATION ACT (2020)

February 2021

SUBMITTED ON BEHALF OF:

1. Jamaicans for Justice
2. SlashRoots Foundation
3. National Integrity Action
4. The Combined Disabilities Association
5. The Jamaica Computer Society
6. AccessNow
7. Open Society Foundations – Justice Initiative
8. The Jamaica Youth Advocacy Network
9. The Caribbean Vulnerable Communities Coalition
10. The Jamaica Network of Seropositives
11. JFLAG
12. Stand Up For Jamaica
13. The Jamaica Accountability Meter Portal

TABLE OF CONTENTS

INTRODUCTION AND GENERAL RECOMMENDATIONS

This submission is made on behalf of 13 organizations with a shared intention to ensure that Jamaica's National Identification System delivers a promise of social inclusion and improved access to legal identification in a manner that fully respects the human rights of all Jamaicans, preserves the security and privacy of their information, and safeguards against the dangers inherent in mass collection of personal data across interoperable systems.

As the Government has affirmed multiple times, a chief purpose of the National Identification System (NIDS) is to facilitate access to a fundamental right, the right to legal identification to which people are entitled. This core purpose should inform the manner in which the system is implemented at every level, ensuring that people's interests are placed first in both the spirit and the letter of the law.

Given the limited time between the tabling of the Bill in late December 2020, the completion of the Town Hall meetings at the end of January 2021 and the deadline for submissions in mid-February 2021, we make this *initial* submission with a focus on selected priority issues. We intend to supplement this submission with additional areas that time did not permit us to address here. We thank the Parliament for the opportunity to share our views on this important Bill.

SYSTEM DESIGN IS EVERYTHING.

A National Identification System established in a people-centred and rights-respecting manner can bring substantial benefits to the Jamaican public. Many of us are all too familiar with the inefficiencies and frustration that stem from ineffective identification options—multiple visits to government offices; numerous calls to find a Justice of the Peace to certify documents; or, in the worst cases, inability to access services when we need them.

We have studied the Bill and considered the implications of its various provisions for present and future generations. We have evaluated what circumstances the Bill could make possible now and, in the future, and have identified concerns that, if addressed, can make NIDS a considerably more balanced, people-centred, and secure system.

We make these assessments based on our interpretations of what circumstances the Bill's text could possibly allow – whether or not they are what the current state actors say are their present-day intentions – and the potential risks that future technology may create. This system and its legal framework must be able to endure changing political administrations, technological advancement, and the inevitable existence of perverse incentives of political, commercial, and other interests.

Our positions, taken together, articulate a primary set of risks that we must remain attentive to: the fact that despite the best of intentions, NIDS is a multi-use technology that, if mismanaged or improperly regulated, can result in wide-scale violations of human rights, privacy, the rule of law, and further contribute to social exclusion.

NIDS is being designed today, but it will potentially last for generations and take on new technological innovations that may outpace legal and regulatory action. We must, therefore, take great care today to put in place a set of powerful and enduring principles that provide interpretive guidance and protect the rights and institutions that we hold dear.

This is the case for many digital ID systems globally, especially those employing biometric technology and interoperability across an ever-expanding set of government and private sector services. The decisions we make now will affect how persons access legal identification, the likelihood of undue tracking, surveillance, profiling of persons using personal data, and how services are distributed for generations to come.

As seen in other societies, when these systems are not designed inclusively or without clear and effective safeguards, flaws in their implementation can have far-reaching implications, including human rights violations.[1]

With these concerns in mind, we remind lawmakers that human rights standards provide an adaptive set of guiding principles that should be integrated at every implementation phase. These principles are our barometers for a "free and democratic society" and are what place the necessary limits on the use of state power in order to preserve the greater good. They are never expendable, inconvenient, or optional. Amidst new technologies altering how we relate to each other and the state, human rights approaches help us navigate this uncertain terrain without compromising what matters.[2]

This submission first presents general observations and recommendations, which are below, followed by specific areas of concern and attendant recommendations.

GENERAL OBSERVATIONS AND RECOMMENDATIONS:

1. **Significant components of the legal framework for NIDS have been left to future regulations.** Key areas include the process of application and enrolment, how authentication will be managed, how verification will be conducted, the manner in which accredited third parties will be managed, the business processes associated with NIDS, and other components.

   While it is not controversial to relegate operational matters to subsidiary legislation, in some cases the Bill does not establish foundational clarity and direction. We recommend improvements to these specific areas in later sections. However, given the significance of the matters to be prescribed in future regulations and the far-reaching implications of NIDS as a novel system of legal identification, we recommend that:

   a) The government commit to publishing the draft regulations ahead of their consideration in Parliament and allow for public input on their contents.

---

1 Kenya and India provide relevant lessons. Earlier this year, the Kenyan High Court delayed the implementation of their ID system after it found that it was systematically excluding minority groups. In India, recent studies of their ID system have found that it has failed to improve the efficiency of the state welfare programmes (similar to our PATH programme) and has actually made them more difficult to access for the communities who rely on them the most.

2 During 2020, more than 60 civil society organizations from all over the world engaged in a consultation process to update the Principles on Identification for Sustainable Development, initially developed in 2017 by the World Bank Identification for Development initiative (ID4D) and a range of international and institutional endorsing organizations. The top recommendation voiced universally by civil society organizations, regardless of their sphere of operation or size, was that human rights must be comprehensively integrated into any standard or statute governing digital ID systems.

b) The Parliament and the wider society receive the draft regulations prior to the passage of the Act, given that the manner in which the Bill is drafted requires an understanding of the regulations to interpret the Bill properly.
c) The government publishes technical and operational documents that will guide key processes within NIDS and allow for public input. Many of the national identification systems lauded by the GOJ as references and exemplars, such as those established in Estonia and India, published multiple white papers and technical specifications to provide greater transparency and engage the private sector and civil society in dialogue.

2) **Interpretation of this Bill is incomplete without the Data Protection Act's regulations in place.** The Government of Jamaica has decided to proceed with the NIRA Bill's formulation and the implementation of NIDS ahead of the operationalization of the Data Protection Act (DPA) or even the appointment of the Office of the Information Commissioner. In the case of the NIDS, institutional reforms(such as those at the Registrar General's Department) and the procurement of systems from third parties have even preceded the Bill's passing before this Joint Select Committee.

   We believe that this is suboptimal sequencing for establishing a NIDS best positioned to achieve the policy objectives, create confidence in the population, and minimize the risks of replicating the harms caused by biometric-based identity systems in other jurisdictions. Core functions of the Authority contained in the Bill, such as the disclosure of identity information to third parties, or the manner in which it organizes and secures the databases of sensitive personal information would be shaped by the Data Protection Act's regulations. Any analysis of the Bill, therefore, cannot fully interpret the adequacy, compliance, or appropriateness of the Bill's proposed safeguards without an operational data protection framework.

3) **NIDS should not be made "de facto" mandatory** by requiring it to access basic goods and services. People should not face the prospect of social exclusion because of non-enrolment, nor should their conditions be made more difficult in order to influence their enrolment. This includes making certain services contingent on enrolment in NIDS. This Bill and subsequent regulations must be clear to not have the effect of degrading or introducing limitations on existing identification options Jamaicans have available to them today. It is important to note that this does not negate the new avenues for identity verification that NIDS will enable due to the features of the system. However, these avenues must be viewed as additive, expanding access to legal identification for all Jamaicans.

4) **Collecting biometrics endangers the individual and the system.** Biometric data is sensitive data due to its personal nature and unique association with the individual. Collecting it at national scale for multiple purpose identity verification and authentication will put every enrolled individual at increased risk. The Bill considers that biometric data can prove the uniqueness of an individual and therefore is a secure authenticator for verifying someone's identity. However, there are several considerations that undermine this argument.

a) In our increasingly digital world, data breaches are inevitable and no system is impenetrable.[3] With the expected wide adoption of NIDS, enrolled individuals will use and share their biometric data for authentication and identification purposes at an expanding list of service delivery interactions. Each additional interaction creates an opportunity for bad actors to compromise the privacy of the individual. Once a bad actor has compromised the biometric data, they will be well-positioned to assume that person's identity.
b) Generally speaking, one cannot change their biometric data. If the biometric data is used as an authenticator and this data gets leaked, the affected individual may lose the option to use this authenticator in the future without risking impersonation in NIDS and in other private services.

The United Nations High Commission for Human Rights posits, "identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights". Establishing a rudimentary national ID option that provides a path to legal identification for every Jamaican does not require the mass collection of biometric data. However, the government has chosen this approach. In the following sections of this submission, we present multiple positions and recommendations for how the proposed approach may be strengthened.

PART 1: FOUNDATION PRINCIPLES

1. INTEGRATE RESPECT FOR HUMAN RIGHTS IN THE ACT'S OBJECTS AND THE AUTHORITY'S OPERATIONS

The Government of Jamaica has the opportunity to enact ground-breaking legislation that would, for the first time, fully integrate human rights standards as a guiding reference point for implementing and operating a national digital ID system with the proposed NIRA Bill.

The integration of human rights standards establishes a normative framework that directs the manner in which NIDS is rolled out and how the legislation is interpreted both in the near and distant future. Notwithstanding the best of intentions, NIDS will be an evolving multi-use technology that, if not properly regulated, can result in wide-scale violations of human rights and social exclusion. The scope of the information collected based on the government's stated goal of integrating persons into a new "digital society"[4] creates risks unprecedented in Jamaica's history were the wrong decisions to be made.

This is true of many digital ID systems, especially one employing biometric identification technology and interoperability across an expandable range of government functions, at national scale. We must appreciate that NIDS is being designed today, but it will last for potentially generations and it will take on new technological innovations that outpace legal and regulatory action. We must therefore take

3 An example of this was the recent news on the exposure of immigration data and covid results in Jamaica. This exposure affected sensitive data of more than 1.1 million of people – see: https://techcrunch.com/2021/02/17/jamaica-immigration-travelers-data-exposed/
4 Office of the Prime Minister. "Digital Society Will Bring Economic Growth and Create Jobs – PM Holness." June 2017. https://opm.gov.jm/news/digital-society-will-bring-economic-growth-and-create-jobs-pm-holness/

great care today to put in place a set of powerful and enduring principles, enshrined in the authorizing statute for interpretive guidance, that will protect the rights and institutions that we hold dear.

Commit to human rights principles in law

In order to address these risks, the Bill should embrace a human rights framework in the provisions that establish the objects and aims of the Bill (Section 3), that set out the purpose and functions of the System, and that regulate the institutions that administer NIDS, starting with The Authority (Section 5). Presently, there are no references to the human rights and freedoms of persons within the Act, despite the fact that the human rights implications are a principal area of concern nationally.

These provisions are foundational given the serious human rights implications of the system, and the mounting human rights issues occurring globally related to these systems. It is especially necessary given the controversial history of the Bill - an earlier version being struck down by Jamaica's Constitutional Court after its passage due to unconstitutional violation of the human rights recognized in Jamaica.[5] A commitment to confirm with human rights should never be controversial.

We propose that the Bill plainly and unequivocally state that the legislation should be administered in accordance with the fundamental human rights and freedoms of all persons throughout Sections 3 and 5 where appropriate. They should establish, among the purposes of the system, the promotion and protection of fundamental rights and freedoms, including the right to access legal identification.[6]

These provisions should acknowledge that harms may arise and provide for the kind of transparency and redress that would benefit an endeavour that is truly undertaken to promote the good of all persons in the country.

Affirm access to the right to legal identification as a core purpose of NIDS

A principal purpose of NIDS is to expand access to reliable legal identification in Jamaica. This is an important aim that can bring tremendous benefits to hundreds of thousands of people. Yet, it is not stated in the Bill as an object of the Bill or a function of the Authority.

The Government's White Paper tabling the NIDS Policy in Parliament explains that many Jamaicans "lack basic legal identity documents" and therefore face social exclusion.[7] The NIDS Policy (2016) itself opens with the statement "Identity as a Human Right" and states that "the right to a legal identity is therefore a fundamental human right, where the State is obliged to enable each person to exercise his or her right to a name."[8] Though a national ID Card is not the same as having a legal identity, it is clear that the government's stated goal is to facilitate access to a fundamental right to which people are entitled.

It is strange that the Bill mentions this nowhere, despite the fact that it is the very first reason given for creating NIDS in the original Policy document. The current objects of the Act include many varied goals, including to "prevent identity theft and other instances of fraud". We believe that this rights-based language can be integrated into the objects of the Bill.

---

5 See Supreme Court of Jamaica decision "Julian Robinson vs The Attorney General" (2019)
6 See NIDS Policy 2016. Government of Jamaica
7 Government of Jamaica. White Paper Tabling the National Identification Policy. November 4, 2016. p. 2
8 Office of the Prime Minister. National Identification System Policy. October 2016. p. 1

Clearly establishing that facilitating the human right to access legal identification is a purpose of NIDS will help ensure that the manner in which its operations are organized puts people first. The other goals of the system (such as making business easier for banks and generating statistics) are complementary, if not secondary, to this fundamental purpose of providing the Jamaican people with safe, reliable identification.

IN SUMMARY, WE RECOMMEND THE FOLLOWING:

1. Amend Section 3 (The Objects of the Act) to include explicit reference to *promoting and protecting the human rights and fundamental freedoms of all persons in a free and democratic society* whether as a new object or by integrating it within an existing subsection.
2. Amend Section 3 (The Objects of the Act) to include as an object: *to facilitate access to legal identification.*
3. Amend Section 5(3) and (4) (the functions and powers of the Authority) to include observation of the human rights and fundamental freedoms of all persons, including any specific laws and policies established to give effect to them.

2. DISTINGUISH BETWEEN IDENTITY INFORMATION AND OTHER INFORMATION NOT NECESSARY FOR ESTABLISHING LEGAL IDENTITY AND MAKE NON-ESSENTIAL INFORMATION OPTIONAL

The Bill sets out a new national definition for what is considered "identity information". Moving forward this definition will likely become a point of reference for future laws and policies. In Section 2, it defines identity information as "the biographic, biometric or numerical information that may be collected under section 11 in respect of an individual." According to Section 11, these are:

Biographic Information:

i. full name (including any names used prior to a change of name by deed poll or marriage);
ii. date of birth;
iii. country of birth;
iv. place of birth;
v. names of mother and father;
vi. whether the individual is male or female;
vii. principal place of residence and any other places of residence;
viii. nationality, in the case of an individual who is not a citizen of Jamaica;
ix. period of residence in Jamaica, in the case of an individual who is not a citizen of Jamaica;
x. marital status;
xi. name of spouse (if applicable)
xii. occupation

Biometric Information:

i. facial image;
ii. fingerprints, as defined by the Finger Prints Act;
iii. manual signature, in the case of an individual who is eighteen years of age or older

Reference Numbers:

i. taxpayer registration number;
ii. driver's licence number;
iii. passport number;
iv. National Insurance number;
v. Programme of Advancement Through Health and
vi. Education (PATH) number; and elector registration number.

Section 11 also enables the Authority to require all the above information in order to enrol a person, and would allow them to deny an enrolment (and therefore access to legal identification) where certain information was not provided. It is our opinion that **only information that is directly related to establishing legal identity should be mandatory for enrolment.** Most of the information the Authority is empowered to require for enrolment is not, and therefore must be optional for enrolment. This would align with the government's 2020 NIDS policy which announced that only four attributes would be prescribed.[9]

We remind that for many Jamaicans, their enrolment in NIDS will be the only way to secure their right to access legal identification. As stated in Position 1, a chief purpose of the system is to expand access to reliable legal identification among Jamaicans. The Government's White Paper on NIDS, the NIDS Policy, and many official statements, make it clear that the government's stated goal is to facilitate access to a fundamental right to which people are entitled.[10] It is not a privilege or a favour.

Consequently, the method chosen for enrolment must erect as few barriers as possible to persons who volunteer, and should not be unduly intrusive. Any conditions for enrolment must be compelling and closely connected to a legitimate aim. We outline two revisions to the current approach:

1. Minimize what information is required for a person to enrol in NIDS and therefore necessary for obtaining legal identification.
2. Collect additional information optionally as part of opt-in value-added services.

Explicitly minimize what is mandatory for enrolment.

This Bill was drafted to give effect to the National Identification and Registration Policy (April 2020), which is the government's formal policy directive on NIDS and captures the nature of its stated commitments when establishing the system. The policy was re-designed following the Supreme Court decision striking down the previous Act due to human rights violations. The policy outlines the following approach to identity information.

> *"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."*
>
> *- Excerpt from National Identification And Registration Policy For Jamaica. April 2020. p.17*

The information proposed in Section 11 significantly expands the scope of identification information, specifically the biographical data, that the Authority can require for enrolment based on the

9 See "National Identification and Registration Policy for Jamaica." 2020. P. 17

10 The Government's White Paper tabling the NIDS Policy in Parliament explains that many Jamaaicans "lack basic legal identity documents" and therefore face social exclusion.# The NIDS Policy (2016) itself opens with the statement "Identity as a Human Right" and states that "the right to a legal identity is therefore a fundamental human right, where the State is obliged to enable each person to exercise his or her right to a name."#

Government's National Identification and Registration Policy.[11] It is unclear whether something changed in the drafting instructions between April 2020 when this policy established just four items of information, and December 2020 when drafting of the Bill was completed. The current approach, which empowers the Authority to potentially require all the aforementioned information in order to facilitate access to legal identification would contravene the guiding principles articulated in the 2020 policy which states:

- "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." and
- "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."

A foundational tenet of data privacy agreed globally is the principle of data minimization. Data minimization requires that entities collect, process, and retain only adequate, relevant and limited personal data that is 'necessary' for a specific purpose. Jamaica has adopted this principle in our Data Protection Act under Standard Three.[12]

In examining the Bill's revised identity information list, only a few of these attributes constitute a person's identity, and some of them may create risks if made mandatory for enrolment. Most of the included attributes are information about a person which may enable value-added services (such as meeting "Know Your Customer" requirements within the financial sector) and which are subject to change. However, this additional data **is not identity information** – even if it is helpful to capture for specific sector use cases – and **should be optional for enrolment and authentication** because they are not required to establish a person's legal identity.

Making this distinction does not affect the ability of NIDS to capture this information from persons who voluntarily provide it. However, it should not be possible to deny any person legal identification from the State because they declined to share information that is irrelevant to establishing who they are, such as their occupation, spouse's name or an occasional place of residence. The system can optionally *include* this extra information without *excluding* persons who elect not to share it.

Simply put, persons should be able to obtain legal identification without disclosing their occupation (they may be unemployed and not want to share that, or work in a controversial field and not want to be permanently identified by it), or their additional places of residence, or whether they have been married anywhere in the world and the name of that person.

The personal and social experiences that may make such disclosure unwelcome for certain persons is significant. It is also **unnecessary** for the central goal of the system, which we remind, ought to be "limited to fulfilling the purposes set out in law." Not only are these and other extra information unnecessary for establishing who a person is, but they are constantly changing. We understand that the main function for collecting these attributes is to support value added services. In the following section, we recommend an approach to collecting this information for those who opt-in.

11 National Identification And Registration Policy For Jamaica. April 2020
12The Data Protection Act, 2020

Accordingly, we also propose that the only information that should be required for enrolment to access to legal identification should be:

BIOGRAPHICAL INFORMATION:

- Full name
- Date of birth
- Sex
- Nationality (for non-Jamaicans)

BIOMETRIC INFORMATION:

- Facial image
- Manual signature
- Fingerprints (we do not concede that these are required to establish legal identity, but include them given they have become the basis for how NIDS is organized)

Collect additional information optionally as part of opt-in value-added services

We recognize that the Government intends for NIDS to enable expanded access to various services (e.g. financial inclusion) that could accelerate development and provide greater ease of doing business in Jamaica. Information such as a verified address is often critical for multiple services and transactions. We believe that there is a strong case for the NIRA to provide value-added verification services, such as address verification, to citizens who voluntarily opt-in to participate.

This approach has multiple advantages. It clarifies the intended purposes for which the data is collected and the benefits its collection will provide, and it better aligns with the characteristics of the non-essential information, which frequently change over time (e.g. occupation, addresses). Identity information, which is core to "who" the individual is, remains distinct from other information about that individual. Lastly, decoupling identity verification in this way increases the scalability of the enrolment process. Information verification activities performed on non-essential information such as address verification will likely require more human and financial resources and time-consuming verification checks than the core identity information.

The Bill itself recognizes that all Section 11(1) 's identity information is unnecessary for enrolment. Section 11(2) expressly gives the Authority broad discretion to enrol persons who are unable to supply "any one or more items of identity information listed in subsection (1)" that is requested. The Bill leaves it to the Authority to make this decision, recognizing plainly that the State is still fully capable of granting someone their entitlement without everything required under Section 11.

This recognition is a positive feature of the Bill. However, the matter should not turn exclusively on what the Authority believes in its discretion. The Bill should clearly and consistently establish what information is **necessary** for enrolment in NIDS and what additional information enables value-added identity services. This would avoid any doubt or the potential to deny legal identification to a person whose identity can be established simply because they did not provide some additional non-essential data.

In making this point, it is essential to note that this does not affect the Authority's ability to request documents or other material to satisfy itself that a person is who they say they are under Section 12. As such, no risk to the credibility of enrolment under Section 11 occurs from this change.

ACCORDINGLY, WE RECOMMEND THAT:

1. Sections 10 and 11 be amended to indicate which information is strictly necessary for enrolment and which information is optional. We recommend that the only mandatory identity information required for enrolment be name, date of birth, sex, nationality (for non-citizens), facial image, manual signature and fingerprints. The Authority retains the ability to collect the other information, but not the ability to prevent enrolment on the basis that they were not provided.
2. The Bill explicitly establishes in Section 11(2) that where a person provides sufficient information to establish identity, that the Authority shall enrol them.
3. The Authority explores value-added verification services distinct from the information necessary for providing individuals with a legal identification through NIDS.

3. REQUIRE THE FULL OPERATION OF THE DATA PROTECTION ACT PRIOR TO BRINGING THE ACT INTO FORCE

Establishing a National Identification System will be the most significant data collection enterprise that Jamaica has embarked on. We believe an effective and fully operational data protection framework is critical to engendering confidence in the NIRA and achieving its policy objectives. One of the pillars of this framework is the Data Protection Act (2020). Therefore, we are requesting that the GOJ commit to the full operationalization of the Data Protection Act (DPA) prior to bringing the NIRA Act into force. We interpret the operationalization of the Data Protection Act as including:

- The Government bringing the Act into force by Gazetting an appointed day of the Act's commencement in a manner that makes all its provisions applicable.
- Establishing the Office of the Information Commissioner necessary to implement the Act and adequately resourcing it
- Instituting necessary regulations to the Data Protection Act that outline how the data protection framework will operate in practice. These regulations are the way that the general standards articulated in the Act become operational and tangible

The current NIRA Bill also acknowledges the centrality of the Data Protection Act as a guiding framework for NIRA's implementation. Section 5(3)(d), Section (6)(1)(B) and Section 27(5) affirm that the Authority must operate in compliance with the Data Protection Act, the Board of Management are responsible for providing oversight of this compliance, and also that the NIRA perform quarterly reporting functions to the Information Commissioner.

Moreover, Minister of Justice Delroy Chuck, Chairman of the Joint Select Committee reviewing this Bill, acknowledged in the January 27 Town Hall meeting that due to the "conformity" requirements of the NIRA Bill with the Data Protection Act, it, therefore, follows that NIDS cannot be operationalized until the Data Protection Act is in operation and applicable in a meaningful way.

We welcome this acknowledgement and look forward to the Government implementing both laws in the appropriate sequencing.

Furthermore, given that the Data Protection Act includes a two-year adjustment period for Data Custodians to comply with the Schedules in the Act and related regulations, the Government must clarify how the NIRA will operate in the intervening period. Addressing this accountability gap requires law reform either in the NIRA Bill or the Data Protection Act. Specifically, either law can be modified

to include provisions that states that the two-year adjustment period currently included in the Data Protection Act is not applicable to the Authority and brings into force all data protection provisions the moment that the Authority commences operations.

ACCORDINGLY, WE RECOMMEND THAT:

1. The Government of Jamaica formally and publicly commit to the sequencing of operationalization of the Data Protection Act ahead of this NIRA Bill. Operationalization of the Data Protection Act ought to include:
   a) Bringing the Act into force by Gazetting an appointed day of the Act's commencement in a manner that makes all its provisions applicable.
   b) Establishing the Office of the Information Commissioner necessary to implement the Act and adequately resourcing it.
   c) Instituting necessary regulations to the Data Protection Act that outline how the data protection framework will operate in practice. These regulations are the way that the general standards articulated in the Act become operational and tangible
2. Section 1 of the NIRA Bill be amended to require that the effective date of the Act's commencement be a date after the date on which the Data Protection Act has come into force. This prevents the Bill from being brought into force without the promised data protection provisions being enforceable law.
3. Provisions be introduced (whether to this Bill or the Data Protection Act) that remove the two-year period of exemption from the provisions of the Data Protection Act for the Authority. The law should ensure that all data protection provisions are fully enforceable on the Authority the moment it commences operations under this Bill.

PART 2: DISCLOSURE OF INFORMATION, AUTHENTICATION AND VERIFICATION

4. STRENGTHEN PARAMETERS AND SAFEGUARDS FOR DISCLOSURES OF INFORMATION TO THIRD PARTIES

The prospect of improper disclosure of sensitive personal information is one of the most significant risks to be managed by any system that collects the breadth and volume of personal data that is proposed to be undertaken by the Authority. At every point where information about an individual is shared a risk is created that must be managed. The severity of this risk grows with the scope of the information being shared. This is why it is imperative that beyond allowing for information exchanges, the Bill must provide clarity on how information exchanges can (and cannot) occur.

The act of disclosure is the only circumstance under law in which the Authority wilfully exposes information that is otherwise shielded from access. As such, the robustness of the process for managing disclosure is a paramount concern for privacy, security, and accountability. Section 24 of the Bill seeks to establish that system.

Section 24 states that the Authority should generally not disclose a person's identity information. It does **not** restrict the disclosure of other information that may be held by the Authority (such as transactional data, authentication logs/requests, etc.). Section 24 then outlines three broad circumstances in which the Authority can disclose a person's identity information:

1. Where an enrolled individual requests that disclosure and pays any applicable fee (Under Section 24(1)(a))
2. Where the police request it and the Court grants permission (Under Section 24(1)(b) and Section 24(2))
3. In any other circumstance enabled under the Act any other law (Under Section 24(1)(c))

While Section 24 establishes an important basis for protecting individuals' privacy and security, many areas need substantial improvement. We highlight three such areas, summarized below and further explained in detail subsequently.

First, Section 24 lacks sufficient provisions explaining what disclosure looks like in practice. This is not an operational matter for future regulation. It is a principal duty of the current Bill to define and clarify *how* disclosure can occur. For example, will the Authority be able to transfer a computer file with someone's biometrics as a form of disclosure? The Bill's silence on this issue presents considerable security and privacy risk. We believe that clear parameters are needed that establish the forms that disclosure can and cannot take, among other things.

Second, the open-ended power created by Section 24(1)(c) to disclose to any third party based on "any other law" without a transparent process or oversight is concerning. We recommend reforming that section to establish oversight of the decision. Just as applies to the police, disclosures that an individual did not request should only occur with the Court's approval.

Third, despite the Authority maintaining various types of information about an individual, Section 24 only prevents disclosure of "identity information." This creates a risk for disclosure of other information such as authentication records/logs, verification requests, and transactional data not being expressly prevented by law. This may have been an oversight. Accordingly, we recommend amending Section 24 to apply to "all information" not only identity information.

It may be suggested that the Data Protection Act (DPA) addresses these issues. It does not. While it provides essential and complementary safeguards, it does not solve the unique challenges created by Section 24. It contains no processes to manage disclosure and does not require judicial oversight to disclose identity information. Without the DPA's regulations outlining its operationalization it is largely a collection of general standards to inform data management. In fact, it calls upon the data custodian - in this case, the Authority - to establish systems to address these things. It is in this Bill that those obligations ought to be established.

Define what forms disclosure may take and outline how it should be managed

The Bill contains no provisions explaining what forms disclosure may take or the process by which it will occur in a material sense. Will the Authority transfer actual records from the database to third parties when "disclosing" information? That would be possible under Section 24. Can it share a computer file with someone's full biographic and biometric data? A file can be copied and transferred indefinitely once received. Will records be decrypted to facilitate disclosure even though the Bill

requires that all information be kept illegible and encrypted? How will the Authority manage third parties when they receive an enrolled individual's identity information?

These are foundational questions for which no answers can be located within the Bill. It does not contemplate the nature or risks of disclosure, but merely establishes legal Authority to disclose.

We believe that the law should establish clear parameters for the method of disclosure. These parameters can explain *how* disclosure can lawfully occur - the actual forms it can and cannot take; how the process can and cannot be managed - and how recipients of disclosed information are managed.

In doing so, the law should establish safeguards on the use, processing, and storage of information by third parties to whom information has been disclosed under subsections (1)(a) and(1)(c). Unlike under Section 24(1)(b) and (2) where disclosures to the police include guiding provisions, no similar provisions inform when and how the data, once processed, should be deleted by third parties the Authority has disclosed the information to under 1(a) and 1(c). The law, as presently worded, allows them to retain and use that information indefinitely and without much restriction beyond general data protection provisions.

We cannot fully assess the nature of the risks involved in this disclosure if the Bill does not envision what they look like in tangible terms, nor can we evaluate the sufficiency of systems designed to manage those risks. Unless greater clarity is provided, how can the law serve as a regulating instrument if it neither gives form nor establishes limits for what it authorizes?

Establish oversight of disclosure of information to other parties under "any other law"

What happens when another party, whether government or private, seeks disclosure under Section 24(1)(c) on the basis that it is "provided by this Act or any other law"? How will that process be managed? What standards will be applied? Will the Authority use its sole discretion to decide? Will an enrolled person be notified? Can they contest?

Unlike under Section 24(1)(c), where a Court must evaluate an application from the police for disclosure of a person's identity information and apply a legal test, Section 24(1)(a) provides broad room for the Authority to disclose, without any judicial oversight.

Oversight from the Court would only be required if some other Act requires it. This is concerning, given that disclosures under Section 24(1)(c) are most likely not consented to by the enrolled individual since those requests are managed under Section 24(1)(b). It is concerning that the Bill would allow the Authority such broad discretion to disclose a person's identity information without an order from the Court and with no clear oversight of the disclosure process.

It is peculiar given the fact that if the police request a person's information under subsection (1)(b), the request must be approved by the Court, but if they (the police) or any other body (including the Authority itself) sought to have the same information disclosed under subsection (1)(c), then no judicial oversight is required. In fact, no process at all is even contemplated by the law.

We recommend that Section 24 be amended to require that any disclosure of an enrolled individual's information that the individual did not request only occur when ordered by the Court.

Disclosure of other information about an individual held by the Authority

The Bill does not restrict the Authority from disclosing other information about an individual held by the Authority, such as records/logs of authentication, verification requests, and transactional data. Instead of prohibiting disclosure of "information" related to an enrolled individual, it only prohibits disclosing "identity information". It is important to note that disclosure or processing of the information above could significantly harm that individual and undermine their right to privacy. As presently worded, the Authority may be able to disclose any of the other information it possesses in unknown ways. (See Position #6 of this submission on the authentication and verification process (p. 17) for recommendations on managing authentication records/logs.)

This clause, as worded, does not align with the GOJ and the NIDS project team's statements and commitments on the central importance of privacy in the conceptualization and implementation of Jamaica's NIDS. Therefore, we are recommending that Section 24 be amended to refer to "any information" not only "identity information." This clarifies that the prohibition on disclosure is not limited to just a person's identity information but extends to all information held by the Authority about them.

IN SUMMARY, WE RECOMMEND THAT:

1 Section 24 create clear parameters for the method of disclosure. These parameters can explain how disclosure can lawfully occur - the actual forms it can and cannot take; how the process can and cannot be managed - and how recipients of disclosed information are managed.
2 Section 24 establish safeguards on the use, processing, and storage of information by third parties to whom information has been disclosed, including the police.
3 Section 24(1)(c) be amended to require that any disclosure of a person's information that that individual did not request only occur when ordered by the Court.
4 Section 24 is amended to reference "any information" not only "identity information" to clarify that the prohibition on disclosure is not limited to just a person's identity information but extends to all information held by the Authority about them.

5. IMPROVE TRANSPARENCY OF THE DISCLOSURE PROCESSES

As described above, section 24 permits the Authority to directly disclose information about a person to multiple third parties under various circumstances with or without their consent. We are therefore making recommendations concerning the need for greater transparency in the disclosure of information under Sections 24.

The Right to Know About Disclosures of Your Information

The Bill permits disclosure of personal information under Section 24 but does not grant the enrolled individual any right to know what disclosures have taken place, when, and to whom - even in circumstances where they requested the disclosure themselves. This runs contrary to persons' data rights outlined in the Data Protection Act and to other provisions in the Bill that grant persons the right to know about requests for verification of their information under Section 25. We believe this should change.

An enrolled individual still possesses agency over their data. Unless a competing interest prevents it (determined by a Court), a person ought to have an explicit, guaranteed right to know how, when, and to whom the Authority disclosed their information. Recall that the enrolled individual's information is voluntarily given based on a promise of utmost confidentiality.

This right to know about disclosures ought to exist in all circumstances of disclosure - both consented and unconsented - unless a Court determines that a competing interest justifies keeping the disclosure secret. This establishes a presumption of transparency based on the inherent data rights of the individual.

The Data Protection Act gives every person a general right to know how their information is being processed and to whom it is being disclosed. To achieve harmony with that Act, the Bill should specifically affirm that persons may access this information through a procedure which may be specified (whether in the Act or in future Regulations) and which shall be free of cost. Without adequate, timely information regarding how data is accessed and processed, data rights and data protection don't work. This includes rights concerning disclosures and other forms of data processing.

Below are some specific reasons why this reform matters.

First, under Section 24(1)(a), persons may consent to the Authority disclosing their information to third parties such as service providers. An individual should be able to verify what information was actually disclosed and when. Knowing what information the Authority has disclosed is rationally connected to how an enrolled individual conducts affairs/business with entities to whom they have given consent. It also helps ensure that persons possess credible information relating to any entity's access to their information through the Authority.

Second, knowing what information the Authority disclosed will also allow individuals to determine if their information was disclosed to parties to whom they have not given consent. Fraud, identity theft, or misrepresentation may have occurred, resulting in the Authority improperly disclosing information to any number of entities. Mistakes may also occur. One way that persons will be able to protect themselves and identify data breaches is by knowing what the Authority is disclosing. During the JSC Town Halls, the NIDS project team indicated that this is, in part, the intent for how disclosure will be operationalized. However, we believe that this must be captured in the primary statute and recognized as the enrolled individual's right.

Third, a person ought to have the ability to challenge an unconsented disclosure. At present, a person is not entitled to even know when their information is disclosed, whether to the police under Section 24(1)(b) or some other entity "under any other law" as is permitted under Section 24(1)(c).

As it relates to applications by the police under (1)(b), the entire application for disclosure is effectively conducted in secret, with no ability for the enrolled individual to participate in proceedings or contest. Regarding disclosures to other entities under "any other" present or future law, the scope of this is entirely unknown. We address this issue substantively under Position 3, but establishing a right to know what information has been or is being proposed to be disclosed allows a person the ability to challenge decisions that may adversely affect their interests. Again, the Court should be able to determine if such information should be kept secret. But in the absence of such a determination, we believe the information should be accessible by default.

Fourth, we remind that the Data Protection Act establishes this right of access in Section 6 and throughout the Act. It also requires that such right of access be granted by data controllers free of charge. Therefore, we believe it is obligatory that this Bill establish a procedure to access that information, just as it has done in Section 25 to access information about verification requests.

Transparency Reporting

With respect to disclosures contemplated under Sections 24, greater transparency concerning the processes and outcomes will ensure accountability and enhance public trust and, therefore, overall inclusivity and functioning of the system over the long term. The Act should contemplate the release of information to individuals whose data is disclosed and facilitate the broader oversight and accountability functions served by sharing aggregate information on disclosures during the system's operation overall. This information on disclosures in practice can be safely anonymized, disaggregated and shared with the public toward these ends.

IN SUMMARY, WE RECOMMEND THE FOLLOWING:

1. Amend Section 24 to establish a right to know when, how, and to whom the Authority disclosed a person's information (regardless of under which circumstance) unless the Court limits such disclosure based on a compelling interest. This right of access should be free of charge.
2. Amend Section 24 to require notification of a request for disclosure of a person's information prior to making such disclosure and allow a reasonable period of response unless the Court limits such disclosure based on a compelling interest.
3. Require a quarterly transparency report related to all disclosures of information that presents aggregate statistics on all disclosures, indicating the category of entities involved (police, private sector, government agencies, etc.), how disclosures were managed (how many requests were honoured, not honoured, disputed, in process, etc.), the circumstances of the disclosure (requested by an individual, ordered by a Court, etc.

6. CLARIFY PARAMETERS FOR THE AUTHENTICATION AND VERIFICATION PROCESSES AND ESTABLISH ROBUST SAFEGUARDS TO MINIMIZE RISKS

Authentication is a critical feature of the entire NIDS architecture. It is the point at which, as part of a transaction or service interaction, the enrolled individual uses NIDS to "prove" their identity to a third party. This may be initiated by the enrolled individual or by a third party and creates data regarding the activities of an enrolled individual in each instance.

Importantly, it is expected that the functionalities for authentication and verification services will become increasingly digitized given the stated ambitions for NIDS to be a "digital Identification system" capable of facilitating online transactions, e-governance, and a new "digital society."[13] This approach assumes the perpetual generation of usage data (also called transactional data or metadata) related to any of the individual's activities using their National ID Card or Number.

13 Add reference

Currently, Section 25 states that authentication and identity verification services may be provided but does not explain in much detail how they are to unfold. Without better knowledge of how authentication and verification services will be managed, it is difficult to fully assess the sufficiency of the Bill's existing provisions.

Based on the circumstances that the current and emerging technology create, it is critical to establish significantly stronger safeguards against the risks inherent in the use of authentication and verification systems. We identify key areas in which the Bill can be strengthened below.

Managing risks from authentication records/logs

We are concerned about the lack of specifications informing the management of authentication and verification records/logs of enrolled individuals in the Identification databases.

The National ID Card is intended to be used to do transactions across society. As Section 17(1)(b) states, the Card may be used "as a means of facilitating transactions between that individual and any other party." Based on government pronouncements, the Card will be a "digital ID," optimized to perform transactions both online and in-person using authentication technology.[14] This technology will grow in the future, and once established, the Authority will be able to maintain a permanent log of each time a person's National ID Card is authenticated as part of a transaction, even if the transaction was with a private entity. This creates a risk never yet contended with in Jamaica.

As NIDS expands and future technologies take come into existence, it is possible that an individual's authentication and verification records/logs could detail all the service providers at which their National ID was used to verify their identity and each time their National ID Card was authenticated digitally. This could capture an expanding record of visits to banks, government agencies, health facilities, and other private entities, all transactions that involve authenticating a National ID Card (such as financial transactions), the receipt of social benefits, such as PATH, and use of online services using their National ID Card.

In the future, with sufficiently broad adoption of NIDS and increased digitization of society, these records could enable near real-time monitoring of each enrolled individual's actions involving the use of the ID card.

Currently, the Bill is silent on how these records/logs will be managed. It does not regulate **what data these records/logs will capture** (will it record when, where, with whom, and why authentication or verification occurred?), **how authentication and verification records/logs will be stored** (for example, the Bill only specifies that "identity information" must be encrypted, and the policy framework directs that biographic and biometric data be segregated with biometric data being kept offline[15]), **how these records can (and cannot) be processed and analysed**, or **whether they can be shared with others** (the Bill does not prevent their disclosure under Section 24, which only prevents disclosure of "identity information.")

14 The National Identification and Registration Policy (2020) describes different components of this technology. One example is including optimizing the National ID Card to deploy "digital certificates, biometrics as digital credentials, cardholder consent and full onboarding for digital services." (pg. 10)

15 See both Section 9(4) of the Bill page 17 of the National Identification and Registration Policy (2020)

The truth is that were this data to ever be misused, the public could face unprecedented risks of social profiling, algorithmic prejudice, and forms of digital surveillance based on patterns in the authentication and verification history. It is therefore critical that the Bill explicitly describe how these records/logs will be managed and place appropriate limitations on how the data's processing[16] and disclosure in a manner that considers future realities.

We strongly recommend that the processing of this information without the individual's consent must be strictly prohibited, as should disclosure under Section 24. Furthermore, the Bill must include explicit language that prohibits individual records processing beyond that required to provide the enrolled individual access to this data. Aggregate and anonymized processing of authentication records must also be strictly prohibited. Furthermore, the NIRA Bill should affirm that this transactional data belongs to the enrolled individual. The enrolled individual should also have agency over retention of this data, rather than the authority, as suggested in Section 24(4). Furthermore, the authentication and verification records/logs should be stored separately from the identity information. It should be impossible to aggregate and process them together.

Given potential privacy and social profiling risk, Parliament should seek clarity on the specifics of the records that the Authority is intended to retain on the enrolled individual and the default length of time for which this information will be kept.

Clarity regarding identity verification is needed in the Bill

First, the Bill includes two types of identity verification processes. Identity verification takes place during the enrolment process (Section 12) and is focused on verifying the veracity of identity of the individual seeking enrolment in the NIDS. The "verification" definition included in Section 2 relates only to this type of verification activity. However, the Bill empowers the Authority to perform a second type of verification activity in Section 25, which is not captured in the definition mentioned above. Further, section 25 does not meaningfully explain the form that this will take.

The Bill also does not stipulate the nature of the information shared with "accredited third parties" as part of identity verification. It states in Section 25(4) that the disclosure of identity information is not included, but without additional specifics it is difficult to evaluate the nature of risks or appropriateness of safeguards included.

We believe that the law should establish clear parameters for the method in which identity verification will occur and the way any information will be disclosed as a result. These parameters can explain *how* the verification services can lawfully be implemented - the actual forms it can and cannot take; how the process can and cannot managed. This law should set parameters.

We remind that at every point where information relating to an individual is shared (not only their identity information) a risk is created that must be managed. The severity of this risk grows with the scope of the information being transmitted. Therefore, the Bill must clarify how information exchanges can (and cannot) occur, not just state that they will.

16 Here we use "processing" as defined in the Data Protection Act, 2020. Processing therefore means "obtaining, recording or storing the information or personal data, or carrying out any operation or set of operations (whether or not by automated means) on the information or data..."

Establish provisions for the management of Accredited Third Parties

The Bill introduces the term "Accredited Third Parties" in Section 25(1)(B). However, it does not define the term or include guidance concerning how these entities should be governed. While Section 25(3) states that a person may apply to be an accredited third party, it is not clear on the limitations of this type of entity. For example, do accredited third parties only include businesses and individuals, or do they also include digital services (applications) created by either of the entities mentioned earlier? We propose that a definition of the entity and a minimum set of governing principles be included in the primary statute.

Improve data access consent & disclosure

The Bill should include guiding principles for consent provided by an enrolled individual to enable identity verification and authentication to accredited third parties (Section 25). We propose that all information disclosures under Section 25 be narrowly construed to be limited in duration and purpose. This aligns with data protection best practices. A specific obligation should be included in the Bill compelling the Authority to create processes that enforce consent parameters and prevent accredited third parties from making such requests.

IN SUMMARY, WE MAKE THE FOLLOWING RECOMMENDATIONS:

1. Establish (likely under Section 25) that the only lawful purpose for which the authentication and verification services can be used (including its records/logs) is the establishment of a person's identity. Generally, authentication and verification records/logs should not be processed, analysed, or shared. These provisions should strictly prohibit the processing of authentication and verification records/logs beyond that which may, in limited circumstances, be strictly necessary to provide an enrolled individual with access to their own information if required. No other form of processing should be legally permitted, and no other function pursued.
2. Introduce provisions that require that the Authority to implement privacy and security provisions equal to those applicable to "identity information" for all records/logs of authentication and verification. For example, currently the law only requires encryption of "identity information" under Section 9(4).
3. Explicitly prohibit the Authority from aggregate and/or anonymous processing of the authentication and verification records/logs.
4. Explicitly prohibit the Authority or any other entity from taking any action whose effect could enable the use of the authentication and verification services under NIDS (including its records/logs) to create profiles of persons or monitor/track their activities.
5. Amend Section 25 to include language that affirms that the authentication and verification records/logs are the personal data of that enrolled individual.
6. Expand the definition of verification to include both types of verification activities that the Authority performs under Sections 12 and 25 and clarify what forms verification under Section 25 may take.
7. Amend Section 25(4) to give the individual, rather than the authority, discretionary control over the period for which records/logs of authentication and verification are kept.
8. Provide a definition for "Accredited Third Party" and associated provisions outlining governance requirements for this new classification of related entities.
9. Introduce a provision that requires the Authority to maintain and publish a public register of all accredited third parties.

10. Add guiding principles to the Bill that define consent and provides limitations for how it relates to all information disclosures, authentication, and identity verification. We propose that consent ought to be limited in duration and purpose.
11. Introduce provisions that compel the Authority to implement controls/processes that enforce limitations on consent requests that accredited third parties can make to ensure compliance. The controls/processes should require accredited third parties to comply with best practice related to consent purpose and duration.
12. Publish technical and policy documents detailing, among other considerations, the business process, system design, information flows, and technical specifications of identity verification processes provided by the authority.

7. ESTABLISH STRONG PARAMETERS AND SAFEGUARDS FOR INTEROPERABILITY

The word "interoperable" does not appear anywhere in the Bill. Still, the Bill's language nevertheless provides some insight into the system's architecture and the extent to which information-sharing and processing may occur. This "negative information" or inference is an insufficient basis upon which to make holistic recommendations. However, it is instructive in surfacing risks and providing recommendations for the next steps to map, assess and mitigate them. The relevant language includes the Bill's provisions covering NIRA's core functions, authentication of identity information, the creation of a National Identification Number, and the sharing of that number and other registry information held pursuant to other laws and regulations articulated in the Bill's Fourth Schedule.

The Act does not set out or limit the number or "identification databases" (plural) covered in the term "National Identification Databases" within the National Identification System. The amendments to other Acts listed in the Fourth Schedule (Aliens Act, Revenue Administration Act, Passport Regulations, Education Regulations, Jamaican Nationality Act) indicate automatic sharing of information through required disclosures, automatic notices between agencies, and seeding of the National Identification Number across a range of government records. Yet, it is not clear whether such information-sharing falls under the scope of Section 24(1)(c) [discussed above] or if it is not addressed at all in the Act. Furthermore, it is unclear to what extent and by what method data across different datasets encompassed within the National Identification Databases and the NIDS systems as a whole will be linked and/or searchable, and to what extent and for what purposes.

While interoperability is important to ensure efficient and sustainable ID ecosystems, strong regulatory frameworks in policy and system design are needed to reduce privacy and data security risks. The World Bank's ID4D initiative recommends that to mitigate privacy risks "some systems limit data sharing to the absolute minimum necessary or prohibit the propagation of a common unique identifier in order to reduce the ability to link information across databases". The coalition is concerned that since the Bill foresees the propagation of a common unique identifier (national identification number) across government systems, stronger protections are needed in policy and system architecture to protect fundamental privacy rights.

Expert testimony given in the litigation regarding Kenya's NIIMS digital ID system by Indian cybersecurity expert Anand Venkatanarayanan highlighted the dangers in an interoperable system.

Every time a functional database is linked through the unique identifier – meaning every time the government or a third party requires the national identification number for access to services – there is the potential to: a) run surveillance on someone through that functional database, and b) breach the entire system by gaining access to that database, "even if you protect or forbid sharing on the central database."

As an example, Mr Venkatanaryananan stated that with this kind of linking it would be very easy for someone with authorized or unauthorized access to "do targeted messaging during elections, this is not like stealing information but to influence the outcome using profiling." He also explained that the authentication required to conduct transactions and access multiple services creates a trail of where people have linked their data. This "metadata" is enough in itself to build a profile of an individual's affairs and habits and monitor aspects of their life.[17]

IN SUMMARY, WE RECOMMEND THE FOLLOWING:

1. The Government conduct a Human Rights Impact Assessment, which will aid in formulating the necessary recommendations to address these collective risks associated with interoperability in a federated digital identification system, in addition to risks to individuals.
2. Conduct a full data protection impact assessment (DPIA) on the system's architecture and design before it is implemented. The DPIA would include mapping the actual or planned information flows, describing the nature, scope, and context of the processing. This would ensure appropriate purpose limitation in the kind of data shared across different systems through NIDS.
3. The Act should place limitations on what kind of data can be shared and accessed across multiple platforms linked to the unique identifier.

8. IMPROVE SAFEGUARDS FOR PRIVACY IN THE DESIGN AND OPERATION OF THE NATIONAL IDENTIFICATION CARD

In the January 5th Session of the Joint Select Committee, the NIDS Project Team lead, Warren Vernon, shared a correction to the Bill with JSC members. Specifically, Section (19) was incomplete as the card's proposed design would include a "finger pattern" of the enrolled individual's fingerprint. He would go on to provide additional context on the nature of the "finger pattern", give an example of how it would enable identity verification, and the international standards that inform its implementation.

This exchange highlighted an important issue. Section 19(1) enables the Authority, through regulations, to add any information it sees fit to the national identification card. While this discretion is not unreasonable for various kinds of information, such as card meta-information (e.g. card issue date, place of enrolment), we do not believe it is appropriate for the Authority to expand what identity information is displayed on the card beyond what the Bill specifies.

For example, as drafted, the Bill grants the Authority the discretion to include additional biometric identity information of the individual (e.g. full pattern of the fingerprint) or other identity information

17 Nubian Rights Forum et al v Attorney General et al (2020) (Kenya), Anand Venkatanarayanan oral testimony, October 2019.

to the card, increasing the privacy risks associated with its use and possession. Whether or not this is the current intention, it is made possible by the Bill.

We also note that the specifics of how the card will work, how it will interact with the identity verification process, and what technologies are envisioned to be embedded in the proposed card options are all left to regulations or determined during system implementation. These specifics are necessary to understand whether the safeguards included in the Bill or the regulations under development are sufficient.

IN SUMMARY, WE MAKE THE FOLLOWING RECOMMENDATIONS:

1) Amend Section 19 to remove the ability of the Authority to require the display of other identity information not presently listed in the Act on the NIDS card through future regulations. To be clear, this does not prevent the Authority from including other information that is not identity information.
2) The NIDS Project team should publish the technical specification and current design options for the national identification card and detail, among other implementation considerations, how the card will work, how it will interact with the identity verification process, and the card's proposed technologies.

PART 3: GOVERNANCE & ACCOUNTABILITY

9. STRENGTHEN INDEPENDENCE OF AUTHORITY

For the Authority to be effective in achieving its policy objectives, confidence in its integrity and insulation from undue influence are paramount.

The Authority will manage the most expansive collection of personal data in Jamaica's history using an untested data protection framework. The system includes people's biometric and biographic data, a digital authentication platform capable of recording (and thereby tracking) when persons use their National IDs, and the potential to link databases with other systems to perform unspecified functions in the future. Suffice it to say, *if this system were ever misused,* the risks could be severe.

Accordingly, strong institutional safeguards are necessary to minimize the risk of NIDS ever being misused or affected by corruption. We recommend that Authority be established as an independent body, shielded from political influence. It should be established in such a manner that political actors cannot affect or modify its operations without law reform through Parliament. Accordingly, we propose that the Authority be established as a Commission of Parliament or as another form of independent body.

The Existing Institutional Arrangement

Section 5 of the Bill establishes the Authority as a regular agency/department of government under a parent Ministry. That Ministry, according to the 2016 NIDS Policy, will be the Office of the Prime Minister. Like any other government body, it could be moved around the public service, reclassified, restructured, and otherwise have its affairs managed by the changing political directorate.

Section 7 then gives the Minister special power to give the Board of the Authority directives on policies to be implemented. The Board is required to adhere to these. That section reads:

> *"The Minister may, after consultation with the Chairperson, give to the Board such directions of a general character, as to the policy to be followed by the Board and by the Authority in the performance of their functions, as appear to the Minister to be necessary in the public interest, and the Board shall give effect to those directions."*

Why shielding the Authority from undue influence is critical for managing risk

Given the government's intention of transforming Jamaica into a "digital society," the encompassing nature of the data functionalities that the Authority will manage could create perverse incentives and dangerous intentions among political, business, and other interests in the future that must be planned for today. These risks include, but are not limited to, tracking persons' life patterns, profiling individuals, facial recognition surveillance, targeting of individuals and groups based on their activities or attributes, and using the system's functionalities to further political or commercial agendas.

Moreover, the controversy and suspicion that has dominated the passage of the NIDS Bill should not be inherited by the Authority. It is no secret that NIDS has been politically polarizing and highly controversial. The system faced parliamentary impasses, a legal challenge that halted its roll-out, and intense public suspicion.

These above factors taken with the deep corruption issues across Jamaican society that have affected even the highest levels of government in recent years[18] require us to intentionally do things differently, not do business as usual.

While we welcome the few safeguards proposed in the current Bill, such as the establishment of the Inspectorate, we believe that establishing the Authority within a Ministry, directable by a politician is a critical weakness and a vulnerability that is far too easy to exploit now and in the future.

If established in the way currently being proposed, the Authority could be subjected to the known political interferences, administrative control, undue Ministerial discretion, and other forms of "soft influence" that are part of the Jamaican public service.

Protecting the Authority from these risks will not only safeguard its integrity but minimize the degree to which its operations shift with the ever-changing political tides. The Authority's operations should be like its legal identification services: consistent, reliable, neutral, independent, safe, and beyond speculation. Our proposed reforms help achieve that.

Examples of Independent Authorities

Bodies in Jamaica have been established with the requisite independence for them to function without political interference. One such body is the Office of the Public Defender which is established under **Section 4(2)** of the **Public Defender (Interim) Act 2000**. Under the Act, the Public Defender is appointed by the Governor-General after consultation with the Prime Minister and the Leader of the Opposition.

18 Add references

Another example is the Integrity Commission which was established under the **Integrity Commission Act, 2017. Section 5(4)(a).** Similarly, this Act makes the Commissioner ultimately responsible and accountable to Parliament.

IN SUMMARY, WE RECOMMEND THE FOLLOWING:

1. Repeal the power of the Minister to give directives to the Board of the Authority (Section (7)). No political actor should be able to direct the manner in which the Authority operates in their discretion. The Board is already quite stacked with government appointees.
2. Establish the Authority as a Commission of Parliament (or other independent body) accountable to its Board, the Inspectorate, and Parliament only.

10. REVISE UNREASONABLE FORMULATION OF CRIMINAL OFFENCES

Reform the offence of providing "False Information" (Sections 10(7) and (8))

According to Section 10(7), a person commits a criminal offence if they "provide false information or makes a false statement of a material nature with the intention of obstructing or misleading the Authority when: (i) providing information for an entry to the National Identification Databases; (ii) making a modification to an entry to the National Identification Databases; (iii) making a confirmation of the content of an entry to the National Identification Databases; or (iv) obtaining the issue or re-issue of a National Identification Card."

According to Section 10(8), a person commits this offence if they "knew or believed the information to be false; or was reckless as to the veracity of the information."

While persons are encouraged to be truthful, a decision to not share full details of life should not be a criminal offence, especially given that most of the identity information that the Authority will be empowered to require for enrolment is not necessary to establish a person's legal identity. (See Position #2 of this submission on distinguishing between core identity information and other information (pg. 7) for a full discussion on this issue.)

IN SUMMARY, WE RECOMMEND THE FOLLOWING:

1. In order to trigger the offence, the Bill should require that the information provided has demonstrably undermined the Authority's ability to establish their identity accurately. We believe that criminalization should only be possible in circumstances where the person's actions harm the Authority's core function, and never in circumstances where information not relevant to establishing identity happens not to be accurate. If no harm can be demonstrated, then no crime should exist. This is about judicious and proportionate use of the state's police powers, not about whether people should be honest.

2. The Bill should explicitly limit the offence to only identity information required to establish a person's identity and exclude decisions not to disclose non-essential information. As the law is presently phrased, a person who got married in a foreign country at some point in life and chooses not to disclose this and the name of their spouse is also at risk because they "knew or believed the information to be false," or were "reckless as to the veracity of the information." Similarly, it should never be legally possible to criminally prosecute someone

because they chose to give the Authority the wrong occupation or made something up because they were unemployed and did not want to say so.

Repeal offence of failure to notify the Authority if a card is lost, stolen, damaged, etc.

Section 16(12) stipulates that a person who, without reasonable excuse, fails to notify the Authority as required under subsection (7)(c), of the loss, theft, damage, mutilation or destruction of a National Identification Card commits an offence.

This offence unjustifiably exceeds what is a reasonable use of the State's power to criminalize people's actions, especially concerning a system that is to be voluntary and optional. Under this provision, if a person's dog damaged their card by chewing on it and they failed to tell the Authority, they could be criminally prosecuted and convicted. Under this provision, if someone was in a car accident that destroyed their card or it was lost in the process, and they did not report it, they could be charged. Is this truly necessary?

There is likely limited precedence for this kind of criminal offence and we are not certain that it would stand up to human rights and constitutional scrutiny as a proportionate and demonstrably justified use of state power.

A person with a lost, stolen, damaged, or destroyed card already loses access to use their card for services and is deprived of its use as a form of identity verification. The criminal justice system does not need to become involved because the Authority was not notified of every unfortunate event affecting a card.

WE RECOMMEND THAT this offence be removed in its entirety. It is likely an unjustifiable form of coercion to make someone a criminal for not telling the Authority that something bad happened to their card.

11. REFORM PROCESS OF CANCELATION TO ESTABLISH RIGHT TO ERASURE OF INFORMATION NON-ESSENTIAL TO DEDUPLICATION PROCESS AND IMPROVE TRANSPARENCY.

Section 14 outlines a framework for which the Authority may cancel an individual's enrolment. Of note, only in subsection 1(a) and (2) will the identity information of the enrolled individual be purged (subsection (5)(a)) by the Authority. In the case of subsection 1(b), the identity information is retained by the Authority, but they lose the ability to use the national identity card and number (subsection (6)).

We note and welcome the government's policy objective which seeks to use the creation of NIDS to combat identity information and fraud in Jamaica. Captured within this policy objective is a desire that national identification numbers should be unique to an individual. Moreover, no individual should be able to receive more than one national identification number. However, we believe that the Bill's proposed cancellation framework can be improved.

We believe that a right to the erasure of all information non-essential to preventing duplicate enrolments should be extended to all enrolled individuals, regardless of their ordinary residence.

This can be achieved through a reformed cancellation procedure. First, the enrolment process must be transparent with persons about how their information may be processed and/or retained. While

the Bill currently a compulsion on the Authority to inform the individual of various things. This list does not currently include that their identity information will be retained, even if in the future they cancel their enrolment. Transparency in the Authority's actions will be critical for building trust and achieving its policy objectives. Therefore, Section 10(2) should be amended to require the Authority to expressly inform all persons that upon enrolment, there is no guarantee that their information will be deleted even if they cancel their enrolment.

Secondly, during the cancellation process, the Authority should be compelled to purge all information non-essential to preventing an individual from multiple enrolments in NIDS. This may include some pairing of the national identification number and a subset of the biometric data. However, the Authority should purge all other data (e.g. authentication records/logs) related to that enrolled individual. Lastly, the processing of the identity information that the authority retains should be limited to only that which would be necessary for deduplication purposes. Additional processing, disclosure and/or verification of the individual's identity information should be prohibited.

These reforms would combine to create a progressive cancellation process that strikes a reasonable balance between data protection best practice, transparency, and government policy objectives.

ACCORDINGLY, WE RECOMMEND:

1) Section 10(2) should be amended to require that the Authority expressly inform all persons that upon enrolment there is no guarantee that their information will be deleted upon their cancellation.
2) Reform the "Erasure procedure" for all persons who have successfully cancelled enrolment under Section 14. All information on that individual that is non-essential for preventing duplicate enrolments should be purged for the Authority's databases. Only information that is necessary to prevent multiple enrolments by an individual should be retained by the Authority. The Act should prevent any further processing or future disclosure of this data.
3) In the case that an individual's enrolment has been cancelled, a limitation should be placed on the Authority's ability to process, disclose and perform verification services on the individual's identity information that has been retained for deduplication purposes.

PART 4: ACCESSIBILITY & INCLUSION

12. SUPPORTING VULNERABLE PERSONS IN ALL SERVICE INTERACTIONS

While the law encourages the Authority to be attentive to the needs of persons with disabilities and allows for persons to apply for enrolment on behalf of children, incarcerated persons, and the mentally ill, it can go even further by creating a cross-cutting mandate to support vulnerable persons at all service interactions - not just enrolment.

Strengthening the mandate to support the vulnerable

Section 5(7) requires that the Authority "have regard to the needs of persons with disabilities" in the performance of its functions. We welcome the inclusion of this language and the policy intent it demonstrates. Below we propose considerations for how it may be improved.

First, persons with disabilities are not the only group that the Authority should be legally required to specially consider. We believe that the Authority should always consider the realities of any groups that are vulnerable or socially excluded, given the nature of its functions which may touch on many areas of life and expansive service areas across society. This includes but is not limited to children, the elderly, illiterate persons, the homeless, non-English speakers, and persons who are sick and shut-in.

Second, "having regard" to persons with disabilities is vague, passive, and weak as a mandate. Standard language would include an obligation to make "reasonable accommodation" and other forms of support that are more active and direct.

We recommend strengthening this mandate to explicitly capture the affirmative and proactive nature of the Authority's responsibility and to expand it beyond persons with disabilities. We propose that a new subsection be introduced under Section (5) that expands subsection 7 and requires that the Authority have due regard to the circumstances and needs of vulnerable groups in executing its functions, make reasonable accommodation, and provide special assistance at all stages of their interactions with the Authority.

Protecting The Mentally Ill

Section 10(4)(b) of the Bill allows someone to apply for enrolment of a person with a mental disorder within the meaning of the Mental Health Act if they are the "nearest relative" of that person. While this is a positive step, it is important to recognize that having a "mental disorder" as defined within the Mental Health Act does not automatically render someone incapable of conducting their affairs or providing consent.

The Authority should be required to make reasonable enquiries as to whether the person proposed to be enrolled has consented to the enrolment or has the capacity to consent. It should only process the enrolment once it is satisfied that the circumstances warrant it.

Many persons with mental illnesses maintain productive lives across society while on treatment and medication. The present wording of Section 10(4) suggests that the nearest relative could apply for enrolment of a person who has a mental disorder regardless of whether that person has consented to that enrolment. We doubt that this is the intention. To best protect the rights and dignity of all persons, and to ensure that the system is genuinely voluntary, that power should only be accessible where a person consents to it, or where it has been *demonstrated* that they lack the capacity to consent, are unlikely to retain such capacity, and the enrolment is in their best interest.

This adjustment protects persons who may experience only episodes of mental illness or have relatives with nefarious intentions from enrolling them and potentially taking advantage of them or their resources once they are enrolled.

Applying On Behalf of Children

Section 11(4)(a)(ii) of the Bill allows the person in charge of a childcare facility to apply for enrolment on behalf of a child at that facility. There are three areas for improvement here.

First, this should be expanded to include any person with lawful custody or care of a child, such as long-term Foster Parents. Many children who are in forms of alternative care are not only in facilities. Many are with foster families and in other forms of care not limited to a "facility."

Second, this power of persons who are not parents or guardians to enrol children in NIDS should be limited only to circumstances where parental rights have been severed, or a child is in long-term state care.

In reality, a child may come into the care of a facility due to an emergency, only for a short time, or just in-between legal proceedings. Often, the placement of a child in a facility is the subject of legal proceedings involving the parents or is even contested by the parents. In those circumstances, we see no reason why a facility manager should be able to assume the power to apply for enrolment on behalf of a child in circumstances where the parents are available and where parental rights have not been severed.

Third, where applications are made under Section 11(4)(a) by a facility manager or other person who is not a parent or guardian, the Bill should require notification of the parent or guardian and allow a reasonable period of response before processing the enrolment.

IN SUMMARY, WE RECOMMEND THE FOLLOWING:

1. A new section be established (likely under Section 5) that mandates that the Authority have due regard to the circumstances and needs of vulnerable groups in executing its functions and make reasonable accommodation and provide special assistance at all stages of their interactions with the Authority.
2. Section 11(4)(b) be amended to require that in circumstances where a person seeks to enrol a person with a "mental disorder" that the person to be enrolled consents to the enrolment unless it has been *demonstrated* that they lack the capacity to consent, are unlikely to retain such capacity, and the enrolment is in their best interest.
3. Section 11(4)(b) be amended to require that in circumstances where a person seeks to enrol a person with a "mental disorder" that the Authority make reasonable enquiries into whether the person proposed to be enrolled has the capacity to consent, and only process the enrolment once it is satisfied that the enrolment is in the person's best interest.
4. Section 11(4)(a) be expanded to include any person with lawful custody or care of a child, such as long-term Foster Parents.
5. Section 11(4)(a) be amended to limit the power of managers of childcare facilities and other persons who are not parents or guardians to enrol children only to circumstances where parental rights have been severed, or a child is in long-term state care. Further, where such applications are made, the Bill should require notification of the parent or guardian and allow a reasonable period of response prior to processing the enrolment.

13. MAKE APPEALS PROCESS MORE ACCESSIBLE:

An integral part of any legal framework is the accessibility and credibility of its system of review. As part of a judicial framework, appeals function as a process for error correction as well as a process to clarify and interpret the law or a decision.

Section 26(1) of the Bill establishes an Appeals Tribunal. Subsection (2) further provides for the appeal to be made by an enrolled individual within twenty-eight (28) days of the adverse decision being communicated to the individual or such longer period as the Tribunal may allow.

The current Bill includes several limitations on the appeals process we believe inhibit its effectiveness. We will outline these limitations and propose related recommendations in the sections below:

Definition of Appellant

Section 26(2) states that the appellant must be an enrolled individual. Under Section 2, an enrolled individual is defined as an individual whose identity information is stored in the National Identification Database. The creates a challenge in which the current definition of an appellant does not include an individual denied enrolment and who wishes to appeal the decision. This appears to be an error because the law establishes that in both Section 10 and 14 that decisions related to enrolment are subject to appeal. The conflict therefore occurs in a definition of "appellant" that frustrates this.

One way to address this is to define an appellant as any individual affected by a decision of the Authority.

Time Allowed For Appeal

The twenty-eight (28) days allowed under the Act is woefully short compared to appeal processes under other legislation. In comparison, the Access to Information Act, Section 32 (3)(a), provides an appellant ninety (90) days in which to appeal a decision.

Respectfully, a Twenty-Eight day period is quite short considering the fact that it is likely that persons may attempt to resolve issues by first contacting the Authority prior to immediately appealing a decision. That process of corresponding with government agencies is normally not quick. It is likely that an aggrieved person may take over a month to go back and forth with the Authority about a decision to then realize that they will need to lodge a formal appeal.

However, with such a short timeline, aggrieved persons may either decide to immediately appeal (even if unnecessarily) in order to not affect their allowed time to appeal or decide to engage the Authority in a standard grievance/customer service enquiry at the expense of their appeal. The Authority could also benefit from delaying these administrative grievance processes or customer service complaints since appellants only have a short window to appeal.

While the Bill does grant the Tribunal discretionary powers to extend the period in which an appellant may appeal a decision, that power is completely at the Tribunal's discretion and does not address the underlying issue: the short window in which an individual can appeal. As is, the standard appeal window will likely place an unnecessary burden on the Tribunal to frequently consider extension requests when the more sustainable option would be to extend the time in the Bill to give appellants sufficient time to appeal decisions.

Appeal Tribunal Panel To Regulate Own Proceedings

In the Second Schedule (9), broad discretion is given to each Appeal Tribunal panel to regulate its proceedings. This does not constitute best practices. The proceedings of the Tribunal should be regulated to create a standard procedure for its operation. Certainty is a critical component of the right to due process under the law. The Tribunal should not be empowered to modify its own procedural rules, which may include, but not limited to, how evidence is adduced and how decisions are made.

IN SUMMARY, WE RECOMMEND THE FOLLOWING:

1. Section 26 should define an appellant as an “individual” and not as an “enrolled individual”. This would remove the limitation placed on who may appeal a decision of the Authority.
2. An individual’s window to appeal a decision be extended to Ninety days (90) due to the importance of issues concerning access to legal identification. The discretion of the Tribunal to extend the time thereafter should be retained.
3. Regulations be created to govern the operational procedure and processes of the Tribunal. This power is presently delegated to the Tribunal itself, which has authority to set and change its own rules of procedure at its discretion.