**SUBMISSION OF THE MAJOR ORGANISED CRIME AND ANTI-CORRUPTION AGENCY (MOCA) ON THE NATIONAL IDENTIFICATION AND REGISTRATION ACT, 2020 TO THE JOINT SELECT COMMITTEE OF PARLIAMENT- JANUARY 2021**

**Preamble**

The National Identification and Registration Act 2020 provides for the establishment of a National Identification Registration Authority (NIRA), which will be responsible for the setting up of a National Identification System. The National Identification System encompasses a National Identification Database, National Identification Numbers, National Identification Cards and the necessary processes for the required storage, retrieval, services, networks, measures for enrolling individuals, verifying their identity and issuing Identification Numbers and Cards.

The intention of this submission is to identify areas in which this legislation can be made more robust in its application and scope and also to indicate areas in which the legislation may enhance national development.

**General Discussion and Recommendations**

The Agency believes that this act will have great utility in improving efficiency in governance. From a Law Enforcement perspective, lawful access to the information contained in the database should, it is anticipated, be an asset to the conduct of investigations. With such a system, the ability of assuming multiple and false identities should be decreased significantly.  The use of Biometrics, for example should assist to curtail these practices.

* The bill proposes that enrollment in NIDS is voluntary and given this reality, it is not unlikely that individuals involved in nefarious activities may decline to register or in fact de-register if they were previously enrolled. Section 14, states, the Authority shall cancel the enrollment of an enrolled individual if -(b) the individual requests in writing to the Authority, accompanied by the National Identification Card issued to the individual, that the enrollment be cancelled. **It is recommended that even if enrollment is cancelled, consideration should be given for the non-expungement of the identity information from the national ID database. At the minimum, some basic data (name, D.O.B, address) should be retained and an audit trail maintained, highlighting date and reason for expungement.**
* Section 25, which makes reference to an accredited third party to whom information from NIDS may be entrusted, with an individual’s consent. **It is recommended that the term “an accredited” person be defined or expounded upon in the Act.**
* Regarding Disclosure of Identity Information, Section 24(2) permits the Commissioner of Police (without notice) through application to a Judge of the Supreme Court, for an order to the Authority to release information for specific purpose; this we found is a very useful and prudent insertion. However, given that accessing the data in this manner is required for prevention, detection and investigation as well as for National Security (sec 24(20)(a)(b) purposes, then other law enforcement entities may also require the information, hence the head of those entities should also be considered, example the Director General of MOCA, Chief Technical Director, FID.
* There is currently a heavy reliance on information provided by the Register General’s Department (RGD). Given that according to the act, the database will be subsumed by the NIRA, consideration should be given to the process of acquiring information from the department. Currently, MOCA and to the best of our knowledge, other law enforcement agencies obtain information by applying to the CEO of the RGD. It is suggested that the bill indicate if that process will remain (given that the data being sought would be data that does not comprise part of the NIDS) or follow the stipulated protocol in the Act for obtaining NIDS information, which by virtue of the current formulation would preclude MOCA from making an application.
* It is highly recommended that there is continuous vetting of all staff members, especially those that will have access to the database records, electronic or physical. This is based on the sensitive nature of the information that will be contained in NIDS.
* There is no provision at Section 19 (3) for possession as an offence. This could pose a challenge, where an individual is found with NIDS data in either physical or electronic form, without a lawful excuse. There is also no mention of the computer as a repository or being incidental to a crime. It is recommended that an offence of possession simpliciter be considered and it should cover both physical and electronic records.
* Section 23(a) (c) (d) (e)(f)(g) and (h) refer to a generic outline of cybersecurity and information security standards. It is suggested that there is also an outline of adherence to or mention of international standards with defined security controls.These standards, while not an exhaustive list is critical for data management. Two recommended standards that relate to **Data Privacy** and **Data security** are **ISO 27701** and **ISO 27001.** They are described as:

1. ***ISO 27001*** *relates to the way an organization keeps data accurate, available and accessible only to approved employees.*
2. ***ISO 27701*** *relates to the way an organization collects personal data and prevents unauthorized use or disclosure*

These adherences serve to prevent the bill’s itemized standards from becoming outdated as best practices evolve and new technologies become available as well as being General Data Protection Regulation (GDPR) compliant.

* Section 23, (d)(i) The reference Viruses falls under the category of malware and need not be separated. It is recommended that the reference to viruses and malware should be rephrased to say *‘Malware including viruses, ransomware, trojan, worms etc.’*
* With respect to Section 23, as part of the security of information, there should be consideration for a Cyber Incident Response process. For example, where a breach occurs during regular operation and outside the control process of the Inspectorate as outlined at section 27(3) (f).
* A **protected computer** is defined as belonging to a class of computers or used by a certain body as outlined below and is used directly with;

1. the security, defence or international relations of Jamaica;
2. the existence or identity of a confidential source of information relating to the enforcement of the criminal law of Jamaica;
3. confidential educational material, such as examination materials;
4. the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or essential public infrastructure such as hospitals, courts, toll roads, traffic lights, bridges, airports and seaports;
5. the protection of public safety, including systems related to essential emergency services such as police, fire brigade services, civil defence and medical services.

It is recommended that the servers that host NIDS database and any other related hardware be regarded as protected computers. Section 9 (10)(a) of the Act states that a person who commits an offence under subsection (9) shall be liable on conviction before a **Parish Court**, to a fine. If our recommendation is accepted it would therefore be consistent with the existing Cybercrimes Act 2015, where the applicable sections in regards to protected computers, state that where an offence is committed, the offender shall be tried on indictment in the **Circuit Court** and shall be liable upon conviction to a fine or imprisonment. To effect same, a consequential amendment to the Cybercrime Act, 2015 would be necessary.