GOVERNMENT OF JAMAICA

OFFICE OF THE PRIME MINISTER

Design and Development of the ICT Architecture
for the Planned Implementation of a
National Identification System for Jamaica

Project QCII #2013/NRU/001

ASSESSMENT REPORT

February 24, 2014

PREPARED BY
Henry Dreifus
ICT Project Executive

TABLE OF CONTENTS

1. Executive Summary 5
2. Assessment Objectives 8
2.1 Approach 8
2.1.1 Stakeholder Interviews & Site Visits 8
2.1.2 Prior Documentation & Report Review 9
3. Preliminary Findings 10
4. Forward Considerations 15
4.1 Leveraging of Existing Identity Components / Resources 15
4.2 Validating and Reconciling Data 15
4.3 Establishing Unique Person and Document Identifiers 16
4.4 Biometrics 17
4.5 Digital Signatures and Electronic Identity 18
4.6 ID Cards 18
4.7 Standards 18
4.8 ICT Infrastructure 19
4.9 Laws and Legislation 19
4.10 ROI & Sustainability 19
Appendix A: eGov Jamaica Limited 21
Appendix B: Ministry of Labour & Social Security 30
Appendix C: Jamaica Constabulary Force 41
Appendix D: Tax Administration Jamaica 44
Appendix E: Electoral Office of Jamaica 54
Appendix F: Ministry of Health 59
Appendix G: Registrar General's Department 68
Appendix H: Ministry of Education 78
Appendix I: Other NIDS Stakeholders 83
Appendix J: Stakeholder Questionnaire 90
Appendix K: Source References 93

PROJECT SYNOPSIS

Project Title:	Design and Development of the ICT Architecture for the Planned Implementation of a National Identification System for Jamaica
Project ID:	QCII #2013/NRU/001
Project starting date:	January 02, 2014
Project end date:	June 30, 2014

Document Title	Assessment Report
Purpose	Review of Existing Identification Resources and Stakeholders, including: • Business Processes • ICT Architectures, Databases and Data Models • Network Security • Policies and Procedures

DOCUMENT REVISIONS

Document Revision	Date	Description
0.1	Jan 17, 2014	Internal Working Draft
1.0	Jan 31, 2014	Initial Draft Submitted
2.0	Feb 24, 2014	Revised Draft: • Incorporates Feedback from RGD and eGovJa • Adds input from meetings with NHT, MSTEM and PICA
		Final Deliverable

ABBREVIATIONS

Acronym	Description
ADSL	Asymmetric Digital Subscriber Line
AFIS	Automated Fingerprint Identification System
ATS	Application Tracking System
AVR	Automatic Voice Response
BDMS	Birth, Death, and Marriage System
BMIS	Beneficiary Management Information System
CHDP	Child Health Development Passport
COJ	Companies Office of Jamaica
eGovJa	eGov Jamaica Limited
EOJ	Electoral Office of Jamaica
ePAS	Patient Administration System
FSL	Fiscal Services Limited
GOJ	Government of Jamaica
ICT	Information & Communication Technology
ICTAS	Integrated Computerized Tax Administration System
ID	Identity *or* Identification
IDB	Inter-American Development Bank
IP	Internet Protocol
IRIE	Index Rebuilding Implementation Exercise
JCF	Jamaica Constabulary Force
LAN	Local Area Network
MDA	Ministries, Departments and Agencies
MIS	Management Information System
MLSS	Ministry of Labour & Social Security
MOE	Ministry of Education
MOF	Ministry of Finance
MOFP	Ministry of Finance and Planning
MOH	Ministry of Health
MSTEM	Ministry of Science, Technology, Energy and Mining
NAS	Network Attached Storage
NHC	National Health Card
NHF	National Health Fund
NHIS	National Health Information System

Acronym	Description
NIDS	National Identity System
NIF	National Insurance Fund
NIMS	National Insurance Management System
NIN	National Identity Number
NIS	National Insurance Scheme
OPM	Office of the Prime Minister
PATH	Programme of Advancement Through Health and Education
PBX	Private Branch Exchange
PICA	Passport Immigration & Citizenship Agency
PIOJ	Planning Institute of Jamaica
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PPS	Pension Payment System
QC	Quality Control
RGD	Registrar General's Department
SQL	Structured Query Language
TAJ	Tax Authority Jamaica
TRN	Tax Registration Number
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access

1. EXECUTIVE SUMMARY

The Consultant Team has been engaged to support the Design and Development of the ICT Architecture for the Planned Implementation of a National Identification System (NIDS) for Jamaica. Establishing a robust and accurate electronic Identity framework is recognized as an essential step in the evolution of Public Sector modernization. Such modernization is key to improving efficiency and competitiveness within the country; provisioning the efficient, secure and effective delivery of in-line and on-line government services including healthcare, social services, voter registration, taxes, national insurance, education, skill provisioning, licensing, etc. at lower costs and greater stakeholder convenience.

This Assessment Report summarizes the Consultant Team's initial findings of the existing Information & Communication Technology (ICT) ecosystem, the key needs and the projected use-cases for NIDS in Jamaica. These preliminary findings were established through discussions with stakeholders and the review / analysis of supplied prior project documentation.

All the organizations we met with have been extremely open and supportive. There is a strong common desire for NIDS among the interviewed stakeholders and there is a good understanding of the benefits to be gained, both on a micro level within their own organizations and at a macro level for immediate and long-term positive outcomes across Jamaica.

There are both gaps and opportunities to achieve the objectives and successfully implementing NIDS to both lower the total costs of management of Identity – and improve precision and data protection/assurance. None of the challenges identified so far are considered by the Team to be insurmountable, and the stakeholders have shown great resource and innovation in overcoming current constraints.

Jamaica is NIDS-ready. A common unique person identifier (NIDS) is universally anticipated by the stakeholders interviewed, for both provisioning and improving of fit-for-purpose identity systems within each ICT infrastructure domain. What is needed is a NIDS operational framework, business process and common architecture that will harmonize the present identity "silos" to maximize their effectiveness and streamline each current ID processes and cost structures. NIDS will greatly reduce much of the duplication of effort and costs in establishing and managing identity across the country. The introduction of NIDS offers a unique opportunity to help improve the quality of current identities; to fill in gaps and missing information in the civil registry, etc., and establish and enforce consistency. Robust identity

vetting is therefore a crucial component to NIDS; critical in creating the necessary confidence and trust in identity that will lead to widespread adoption and use. NIDS will also enable a reconciliation of the existing ID databases that may have errors, duplicates, incomplete and / or missing records.

A number of key initial considerations have been formulated by the Team from the meetings and research to-date. There are summarized below and addressed in more detail in the report. These considerations provide focus for the ongoing analysis of best-practice Identity System components to meet the NIDS identified needs, resources and capabilities. Considerations include:

- Leveraging of Existing Identity Components / Resources:
  - Wherever possible, leverage existing investments and infrastructures; streamlining existing systems and eliminating the duplication of effort.
  - Enable the association of disparate ID silos to improve stakeholder outcomes.
- Validating and Reconciling and Improving Existing Identity Data:
  - Establish the trust baseline that will encourage widespread adoption of NIDS by assuring the integrity, accuracy, security and privacy of data.
- Establish a common framework for both Unique Person and Unique Document Identifiers:
  - Enable unambiguous identity resolution to an individual (or entity); independent of the associated document identifiers that are bound to that identity.
  - Supports both the governmental stakeholder needs and also provides for the private sector a secure and verifiable identification framework.
- Prepare for Electronic Digital Signatures (PKI):
  - Assess the immediate need for PKI in NIDS for supporting online as well as physical identity; or whether it should be accommodated as a future enhancement.
  - Assure threshold of unique person data can be vetted to meet ITU standard X.509v3 for developing a digital certificate (e.g. make NIDS digital certificate ready)
- Assuring a Robust Data Protection, Privacy and Security Framework
  - Identify the appropriate system standards to protect data privacy and integrity, and to enable interoperability, transparency, accountability and secure connectivity between systems.
- Evaluate Issuing a Multipurpose NIDS ID Card
  - Assess the options and trade-offs of smart cards vs. lower cost identity card options.
  - Determine if existing issuing infrastructures can support a NIDS unique document production.
  - Should there be a NIDS Multi-purpose ID card, and if so, when and how.

- Architect a Sustainable and Reliable NIDS ICT Infrastructure:
  - Provision a robust ICT infrastructure built on existing capabilities that supports the efficient delivery pf services in a more streamlined and cost-effective approach.
  - Consider on-line, real-time verification (e.g. like credit card validation), and associated system availability and highest levels of reliability.
- Consider Implementing Civil Biometrics:
  - Evaluate the need, type and use case(s) for biometrics in assuring uniqueness for identity verification/authentication.
- Consistent with Best Practice Laws and Legislation:
  - Liaise with legal consultant team to confirm framework is consistent with current and anticipated legal and policy constraints and / or ensure that laws and legislation are aligned to the desired outcomes.
- Lower Total Cost of Ownership with Demonstrated ROI:
  - Ensure appropriate stewardship and governance is in place for long term NIDS sustainability, evolution/continuous improvement and robust management of physical and virtual identities.
  - Develop a high level ROI and high level cost savings model based upon streamlining and simplification duplicative efforts and evaluate the potential for revenue generation from an online verification service to become self-sustaining.

These considerations shall be incorporated into the analysis of current capabilities against the specific objective for NIDS. This shall result in the development of cost-effective solution options that can be implemented as seamlessly as possible to enhance current ID capabilities across the existing investments in ID systems.

Continued review of the current ecosystem is ongoing with the stakeholders, as well as an analysis of findings that will result in a High-Level Concept Design. This design will have its foundation in the findings from this assessment coupled with global identity best-practices. The Concept Design will define and outline the key framework components and will include business process re-engineering recommendations to streamline the identity ecosystem. A detailed ID system design will subsequently expand upon the Concept Design to describe a feasible architecture, components, interfaces and process requirements, applying and leveraging as much of the existing and forthcoming infrastructure as appropriate.

The team will continue to consult with stakeholders during the course of the project in each of the participating MDA's to further refine the understanding of needs and capabilities, and to ensure the resultant NIDS framework design and go-forward recommendations are fit-for-purpose and accommodate the specific needs of each of the stakeholder communities.

2. ASSESSMENT OBJECTIVES

This Assessment is the first of four steps in the design of the NIDS architecture. Subsequent phases will deliver a High-Level Concept Design, a Detailed System Design, and an Action Plan for implementation.

2.1 APPROACH

2.1.1 STAKEHOLDER INTERVIEWS & SITE VISITS

To enhance efficiency and increase consistency, the Consultants formulated a short questionnaire submitted (see Appendix J:) in advance of meetings with stakeholders using/needing government ID systems and data registries, including the national electronic transactions initiative developed by the Trade Board. This questionnaire served as a guide for the meetings, and detailed responses helped the team formulate a common understanding of the baseline identity frameworks, opportunities, issues and challenges during stakeholder meetings.

Note: responses have not yet been received from all stakeholders. The team will continue to update / revise the report to reflect as full picture as possible as more information is received.

Meetings and site visits were held during the week of January 13th, 2014 with follow-up meetings scheduled where needed:

- eGovJa Jamaica Limited (formerly Fiscal Services Limited)
- Ministry of Labour & Social Security
- Jamaica Constabulary Force
- Tax Administration Jamaica
- Electoral Office of Jamaica
- Ministry of Health
- Registrar General's Department
- Ministry of Education
- Trade Board Limited

A brief teleconference was also held with the Passport Immigration & Citizenship Agency (PICA) and an in-person meeting and walk-through is being scheduled for a later date.

2.1.2 PRIOR DOCUMENTATION & REPORT REVIEW

A review of documentation supplied by Ministries, Departments & Agencies was conducted, along with a review of reports and presentations developed during prior NIDS projects and seminars. This has helped the Team develop a deeper, more detailed understanding of current capabilities and future requirements.

Appendix J: provides a list of project reports and other documentation reviewed by the Consultant Team.

3. PRELIMINARY FINDINGS

The preliminary meetings and site visits provided invaluable insights to the present and planned systems and challenges within Jamaica's ID ecosystem. There are a number of challenges facing the country in moving toward a common National ID System (NIDS) that will support secure, reliable and robust identity verification and authentication, but none so far are considered insurmountable by the Team. The requisite "building blocks" for NIDS are generally established, accepted and in place.

The country has done a remarkable job achieving so very much to-date with fit-for-purpose identity systems and ICT infrastructures within its austere financial constraints. The systems reviewed demonstrated well thought out processes to overcome some of the technical constraints and shortcomings. There are no critical single-points of failures, although there are areas that should be reviewed and consider improvement.

There are pre-existing expectations and demand for NIDS. Everyone we interviewed uniformly welcomes NIDS as a way to avoid spending for standing up and maintaining costly ID infrastructure(s) and sees the benefits, both on a macro level for the country and on a micro level to achieving their specific goals/objectives. Most have some level of planning/anticipation for NIDS and in some cases have incorporated a data field for linking a NIDS unique person identifier into existing databases and database designs. Others have expectations of NIDS as becoming their core unique identifier – such that implementing NIDS has become mission critical.

The identity ecosystem presently consists of a number of independently managed identity "silos" – purpose built to meet the needs of the stakeholder organization but unable to effectively interface with other systems. There are some checks, but only cursory cross-domain verification between identity silos. As a direct consequence, there is a large number of purpose driven identity numbers created – and still growing – with no consistency or standards driving the creation and long-term accountability of these numbers. Some forms of identification do not expire, and there are no easy ways presently to provide reconciliation. Further, there is no consistency across regimes in the vetting of IDs – as each application and vetting process is unique and purpose-driven – resulting in a potential net lower confidence in the integrity and accuracy of the identity data captured, with the exception of the Electoral Commission, as it operates a continuous verification model.

Other initial observations include:

ID Numbers: There are many concurrent ID numbers in use across Jamaica and there are a lot of resources dedicated their individual ID creation, management and maintenance. In many cases this are duplicative efforts that could be streamlined through NIDS.

Paper Records: Almost all of the authoritative records are paper based. There are several MDA initiatives seeking to digitize / digitalize legacy paper records (including at RGD, MOH, TAJ, etc.) but there has been only sporadic, not systematic efforts seeking to re-engineer of the business processes regarding common identity.

Proof of Identity: There is no consistency between MDAs as to a common acceptance of foundational ID documents that form the basis of proof-of-identity. The Tax ID (TRN) appears to be a widely used form of identification, but is not a picture ID document nor biometrically differentiated, and has little vetting associated with its issuance. The TRN was designed to provide for a means of payment to the government (customs, taxes, etc.) Certified photographs are also accepted as proof of identity for some stakeholders.

Criminal AFIS: Hosted and operated by the JCF, the criminal Fingerprint data base (AFIS) is also used in the vetting process to issue a large number (>120,000/year) of police certificates, each for a defined term/period. Background checks are limited to verifying there is no criminal record on file in support of certain employment, visa applications, etc. at the time of application.

Civil Biometrics: An AFIS is also used by the EOJ and is very narrowly governed by legislation. Fingerprints as a unique means of identification appears to have broad acceptance as a valid and authoritative form of identity assertion by the civilian population but for those specific purposes. There are sensitivities that need to be understood and carefully managed in the incorporation of biometrics for NIDS.

Appendices A - H summarize the Team's findings for each of the stakeholder interviews by the Consultants. Below are a few of the high-level, summary points:

eGovJa: Has the most experience hosting enterprise ICT solutions for multiple agencies.

- Hosts ICT systems for TAJ, MOH and others.
- Chartered to provide shared ICT services and solutions government-wide and will be instrumental in ensuring that the Jamaican people and government can truly participate in the global digital evolution.
- Has documented ICT security policies and practices.

RGD: Provides a critical authoritative source for identity that is considered and accepted as foundational in establishing a person's identity.

- Best practices initiatives for accurate and timely birth registration, including bedside newborn registration.
- Most identity documents rely on the civil registry as the authoritative source record.
- Faces significant challenges with missing, inaccurate and incomplete data records.
- Presently not able to reconcile all life events (birth, marriage, death).
- Historically sporadic automation, including developing a rudimentary online verification service.
- Identification numbers are not assured to be unique.

EOJ: Has a proven and accepted, purpose-driven identity capability:

- Mandates an AFIS biometric to enroll to identify and assert a unique identity for voting.
- Well established continuous vetting process for both intake and life cycle identity assurance
- Maintains the largest biometric database in the country (~ 1.7 million records) but legally restricted from being used outside of voting.
- Has an internally managed ID card personalization facility to issue the voter's ID card, once a person's identity is vetted.
- Operates a national identity verification service during elections

TAJ: The Tax Registration Number (TRN) is an institutionalized and accepted entity identifier commonly accepted as an identity number.

- TRN was initially designed as a purpose driven method to associate an identifier with collection of revenue for the Government. It was not designed as a national ID.
- Any interaction with the government that may have a fiscal component – such as obtaining a Driver's License requires a TRN.
- Currently all authoritative records are on paper. An initiative is underway to introduce a Document Management System to digitalize all records.
- Current provides a basic on-line TRN number look-up tool.

MOH: Recognizes the importance of a unique patient identifier and is expecting to incorporate the NIDS in the developing comprehensive Health Management System.

- In the interim, stakeholders have created and issued a patient ID number for use with first step in the HMS rollout: The Patient Administration System (ePAS) pilot scheduled to start in April, 2014.
- The "NHIS Strengthening and e-Health Strategic Plan 2014-2016" critically relies on a unique person identifier and would benefit immediately from NIDS.

NIS: Presently has several concurrent identity "silos" and needs to link to multiple resources across government as part of its mission, including RGD, TAJ, COJ, MOFP and others.

- Identifiers are not unique used in different systems with no easy way to cross-reference.
- Has been planning on forthcoming NIDS identifier as part of their system upgrades, which would help with streamlining and reconciliation.

MOE: Needs the ability to better track stakeholders (including students, teachers, etc.) throughout the educational system.

- Has a proposal for a unique student identifier – not yet implemented.
  - Unique Identifier needed to better track teachers & students
- Of notable concern is education and training for the 15 – 24 year old group whose unemployment rate is estimated to be more than 3 times that of the adult unemployment rate.
- MOE responsibility includes public, private schools and those being home-schooled.

Trade Board: Has implemented a Digital Certificate Authority to secure online transactions for stakeholders across government e.g. Tax Payments.

- Given the authority under the 2006 Electronic Transactions Act. The Act may require clarification and update and will be reviewed / assessed.
- Has established a Digital Certification platform – provides the potential to form the baseline for digital identity subject to further review/assessment.

4. FORWARD CONSIDERATIONS

4.1 LEVERAGING OF EXISTING IDENTITY COMPONENTS / RESOURCES

There are many concurrent Identity Systems established and in use in Jamaica – in several cases there is more than one ID system in operation within an organization. Significant investments have already been made (and are ongoing), in equipment, business process engineering and in time to implement and improve these systems. An important guiding objective of this project is to leverage existing investments wherever possible in the realization of NIDS, and to streamline the existing systems and avoiding duplication of effort and costs.

Evaluation of resources already in place that may be re-used and / or re-purposed for NIDS is being assessed for technical viability. There may be legal and/or operational constraints that may prevent fully leveraging these investments, and to the extent possible these observations will be documented.

4.2 VALIDATING AND RECONCILING DATA

Key to establishing trust and encouraging widespread use of the NIDS is ensuring the foundation integrity, accuracy, security protection and privacy of the underlying data. Although tempting to "kick-start" an identity system by importing existing databases, if the accuracy and integrity of the imported data is questionable, then the system will not garner the trust of stakeholders.

There are well documented gaps and errors (duplicates, omissions, partial records, etc.) in the existing identity databases (including birth certificates, tax, electoral, NIS, health, etc.) – and this is not unusual. There is no 100% perfect framework. Validation and reconciling of existing records, and providing a robust business process to correct and fill in the missing gaps and omissions will be a key factor in building confidence in the underlying data. Identity vetting is therefore a crucial step for NIDS. Claimed identity data presented by an applicant as proof-of-identity (such as a birth certificate, etc.) must be vetted to the best practices framework where possible balanced by the economic tradeoff's to maximize the integrity of the system, to prevent introducing genuine errors and to mitigate fraud and abuse. Taking advantage of the identity ecosystem pieces already in place – including the extensive frameworks of the EOJ, RGD and others can provide a 'sum greater than the individual parts' outcome for NIDS.

Birth is the first life event that sets in motion the process to establish identity for the super majority of Jamaicans. Birth records are the primary foundation point that drives an

individual's subsequent proof of identity. Thus the birth certificate is a critical proof of identity. Subsequent life events (obtaining healthcare, enrolling in school, entering the work force, earning a Driver's License, applying for a passport, registering to vote, voting, etc.) all require an identity verification transaction and this becomes an opportunity to perform ongoing, periodic verification of identity. This is a best practice, as already performed by EOJ.

At the introduction of NIDS, this will also create the opportunity to "clean-up" and fill in gaps, errors and omissions across existing databases. NIDS once instituted will allow the reconciling of identity across multiple sources of identity information by providing a consistent, uniquely resolvable means of identification.

4.3 ESTABLISHING UNIQUE PERSON AND DOCUMENT IDENTIFIERS

Unique Identifiers are the foundation for a consistent, standards based identity framework. Such identifier must be unique to an individual (or entity) and bound to that individual for life (and even beyond). This Unique Identifier should allow the unambiguous binding of that individual to significant events (e.g. registering to vote, certification to drive a car, marriage, retirement, etc.).

Presently there are a large number of purpose-driven identity numbers in use across the Government. Each has evolved to meet the needs and purpose of the stakeholder for that particular application, but none are truly interoperable across other systems. Often, as is the case with the TRN, an ID scheme was designed and crafted for a single purpose, but ends up being applied beyond that initial intended use.

A critical component of NIDS, therefore, is the definition of a Unique Person Identifier, usable across government – and in the private sector – which can uniquely identify an individual in all scenarios and for all applications. The prior research and analysis, including data field mapping across identity domains yielded a high degree of commonalities. Once a person's identity is uniquely resolved, all subsequent services can be greatly streamlined and provisioned more efficiently and at significantly lower costs. The Consultant Team will provide a recommendation for the structure and assignment of a Unique Identifier that can be applied country-wide. The concept design will also identify best practices for assigning and utilizing Unique Person Identifiers, especially in cases where there are gaps and errors in the underlying authoritative records. Once developed, stakeholders can begin the process of streamlining and improving the individual and combined ID processes, however it is important to note that a new ID solution will take time to roll out, and legacy ID's will still need to be accepted and used during a transitional period of time.

There have been a number of prior efforts and proposals related to the creation of a National Identification Number (NIN), as documented in prior reports by Delaware and others. This work has led to provision being made by a number of MDA's for the future use of a NIN. The Consultant Team has not yet identified a final recommendation for the structure of a unique person identifier. Regardless, responsibility for the creation, generation and management of the unique person identifiers must be clearly defined, along with an understanding of how this will co-exist with existing ID numbers with the potential to replace them over time.

4.4 BIOMETRICS

A determination must be made regarding the use of Biometrics for NIDS. Many best-practice ID systems increasingly use biometrics for two purposes:

1. To ensure uniqueness of an identity during the enrollment process, and
2. For authenticating identity once enrolled.

The Consultant Team is evaluating not only the need for biometrics for NIDS, but also the type(s) of biometrics that may be recommended (fingerprint, iris, facial etc.). There are also legal and cultural considerations that shall need to be addressed.

Jamaica presently operates two AFIS systems and additional biometric verification at the EOJ and JCF. Additional biometric identification solutions are used or are being considered for Passports (face recognition) and fingerprints (Firearm license), and potentially others. These platforms collect and compare biometrics. These systems are being evaluated for possible ways they can be applied – such as a pre-existing identity verification tool for NIDS, in keeping with the aim to maximize existing resources and investments.

EOJ: Fingerprints are collected at enrollment and used to ensure uniqueness on the voting register. They are also presently used at a select number of voting precincts to assert identity at the time of voting and prevent voting more than once. The use of fingerprints in the EOJ AFIS is strictly regulated by law (Representation of the People Act and also the Fingerprint Act). This limits the use of biometrics for voting purposes only and prohibits the sharing of the data.

JCF: The criminal AFIS system is used to maintain a database of fingerprints for convicted felons and latent prints from crime scenes. It is also used to perform criminal background checks for employment and other purposes. Presently, the JCF AFIS is restricted (legally) to maintaining fingerprints of convicted criminals – any other fingerprints collected for checking are erased – however, there is

proposed legislation that will also allow the storage of certain types of non-criminal fingerprints.

4.5 DIGITAL SIGNATURES AND ELECTRONIC IDENTITY

A digital identification framework to enable digital signatures for electronic transactions and other purposes are increasingly being implemented and/or on the road-map for many National Identification schemes worldwide. Most common implementations are based on a Public Key Infrastructure (PKI) allows an identity to be securely used as an on-line ID or off-line ID and as a physical ID (card). The Trade Board has stood up a national Certificate Authority based on a Public Key Infrastructure in support of the Electronic Transactions Act. The Consultant Team is evaluating the efficacy of this PKI to be included as a feature of NIDS, and if this should be considered or accommodated as a future upgrade.

Enabled by the Electronic Transactions Act passed in 2006, the Trade Board serves as the Certification Authority within the country. Equipment is installed and in place but presently supports only a sparse number of digital certificates (understood to be 1,000

eGovJa uses VeriSign digital certificates to secure public and Internet facing web applications using SSL.

4.6 ID CARDS

Should there be a NIDS ID card? Currently individuals have been issued and possess a number of identity documents ranging from low cost, paper documents, laminated paper or plastic cards to Passports. Today there are no smart cards in use. Consideration shall be given to global best practices and intentions for issuing a NIDS card. Options and a recommendation will be provided as part of the Concept Design.

If a multipurpose NIDS ID card is to be issued, will assess if document issuing stakeholders and existing resources can be leveraged and used subject to minor modifications.

4.7 STANDARDS

The use of standards provides a mechanism to allow for interoperability between systems. The best illustration of this is the Internet, which allows connectivity between disparate systems and vendor products. There are a variety of standards needed for ID systems covering multiple areas including security, unique identifiers and secured communication protocols.

For interoperability of identification information, including a photographic image, biometrics, digital certificates, etc. will need to adhere to standards across all ID stakeholders. Standards are not used to dictate specific hardware or software; they provide a set of criteria to be met so systems can be interoperable and promote competitive sourcing.

4.8 ICT INFRASTRUCTURE

A robust communication infrastructure, built on existing capabilities, is essential to support the efficient delivery of Government services. Many of the existing identity systems do not presently have electronic connectivity to other systems. Consideration will be given to provisioning a means to validate an ID as a core NIDS service; an important step to enabling a more streamlined, efficient and lower cost approach.

The NIDS ICT Infrastructure must be governed by consistent security policies (e.g. access, remote access, data security, etc.) as the cornerstone to establishing a trusted environment that encourages confident participation. Well defined and enforced policies are essential to maintain the confidentiality and integrity of data, and high availability of the systems and information on the network. The existing security policies have been provided and are being evaluated.

The concept design will highlight and illustrate the different sub components of the Identity issuance and management platform required to support the NIDS framework.

Data sharing between MDAs is beyond the scope of this assignment. However, NIDS will need to consider a framework that can support data sharing and policies both across government and with the private sector.

4.9 LAWS AND LEGISLATION

Legislation currently governs all the frameworks for present identification implementations. An in-depth analysis of legal environment applicable to NIDS (such as in the use of biometrics, data sharing, digital signatures, etc.), is being conducted concurrently with this effort. The legal and technical frameworks must be aligned.

At the direction of the project manager, the Consultant Team shall liaise with NIDS Legal Consultancy to assure a legally compliant solution is described.

4.10 ROI & SUSTAINABILITY

Stewardship and active governance of NIDS is essential to ensuring long term sustainability and success for the program.

An ROI and cost savings model will be based upon two major drivers – cost savings through the streamlining of duplicative efforts and costs that could be avoided or reduced and revenue generation through an online NIDS verification service – a service that will allows both the MDAs and private sector to use NIDS to validate / verify a presented identity.

Appendix A: eGov Jamaica Limited

eGov Jamaica Limited was operating as Fiscal Services Limited (FSL) under the Ministry of Finance until late last year (October 2013). FSL was formed as a Government-owned LLC in 1985 to perform data processing for the Ministry of Finance (MOF) in 1985. For a brief period (approximately 1 month), FSL was transferred to the Office of the Prime Minister (OPM) but was then moved back under the MOF. In 2012, the current Prime Minister, the Most Honourable Portia Simpson-Miller, proposed that FSL should again be transitioned into a government-wide resource under Ministry of Science, Technology, Energy and Mining (MSTEM). E-government is a key pillar of the Vision 2030. A NIDS solution shall be consistent with the Vision 2030, and therefore be forward looking in its design to support a future digital government. Cabinet ratified the decision in December 2012 and the transition was completed in October 2013.

eGovJa, as a central government wide capability, shall play a strong role in the implementation of a National ID solution. eGovJa senior management has visited other countries – including Chile and South Korea – and observed the positive impact a National ID platform.

A.1 Business Processes

A.1.1 Environmental Analysis

Originally known as Fiscal Services Limited (FSL), in January 2013, the Cabinet gave approval for the repositioning of the organization as the entity with responsibility for implementing Information and Communications Technology (ICT) across the Government of Jamaica.

While the initial focus was mainly on supporting critical systems of the Ministry of Finance – namely customs duties and excise, taxes and fees, etc. – much work has been done to automate many of their processes. The expanded eGovJa mission is evolving in support of its mandate "To lead the development and implementation of ICT strategies, frameworks and solutions for the Government of Jamaica to facilitate the achievement of business objectives and greater efficiency".

The main objectives of eGovJa are to:

- Optimize ICT investment across GOJ.
- Develop centralized methods of creating, managing and supporting technology across the GOJ.
- Develop standardized approaches to ICT implementation within GOJ.

- Provide efficient delivery of GOJ services to citizens and businesses.

eGovJa does not currently second people to other Agencies (other than one special case) - or vice versa (do not have the financial resources to do so). Instead, eGovJa is working to transform the way business is done by encouraging and supporting the creation of business analyst positions within the different Agencies. The analysts take ownership of defining specific requirements (will always be more expert in their own fields than eGovJa) and eGovJa interfaces with those people.

eGovJa has the experience and skillsets. They are looking for champions to help to break the "silos" across government, for which a NIDS implementation will touch every major stakeholder, and can help to accelerate the eGovJa mandate.

Presently, the eGovJa services offered are:

- ICT consultancy services.
- Data Centre Services (systems and application hosting).
- Infrastructure Design and development.
- Software acquisition and development.
- GOJ Validation Web Services.

A.1.2 Documented Existing Business Processes

Specific details of the existing business processes were not available to the Consultant Team at the time of this report and will be updated when available.

A.2 ICT Architectures

eGovJa currently hosts and supports ICT solutions for a number of government agencies, including the Jamaica Customs Agency, Trade Board and the Ministry of Finance (MOF).

In the past 5 years, the eGovJa team has been transforming from a bespoke software development shop to a broader ICT services organization. They are institutionalizing a structure for system disciplined development and implementation that is focused on best practices and standards. Their plan is to apply these standards to ICT systems government-wide, and to provide shared services and next generation solutions that ensure better outcomes for all stakeholders. In doing so, they hope to help break the current data and information “silos” that exist across the government.

eGovJa stated a focus on facilitating transactional services for stakeholders, as opposed to simply providing data services. The aim is to help government collect revenue as efficiently as possible – whether through taxes, registration fee, licenses, etc. The Tax Portal they developed facilitates online payments – and they have a vision to create a single standardized Portal that could become a single point-of-entry into the Government for multiple services and applications. eGovJa has acquired PKI knowledge and experience through the issuing and management of digital certificates in support of online payments. This experience will be important moving forward if NIDS is to be established as an online identity as well as an "inline" (physical) identity.

Another key area of focus for eGovJa has been the enabling and securing of Trade, which touches and impacts many different stakeholders across the government. A secure, common identifier – such as will be established through NIDS – is essential for reconciling identity across each of the stakeholder systems that must interact.

A.2.1 eGovJa Proposed NIDS Data Items

In 2012, eGovJa (then FSL) created a proposed data model for NIDS. The elements of this data model will be evaluated by the Consultant team against international best practices and standards in the development of a NIDS data model.

The data items proposed by eGovJa are as follows:

Column Name	Description	Type	Required	Values
NIN	National Identification Number	Integer	Y	
CURRENT NAME				
First Name	First Name	Character	N	
Middle Name	Middle Name	Character	N	
Last Name	Last Name	Character	Y	
Alias Name	Alias	Character	N	
NAME AT BIRTH				
First Name	First Name	Character	Y	
Middle Name	Middle Name	Character	Y	
Last Name	Last Name	Character	Y	
Changed Via	Means by which name was changed	Character	N	Marriage, Deed Poll,

Column Name	Description	Type	Required	Values
				etc.
Date of Change	Date on which change was effected	Date	N	
Sex	Sex	Character	Y	
Gender Remarks	Comments on gender issue	Character	N	
Date of Birth	Date of birth	Date	Y	
Remarks	Notes on date of birth accuracy	Character	N	
MOTHER'S/FIRST GUARDIAN DETAILS				
NIN	National Identification Number	Integer	N	
First Name	First Name	Character	Y	
Middle Name	Middle Name	Character	Y	
Last Name (Maiden)	Last Name	Character	Y	
Relationship	Relationship to individual	Character	Y	Mother Guardian Adopted Mother Stepmother
FATHER'S/SECOND GUARDIAN DETAILS				
NIN	National Identification Number	Integer	N	
First Name	First Name	Character	Y	
Middle Name	Middle Name	Character	Y	
Last Name	Last Name	Character	Y	
Relationship	Relationship to individual	Character	Y	Father Guardian Adopted Father Stepfather
Place of Birth	Place of birth	Character	Y	

Column Name	Description	Type	Required	Values
Town of Birth	Town of birth	Character	N	
Parish/State of Birth	Parish/State of Birth	Character	Y	
Country of Birth	Country of birth	Integer	Y	
Nationality	Country of which person is a national	Character		
Marital Status	Marital Status	Character	Y	S=Single; M=Married; D=Divorced; P=Separated; W=Widowed; C=Common law
SPOUSE DETAILS				
NIN	National Identification Number	Integer	N	
First Name	First Name	Character	Y	
Middle Name	Middle Name	Character	Y	
Maiden Last Name	Last Name (Maiden)	Character	Y	
LAST KNOWN ADDRESS				
Mark	Mark that identifies address	Character	N	
Street Number	Street Number	Character	N	
Street Name	Street name	Character	N	
Town Name	Town Name	Character	Y	
Parish/State	Parish/State	Character	Y	
Country	Country of residence	Integer	Y	
Zip/Postal Code	Zip/Postal Code	Character	N	
Date of Residence	Date on which residence was done at address	Date	N	
BIOMETRICS				
Photograph	Picture	Blob	Y	
Date photographed	Date photograph was taken	Date	Y	

Column Name	Description	Type	Required	Values
Finger Print	Finger Print	Blob	N	
Date finger-printed	Date finger-print(s) were taken	Date	Y	
Status of Person	Status of individual	Character	Y	A=Alive, D=Deceased, etc.
Status Date	Date at which status applies	Date	N	

A.2.2 ID Database Designs

eGovJa (as FSL) performed an analysis of databases and data models used by TRN, EOJ, RGD, NIS and PICA and developed a mapping of those fields against each other and to their proposed NIDS data structure.

Details of this analysis is available to the Consultant Team and is being analyzed. It has not been replicated in this report.

A.2.3 ID System Architectures

Specific details of the Identity databases and ICT architectures were not available to the Consultant Team at the time of this report and will be updated when available.

A.3 Network Security

During the course of the eGovJa and other agency high-level assessment by the Network Security Consultant the following areas were considered throughout the process:

- Policy
- Enforcement
- Physical security (e.g., CCTV surveillance, security guards, protective barriers, locks, access control protocols, others.)
- Logical security (i.e., authenticating a user's privileges on a computer network or system)
- Auditing

Network Security encompasses an organization's strategy and provisions for ensuring the security of its assets and of all network traffic; the implementation is through security policy, hardware, and software.

Policy plays an important role in each organizations network security strategy and is composed of multiply security areas that cover both physical and logical access to systems. Policy cannot be effective without enforcement and routine auditing (annually, semiannually, etc.) helps determine if the organization is in compliance with its policies.

Physical security is designed to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage.

Logical security is the process of using hardware and or software techniques for authenticating a user's privileges on a specific computer network or system. The Confidentiality, Integrity and Availability (CIA) of data must be protected and this is a first line of defense into the systems.

Some common compliance standards for Network Security can include, but are not limited to the list in
Table 1: Common Security IT Standards.

Standard Name	Description
ISO 27001	Specifies a management system that is intended to bring information security under explicit management control.
ISO/IEC 20000	International standard for IT service management.
ISO/IEC 21827	International Standard based on the Systems Security Engineering Capability Maturity Model (SSE-CMM) that can measure the maturity of ISO controls objectives
ISO 15408	Known as Common Criteria
RFC 2196	A memorandum published by Internet Engineering Task Force for developing security policies and procedures for information systems connected on the Internet focusing on day-to-day operations.

TABLE 1: COMMON SECURITY IT STANDARDS

A.3.1 NETWORK AND SECURITY ANALYSIS

A site visit of eGovJa took place on Tuesday, January 14, 2014.

Physical security is addressed through a layered approach at the eGovJa facilities with security guards, razor wire around the fence perimeter, and security cameras. Everyone who enters the facility is required to sign in/out at the front guard desk. Only authorized designated personnel are allowed into the computer data center area, and for others only escort provided access to the server systems, access requires a fingerprint scan for entry.

eGovJa already supports multiple agencies systems and has developed policies, procedures and processes to ensure the highest level of service and security for its clients. The Network Security Consultant was supplied policy documentation covering many areas of security. eGovJa is able to provision Infrastructure as a service (IAAS). IAAS is a model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. This model shifts some of the security to the provider and thus eGovJa must maintain a well-defined model to support the security of the data center.

A.3.2 Documented Existing Information Security Policies

The Network Security Consultant was provided the following security policy documents listed in the table below:

Policy Name	Current Version	Revision Date
eGovJa - Email Policy (February 2013)	0.3	21.02.2013
eGovJa - Internet Policy (March 2010)	0.2	27.05.2010
eGovJa - IT Usage Policy (Nov 2013)	0.3	20.11.2013
eGovJa - Password Policy (March 2010)	0.1	19.03.2010
eGovJa - Physical Access Control Standards & Procedures (Nov 2013)	0.3	20.11.2013
eGovJa - Remote Access Usage Policy (Nov 2013)	0.3	20.11.2013

TABLE 2: EGOVJA SUPPLIED POLICY DOCUMENTATION

Each of the policies provided had a consistent format throughout the documents provided and had a straight forward approach to describing the topic at hand. The documents also mention under the “Contact Information” heading on page 2, that there was “a variety of standards, procedures, guidelines and other materials supporting and expanding upon this and other information security policies are available in the organization’s “Information

Security Manual. The "Information Security Manual was not available to the Consultant Team at the time of this report which will be updated when available.

All policy documents stated the control owner as the Security & IT Risk Management Department and were available through the information Security Manager and on the corporate intranet but none had the signature of the Managing Director on the last page. In the "Related Policy, Standards, and Guidelines" table in the back of each of the documents there were no international standards (e.g., ISO, IEC, ITIL, etc.) or country regulations listed other than references to other polices and the "Human Resource Code of Conduct". There is an expectation that country laws relating to privacy, data retention and others will be listed in this area when available. The documents do make a statement regarding Monitoring and Auditing to stay in compliance with the particular policies.

A.3.3 DOCUMENTED COMPLIANCE STANDARDS

Specific details of Compliance Standards were not available to the Consultant Team at the time of this report and will be updated when available.

Appendix B: MINISTRY OF LABOUR & SOCIAL SECURITY

NATIONAL INSURANCE SCHEME (NIS)

The National Insurance Act was passed in 1965 and implemented on April 4, 1966, giving birth to the National Insurance Scheme (NIS). NIS is a compulsory contributory funded social security scheme and requires all persons between the ages of 18 and 70 who are gainfully occupied in insurable employment to be registered and contribute to the Scheme. Qualification for NIS benefits requires fulfillment of the conditions defined by the National Insurance Act. Contributions paid to the NIS are invested by the National Insurance Fund (NIF) in real estate, money and equity markets. The NIF deposits money to various banks accounts to facilitate benefit payments on receipt of requests from the Fund Accounts Unit.

NIS makes several types of benefit payments / grants including:

- Maternity Allowance
- Orphan Pension
- Employment Injury Cash Award
- Invalidity Pension
- Retirement Grant
- Widows'/Widowers' Pension
- NI Gold (health insurance)
- Special Child Pension
- Orphan Grant
- Employment Injury Disablement Pension
- Invalidity Grant
- Spouse Allowance
- Widows'/Widowers' Grant
- Special Child Grant
- Employment injury Medical Treatment
- Employment Injury Death Benefit
- Retirement (Old Age) Pension
- Funeral Grant
- Special Anniversary Pension

Citizens and legal residents are required to register with NIS at the age of 18 at which time an NIS is issued – not everyone registers, partly due to a distrust for government and "informality" – wishing to remain under the radar. An IDB study estimated that only 30%-40% of the workforce are contributing to NIS. NIS also recognizes that there is some fraud and abuse within the system that would benefit from NIDS to create a more verifiable means of identity.

NIS performs "proof-of-life testing" every 6 months where a notice is mailed to a benefit recipient and must be validly signed and returned to affirm continued eligibility to receive the benefit. This involves over 100,000 pensioners (over 99,000 pensioners in Jamaica, the rest overseas) and is a costly and time-consuming process that could significantly benefit from NIDS.

There are also a number of other life-event indicators that cannot currently be accessed automatically, including:

1. Notification of death events to trigger death benefits and/or to cease payment of retirement benefits.
2. Birth data from the Civil Registry which is necessary to determine age for retirement benefits, etc.

The challenge to MLSS /NIS is global since they pay benefits to Jamaicans all over the world.

PATH

The Programme of Advancement Through Health and Education (PATH) is a conditional cash transfer program under MLSS, funded by the Government of Jamaica and the World Bank. It is aimed at delivering benefits by way of cash grants to the most needy and vulnerable in the society. PATH was introduced island-wide in 2002. PATH currently has 382,000 active beneficiaries (in approximately 40,000 households) with approximately 720,000 registrations in the database.

B.1 BUSINESS PROCESSES

B.1.1 ENVIRONMENTAL ANALYSIS

MLSS Functions:

1. Provides Grants (max $50K) for:
    - Compassionate Assistance.
    - Small Business Assistance.
2. Uses the TRN as the personal identifier.

PATH

The Programme of Advancement through Health and Education (PATH) provides cash transfers to poor families, who are subject to comply with conditions that promote the development of the human capital of their members. It has four main objectives, as follows:

- To alleviate poverty by increasing the value of transfers to the poor;
- To increase educational attainment and improve health outcomes of the poor by breaking the intergenerational cycle of poverty;
- To reduce child labour, by requiring children to have minimum attendance in school;
- To prevent families from falling further into poverty in the event of an adverse shock.

PATH was created in 2001, as part of a wide-ranging reform of the welfare system carried out by the Government of Jamaica (GoJ) with support from multilateral institutions. The aim has been to replace the former system, consisting of food stamps, outdoor poor relief and limited public assistance, with a single CCT programme.

PATH uses its own unique registration number for applicants:

- Central system first generates a number upon application for assistance.
- Part of the number identifies where the person is resident at the time of application.
- Manual vetting of the applicant details.
- A unique PATH number is first assigned to a family and then each family member is assigned a derived version of that number (e.g. -1, -2).
- Applicant details are manually vetted and a “needs score” is statistically generated and then validated by a social worker in the field.
- Benefits provided are conditional upon such things as attending clinics on a pre-specified basis, etc.
- The ID stays with the person for life.

PATH would benefit from using NIDS not only to check what other benefits are being received – this affects what they might be eligible for under PATH, but as well to link family members together. There are efforts currently directed in an initiative to link PATH with the MOE student ID number database regarding school meals.

NIS relies on "self" reporting of deaths: There have been attempts and initiatives to electronically link to the RGD system regarding deaths but have encountered both operational and legal impediments as well as data privacy issues.

National Insurance Scheme

The National Insurance Scheme was developed to meet the social security minimum standards of the ILO (International Labour Organization) to offer financial protection to the worker and his or her family against loss of income arising from injury on the job, incapacity, sickness, or retirement.

It requires all persons between the ages of 18 and 70 who are occupied in insurable employment to register with NIS; each applicant is issued a NIS number. But not everyone registers: NIS representatives indicated that a prior IDB study had estimated that only 30%-40% of the workforce are participating in NIS.

"Informality" is one of the greatest challenges to participation (across all systems and frameworks): Jamaican culture is an informal one. Many prefer to remain “informal” – under the radar and especially those in the population at risk do not grasp the reality of early contribution for a pay later benefit if needed. A culture change is needed regarding contributing to Pensions.

There is some fraud and abuse of the system and NIDS may help to reduce this fraud.

NIS periodically (rate to be confirmed) sends the National Housing Trust (NHT) a list of valid NIS numbers on a DVD to allow them to check for valid NIS numbers used on NHT applications.

NIS is currently revising application forms to require a photo ID and a TRN – this is not yet implemented, and there is no defined timeline when it will be completed.

Work Permits

MLSS Grants work permits to British Commonwealth citizens, CARICOM nationals and others who do not otherwise qualify for a work permit.

- Requires a TRN to apply.
- Separate ID number for work permits, stored in separate database.
- Approx. 3,000 issued per year plus 1,800 exemptions.
- Duration ranges from 3 months to 3 years.
- Will keep the same ID number if the permit is renewed to continue working at the same company.

Work Permits are now recently computerized, the new system is currently being populated.

B.1.2 Documented Existing Business Processes

Specific details of the existing business processes were not available to the Consultant Team at the time of this report and will be updated when available.

B.2 ICT Architecture

B.2.1 MLSS ID Numbers

The Consultant Team identified several registration and pension identification numbers assigned by the MLSS to clients. In some cases, different registration numbers are assigned to companies and individuals. Pension numbers are only assigned when an application is made for benefits.

Among the numbers identified are:

1. National Insurance Number (Individual)

The National Insurance number is made up of a letter and six numerals, for example, Q663457. The number assigned to each registrant is determined as follows:

- First Digit (Letter): Denotes the parish in which the individual registered with the NIS.
- Second and Third Digits (Numerals): Denotes the individual's year of birth.
- Fourth Digit (Numeral): Denotes the sex of the individual.
- Fifth Digit (Numeral): Denotes the type of work/industry.
- Sixth and Seventh Digits (Numerals): Assigned sequentially by the electronic system.

2. National Insurance Number: (Employer)

This is assigned to companies/businesses when they register with the NIS. It is made up of seven numerals and is determined as follows:

- First Digit (Numeral): Automatically assigned by the electronic system.
- Second and Third Digits (Numerals): Denotes the industry code.
- Fourth through Seventh Digits (Numerals): Sequentially assigned by the electronic system.

3. Pension Number

The pension number is made up of seven numerals and a letter, for example, 1512348G. It is determined as follows:

- First Two Digits (Numerals): Represents the year in which the application was submitted.
- Third Digit (Numeral): Represents the benefit type and sex of the claimant.
- Fourth through Seventh Digits (Numerals): Sequentially assigned by the electronic system.
- Eighth Digit (Letter): Represents the payment cycle. There are six payment cycles, each represented by the different letter.

There are a number of variations with identity numbers associated with the payment of other benefits, including:

4. Sugar Workers Pension

The letter assigned does not denote the payment cycle; it represents the type of benefit.

5. Funeral Grant

The number is slightly different, for example, 66F2430Z:

- The first two digits denote the year in which the application was made.
- The 'F' represents Funeral Grant.
- The subsequent four numbers are assigned by the electronic system.
- The final 'Z' denotes a benefit without a benefit cycle.

6. Employment Injury Benefit

The number is similar to the Funeral Grant, for example, 65E0841Z.

- The first two digits denote the year in which the application was made.
- The 'E' represents Employment Injury Benefit.
- The subsequent four numbers are assigned by the electronic system.
- The final 'Z' denotes a benefit without a benefit cycle.

7. Maternity Allowance

The number is similar to the Funeral Grant and Employment Injury Benefits, for example, 65M09372Z.

- The first two digits denote the year in which the application was made.
- The 'M' represents Maternity Allowance.
- The subsequent four numbers are assigned by the electronic system.
- The final 'Z' denotes a benefit without a benefit cycle.

8. PATH applications have a unique 9-digit number:

Central system generates the number upon application for assistance.

- Part of the number identifies where the person is resident at the time of application.
- The ID stays with the person for life.
- A unique PATH number is first assigned to a family and then each family member is assigned a derived version of that number (e.g. -1, -2).

B.2.2 ID Database Designs and Data Models

For some time, MLSS has been making provision for a common NIDS identifier in their system database upgrades – currently that database entry is being populated with the TRN number.

eGovJa (as FSL) performed an analysis / mapping of database designs / data models in NIS and mapped the fields against other databases and the proposed NIDS data structure. Details of this analysis are available to the Consultant Team and is being analyzed. It has not been replicated in this report.

Further details of the Identity databases and ICT architectures were not available to the Consultant Team at the time of this report and will be updated when available.

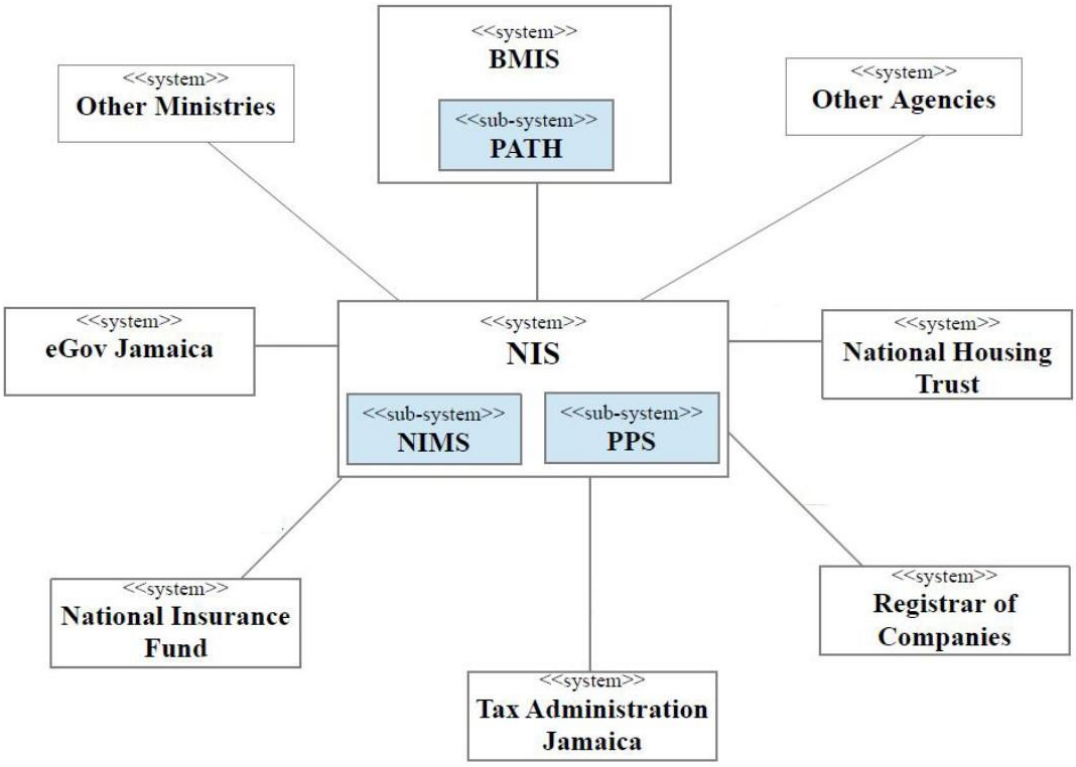
B.2.3 MIS System Architecture & Interfaces

There are several identity "silos" within MLSS and NIS internally and they are very interested in being able to accurately identify clients both internally and in liaison with other government MDAs (e.g. RGD, TAJ, PICA, etc.) in order to reduce costs and improve accuracy and efficiency. There currently have no electronic links with other MDAs that would allow identity reconciliation and cleanup of their own databases which they acknowledge as not being entirely accurate.

The NIS Management Information System (MIS) consists of two separate database systems, the National Insurance Management System (NIMS) and the Pension Payment System (PPS). PATH employs a separate Beneficiaries Management Information System (BMIS).

To operate efficiently and effectively, NIS must interface with a number of other MDAs. There is currently no MDA or other organization that electronically interfaces with the NIS for the purpose of the exchange of data. However, data is indirectly (manually) exchanged (period / frequency to be determined). There are challenges with accurately resolving identity between systems which would be improved with the introduction of a NIDS. The TRN is used (when available) to help resolve identity although the TRN database is acknowledged to have inaccuracies.

The figure below illustrates the current high level architecture for the exchange of data – note that the paths shown are illustrative and may not indicate an electronic connection.



Source: *Information Technology Diagnosis of the Jamaican National Insurance Scheme Final Report C.C.R. Busby-Earle PhD Computer Science, CEH, January 3, 2014,*

Below is a summary of the primary agencies provided by NIS with whom they currently interface, or anticipate the need to interface in the future:

1. <u>Tax Administration Jamaica (TAJ) (through eGovJa):</u>
   a. TAJ collects NIS payments throughout its network of Tax Collectors island-wide.
   b. TAJ uses the Integrated Computerized Tax Administration System (ICTAS) to manage NIS and other statutory payments.
   c. Data on NIS payments is uploaded by TAJ each night via a web portal hosted by eGovJa.
   d. NIS payment data is then downloaded from the site the next day and uploaded to the Ministry's NIS Payments System.
   e. The Taxpayer Registration Number (TRN) data is also stored by FSL and TRN's are an integral part of the NIS database

2. <u>National Housing Trust (NHT):</u>

a. Employers' Annual Returns are either submitted online using the TAJ Online portal or are submitted in hard copy using the Employers' Annual Return Form (S02) at TAJ or NHT offices.
b. Hard copy S02 forms are scanned and the data is extracted by a contractor - Xsomo International Limited for NHT.
c. An interface is essential with TAJ's ICTAS system for seamless transition of electronic data and so that the scanned S02s may be viewed online.

3. Companies Office of Jamaica (COJ)
   a. COJ will soon become a one-stop registration centre for the registration of all companies and business names in Jamaica.
   b. Registration data will also be captured to allow the generation and issuance of NIS Reference Numbers for these entities
   c. A system is under development to capture the COJ data, generate the NIS Reference Number and propagate it to other MDAs.

4. Registrar General's Department (RGD)
   a. NIS relies on proof of birth for the registration of contributors and to determine eligibility for benefits.
   b. NIS needs accurate and timely information on deceased beneficiaries in order that payments may cease and/or to determine eligibility for other benefits.
   c. An electronic interface with the RGD system and a means of accurately identifying contributors / beneficiaries (such as through NIDS) would make these processes more efficient and help reduce costs.

5. Programme of Advancement Through Health and Education ((PATH)
   a. An NIS pensioner who lives in a PATH household is not eligible to receive a PATH benefit. The NIS system would therefore benefit greatly from being able interface with PATH's Beneficiary Management Information System (BMIS) and the PATH Poor Relief System to identify and prevent the payment of duplicate benefits.

6. Ministry of Finance and Planning (MOFP)
   a. MOFP is currently planning a comprehensive automated Pension System for the capture of data on GOJ employees in order that this information may be stored electronically to ensure efficient processing of GOJ pension benefits.
   b. This system is intended to be utilized across the various MDAs.
   c. The data to be collected for civil servants is similar to the data used by the NIS.

d. Additional benefits may accrue from having the NIS and MOFP systems interface with each other.

7. National Insurance Fund (NIF)
   a. NIF currently utilizes an Investment System but there is no electronic link between this system and the collections or benefits data from the NIS.

B.3 NETWORK SECURITY

The site visit for Ministry of Labour & Social Security – National Insurance (NIS) took place on Tuesday, January 14, 2014. The discussion with the stakeholders delved deep into business processes about registration and the organizations that are closely tied together.

The MLSS/NIS operates many databases with no physical connection between the systems. As an example the National Housing Trust (NHT) checks for valid NIS numbers using a DVD provided by NIS. Transporting data through physical media has security implications that can be difficult to protect, this is not to say that transporting data over a network is safer but there is more control.

The "Information Technology Diagnosis of NIS" IDB final report has information that provides details on security topics relating to their data center.

B.3.1 NETWORK AND SECURITY ANALYSIS

NIS provided an "Information Technology Diagnosis of NIS" IDB final report (completed January 3, 2014) which covered many areas regarding IT Systems, Operating Environment, External Data Exchange and security related topics. The report also contained pictures of the systems and the environment.

Based upon the discussion with the stakeholders and the provided report it appears NIS has a good understanding of their strong points and weak points regarding network security. Security policy has been created although it may still be in draft form and the pictures provided in the report show a secure physical environment.

B.3.2 DOCUMENTED EXISTING INFORMATION SECURITY POLICIES

The "Information Technology Diagnosis of NIS" report provided a summary of the NIS IT Policies listed as a draft Version 1. The policies covered the following areas:

- Summary of Main Security Policies

- Virus, Spyware & Malware Protection
- Physical Security
- Access Control
- LAN Security
- Server Specific Security
- Unix and Linux Specific Security
- Wide Area Network Security
- TCP/IP & Internet Security
- Purchasing, Development and Maintenance of Software

There were many policy areas covered in the report but none of policies appeared to be broken into an individual documents. There may in fact be individual policy documents but they were not provided to the Network Security Consultant.

Policy Name	Current Version	Revision Date
Ministry of Labour & Social Security: IT Policy (Draft)	1.0	April 2008

TABLE 3: NIS SUPPLIED POLICY DOCUMENTATION

B.3.3 DOCUMENTED COMPLIANCE STANDARDS

Specific details of the Identity databases and ICT architectures were not available to the Consultant Team at the time of this report and will be updated when available.

Appendix C: JAMAICA CONSTABULARY FORCE

The Jamaica Constabulary Force (JCF) has a criminal Automated Fingerprint Identification System AFIS) from Morpho that was commissioned in October 2006. The system is capable of capturing fingerprints (10-prints), palm prints and latent fingerprints from crime scenes. It has a capacity for 1.2 million sets of 10-prints with approximately 370,000 sets stored in the database at the current time. The AFIS can also capture / store latent fingerprints taken from crime scenes and presently holds approximately 10,800 on file.

The AFIS is restricted (legally) to maintaining fingerprints of convicted criminals – the fingerprints collected from non-convicted felons are erased following the check against stored prints. There is proposed legislation that will allow the storing of certain non-criminal fingerprints in the system, maintained in a separate database from those of convicted criminals.

In addition to its use in the justice system, the AFIS is also used to perform criminal background checks for employment and other purposes. More than 100,000 background checks are performed each year with Police Certificates issued to those who pass the check.

There are thought to be a number of issues to be overcome if the JCF AFIS was to be considered for use as part of the NIDS system:

- Current legislation does not permit the use of the JCF AFIS for civilian purposes. The AFIS use is governed by the 2005 Fingerprint Act.
- JCF does not have the physical space to host the enrollment, vetting, card production / issuance, etc. requirements for NIDS.

C.1 BUSINESS PROCESSES

C.1.1 ENVIRONMENTAL ANALYSIS

The JCF commissioned a criminal AFIS System in October 2006. The capacity is for 1.2 Million sets of 10 prints and the system has currently 370 k ten print records in the database:

- JCF only maintain criminal prints in the database – others are deleted following a check. Officers capture 10 prints and palms.
- Non-convicts in the future are anticipated to be maintained in a separate database.
- Performs >100,000/year background checks for other Government Agencies and for employment

- Issue Police Certificates following successfully clearing the AFIS check.

JCF also uses the AFIS to perform background checks for Firearm licensing.

Over 800 crime scenes have been solved thanks to the AFIS since 2006.

Based on the latest JCF report 2012, fifteen police personnel and twenty one civilians have been trained in the use of the AFIS system; ninety seven police personnel have been trained in the use of the MORPHO RapID platform.

All the activities are Governed by the 2005 Fingerprint Act place specific limitations and constraints on the information which can be stored and who can access these records.

At this stage, the use of JCF AFIS for civilian purposes will require a change of the Fingerprint Act, and a major investment to increase the system capacity. In addition, if JCF were to keep all the captured prints of people who presented themselves for the police certificate, it would also require a change in the Act.

C.1.2 Documented Existing Business Processes

Specific details of the existing business processes were not available to the Consultant Team at the time of this report and will be updated when available.

C.2 ICT Architecture

The JCF AFIS database is mirrored offsite to another JCF location using a secure network. On-site and offsite backups are routinely performed.

Further details of the ICT architecture and database were not available to the Consultant Team at the time of this report and will be updated when available.

C.3 Network Security

C.3.1 Network and Security Analysis

The site visit for the JCF took place on Tuesday January 14 and included a review of their automated fingerprint identification system (AFIS) as well as a demonstration of the system.

A technician demonstrated the physical process of how JCF enters fingerprints into the systems being used.

The system only maintains criminal prints in the database; others are deleted following a check. Fingerprint Image capture is 10 prints and palm. The database is mirrored offsite to another JCF location through a secure network and backups are made. The system is governed by the 2005 Fingerprint Act.

C.3.2 Documented Existing Information Security Policies

Based strictly on the onsite visit it appears the JCF does have both policy and procedures to handle networking and security related items. Areas were designated for processes such as fingerprint analysis and fingerprint capture as well as physical security to limit the access of unauthorized personnel. A demonstration of how individuals are fingerprinted utilizing their AFIS systems shows a well thought-out process.

Through discussion, it was determined that the JCF systems in place were both backed up and redundancy was in place to handle availability issues.

Specific details of the Information Security Policies were not available to the Consultant Team at the time of this report and will be updated when available.

C.3.3 Documented Compliance Standards

AFIS systems by their nature adhere to best practices and international standards for image quality and data exchange formats. Upon visual inspection physical security, logical security and auditing procedures and processes do seem to be in place.

Specific details of Compliance Standards were not available to the Consultant Team at the time of this report and will be updated when available.

Appendix D: TAX ADMINISTRATION JAMAICA

D.1 BUSINESS PROCESSES

D.1.1 ENVIRONMENTAL ANALYSIS

Tax

The Taxpayer Registration Number (TRN) is a unique identification number assigned to all taxable entities namely: individuals, sole proprietors and organizations for facilitating business transactions with the Tax Departments.

The main purpose of the TRN is to:

- Uniquely identify each taxpaying entity which interacts with the Revenue Departments.
- Facilitate the establishment of relationships between taxpaying entities which will facilitate the reconciliation of accounts and integrate the assessment of all taxes.
- Improve the services to the taxpayers by using the TRN as a link among the systems within the Revenue Services.
- Facilitate tax type registration, account and ledger closure, updating registration details and printing certificates and reports.

Implementation of the use of TRN commenced November 1996. At this point a TRN was required for businesses and individuals to complete some transactions at the Revenue Departments. The first individual TRN was generated on July13, 1996.

A TRN can either be “Confirmed” (Requirements for application was met and for which use is not limited) or “Provisional” (use is very limited as it cannot be used to do transactions such a motor vehicle transactions, customs clearance etc.). A provisional TRN is issued when the applicant has not fulfilled all the requirements. This expires three months after issue (expiry date can be extended further). Provisional TRNs are confirmed when missing information/document is provided.

Initially applications received were batched and assigned a batch number. Most of the batches were then sent to an external entity (eGovJa) for data entry. After the batches were data entered a process would be run each night to generate TRNs for the applications that

were contained in batches providing they were verified and there was no matches or other incomplete data. At implementation in November 1996 the Taxpayer Registration Centre and some of the larger Tax Offices were linked to the TRN database at FSL therefore allowing for the online assignment of TRNs.

Over the years several changes took place:

1996 TRN was implemented.

1998 The exclusion of Electoral/Voter's/National Identification as a standalone form of identification.

1998 November – addition of a "date Received" field to the TRN System. Previously "date assigned" field was present on the system but it was recognized that the system also needed a date received field.

2001 April – addition of a birth certificate number field (previously birth certificate numbers had to be entered in the other documents or remarks section of the System).

2002 All applicants that used certified photographs as part of the requirements for TRN were required to leave those photographs as part of the archived file for that applicant.

2002 August – modifications to the TRN Application forms were completed and gazetted.

2004 Major enhancements were done to the system which included for its capability to allow the user to modify the names of applicants being matched in database during assignment of TRNS.

2009 Modifications were made to the system to enforce automatic matching of names for new applicants with existing applicants in the database with the same names and date of births within three years of that of the applicant.

2011 September – supporting documents were required to be photocopied and attached to applications.

2013 June – declarations by certifying officer became part of the requirements for new applicants using certified photographs as a form of identification.

TRN was initially implemented for use within revenue departments. However, there has been expansion in use to other Government and Non-Government entities over the years of its existence. Current uses of the TRN include:

- All payments at Tax Offices (except for cash payments for Property Tax which is currently being implemented).

- Identifier for persons receiving payments via most of the government accounting systems.
- Part of the requirements for a number of social, financial and health benefits including: Programme of Advancement Through Health and Education (PATH); National Health Fund (NHF) and Student's Loan.
- The implementation of NHF in 2003 lead to a high number of minors and retired individuals who were not taxpayers acquiring TRN.
- Needed to acquire a Tax Compliance Certificate (TCC).

Now the TRN application is part of a "One Stop" business registration process at the Companies Office of Jamaica where entities receive Business/Company Registration and registration for TRN, National Insurance Scheme (NIS), and National Housing Trust (NHT).

Uses also include:

- Required at financial institutions to open accounts, money transfers, loans and other financial transactions. It will be a critical part of the information that the first Credit Bureau formed in Jamaica will use.
- Part of the Enrollment process in the major tertiary institutions of learning, as well as for the HEART training program.
- Driver's license identification number.
- Requested as a Personal identification number for purchase of cellular phones from the local telephone providers.

There are approximately 100,000 new TRNs created per year:

- The death rate is approximately 25,000/year but data is difficult to collect and validate to closeout a TRN.

A TRN a paper card is currently issued, currently issuing 7,000-12,000 per month.

TAJ Believe NIDS could big help in streamlining the ID validation at enrollment (including the use of biometrics).

Space and personnel are significant issues for TAJ, particularly related to the storage of paper TRN applications.

- In the process of procuring a Document Management System to begin the process of capturing/storing the applications electronically.
- Propose to eventually scan everything at enrollment.

Driver's License

An upgrade is in the process of being planned to the De La Rue Driver's License system – needs have been identified but there are no plans for implementation yet.

Currently the DL office uses the TRN as the Driver's License number but maintain a separate database. The Driver's License also has a unique document number ("Control #").

Card is printed on Teslin, manually die cut and laminated on site.

- Process managed by the De La Rue MIDIS system.
- Last updated in 2008 – "due an upgrade" to both software and hardware.
- May go to market for a new solution.
- Potential to combine with another tax system to cut costs.

Applications are stored in paper format: a proposal is developed to be included as part of the Document Management System project at TAJ;

The Barcode on the DL contains the TRN # and a unique sequential Control #

Banks typically ask for a DL or a Passport as a photo ID.

- If a Voter's ID is presented, another supporting document is typically required.
- Web services allow organizations to validate a presented Driver's License:
  - Fee for service.
  - Revenue goes to eGovJa, not TOJ.

General Comments from TAJ

There may be reluctance for people to sign up for a National ID:

- There was initially strong resistance to the TRN.
- There may be even more resistance to NIDS if biometrics are used.
- Issues are cultural and religious e.g. have to be very careful that no TRNs or other identification documents issued which contain superstitious numbers e.g. a '666' number sequence.

D.1.2 Documented Existing Business Processes

TRN

There are 29 Tax Registration Offices throughout the country, plus the Head Office that also accepts applications. Applications are made at Tax Registration offices.

- Data entry is performed at the point of registration.
- 2-person enrollment – both have to review/sign-off on the application.
- Additional review (QC) performed at the central facility – all applications sent there for number/card issuance.
- Receipt given to the applicant.
- Enrollment requires a birth certificate.
  - Perform a visual inspection of the birth certificate and a uniqueness check against birth certificates already stored in their database.
- Process does not currently require a photo to be taken at enrollment.
- 60%-70% of applications include a photo ID Document.; voter's ID is the document of choice for most of the applicants
- If no photo ID is available, will accept a photo certified by a Justice of the Peace.
- Photocopy the provided photo or photo ID is made (if possible).
- Maintain paper copies of all applications at the Card Center.

Cards (paper card laminated) are printed at the Card Center and distributed back to the Tax Registration offices.

- In-person collection required unless an overseas application (card is mailed).

<u>Driver's License</u>

Application Process:

- Apply at DL office.
- Pay fee.
- Take test (at Island Traffic Authority).
- Form submitted directly back to the DL office.

License is issued by the DL office.

- Printing performed at a central location in Kingston.
- Instant issuance at that location.
- All other regional locations send the completed documentation to the central office – license is printed and returned to the regional location for in-person pickup.
- DL Office is issuing 140-150/day in Kingston, an additional 300/month for the regional centers.
- License is valid for 5 birthdays.

Renewals are currently automatic upon application (and payment):

- Discussing the need for competency testing prior to renewal.
- Currently no upper age limit.

D.2 ICT ARCHITECTURE

D.2.1 ID SYSTEM DATA MODELS

TRN

9-digit number is assigned to all taxable entities namely: individuals, sole proprietors and organizations for facilitating business transactions with the Tax Departments.

- Allows unique identification of each taxpaying entity.
- Includes a check digit (mod 11).
- The domain of TRNs is divided into two – Business TRNs and Individual TRNs
    - Business TRNs range from 0 – 99,999,999
    - Individual TRNs range from 100,000,000 – 999,999,999
- TRNs with three consecutive sixes (pattern *666*) are not issued due to prevailing public religious perspectives
- The TRN is normally represented using the format "### - ### - ###".
- Possible to have subsidiary numbers (denoted by a suffix e.g. -1, -2, etc.)

The data model supports both a "Confirmed" and a "Provisional" status"

- "Confirmed" indicates that all requirements for application were met
    - Use of a "Confirmed" TRN is not limited
- "Provisional" TRN is issued when the applicant has not fulfilled all the requirements.
    - Use of a "Provisional" TRN is very limited – it cannot be used to do transactions such a motor vehicle transactions, customs clearance etc.
    - A "Provisional" TRN expires three months after issue.

eGovJa (as FSL) performed an analysis / mapping of database designs / data models in TRN and mapped the fields against other databases and the proposed NIDS data structure. Details of this analysis are available to the Consultant Team and is being analyzed. It has not been replicated in this report.

Provision has been made to store a NIDS number in the Tax database.

D.2.2 ID DATABASE DESIGNS

The Tax database system(s) are currently hosted by eGov Jamaica Limited.

- Current system is Taxpayer Registration Number System version 5.26
- Runs on an HP Titanium running HP-UX 11.31
- Database is Informix 11.5 Enterprise Edition
- Application is Informix 4GKL (character based application)

A number of upgrades are proposed to the Tax systems – no details available at the time this report was written.

- Includes a database "cleanup".
- Includes an upgrade to the Driver's License system
    - Needs have been identified but there are no plans for implementation yet.

Tax Database presently holds approx. 2,200,000 TRNs:

- Approx. 800,000 are entities.
- Approx. 100,000 new TRNs are created per year.

A general comment was made that the TRN database is presumed as accurate – if not more accurate - than other identity databases:

- Has been used to "clean up" the PICA and EOJ databases.
- The TRN application has been audited at least 4 times since implementation in 1996. Audits were done by:
    - Symtai (local auditing company)
    - TAJ auditors
    - KPMG Peat Marwick
- Material findings from the first audit done by Symtai (approximately 8 years ago):
    - Issuance of multiple TRNs to the same individual; and
    - Missing records.
- The results of the subsequent audits indicated no missing records, and an estimated incidence of multiple TRNs assigned to the same individual at less than 5 percent.

The accuracy of the TRN data remains especially vulnerable to fraudulent birth certificates, passports, and other instruments used for identity verification. In addition, TAJ is yet to implement a process to have and keep the TRN database current with respect to personal information, especially address. To date, no audit has attempted to establish the extent to which these conditions prevail.

Technical standards

Relating to the eGovJa developed Informix 4GL applications:

- Application deployment directory structure
- User authentication and authorization scheme implemented using:
    - Standard database schema and application modules providing user authentication, authorization, user and access management, user role management, database access management, session management, menu maintenance, management of reports in terms of access to view/print, and report retention.
    - Standard modules for user administration.
- User interface (screen layout, function keys, colour schemes, dropdown lists) implemented as program templates, and standard program modules.
- Database and program variable naming conventions;

Access control models (including remote access)

- Access is restricted to users on the LAN/WAN;
- Each user accesses the application through a OS (Unix) user account where:
    - The user account is also created in the application and enabled.
    - The user is assigned an application and a database role providing access to the application components and database artifacts.
    - The user account is the exclusive property of that user and is not shared.
    - A user account is only reassigned to another user if the previous user ceases to be a system user. In this case, the application creates a new instance of the user account.
    - User application privileges cane be dynamically assigned and revoked.
    - The user account can be dynamically disabled.
    - An additional password account can be enforced within the application with the same characteristics as the Unix account in respect of expiration, account locking on login attempt failures, etc.
    - Generation, viewing and printing of reports require permissions that have to be specifically granted.
    - Some approval functions can only be executed with entry of user's application (not UNIX) password.
    - User's application password must be a minimum length and must contain a mix of characters.

D.2.3 Documented Existing ID System Architectures

Agencies and departments under the Ministry of Finance (with some exceptions) operate on the eGovJa WAN. Other Ministry of Finance (MOF) departments/agencies, and many non-MOF departments and agencies access the eGovJa WAN for application services hosted at eGovJa.

TRN data is accessed on the eGovJa WAN or via the Internet (using Web services) by Ministries Departments and Agencies (MDAs). In addition, stripped down copies of the TRN data are shared with some agencies – National Health Fund (NHF), HEART, and NIS – through an FTP site.

Some dependent systems are not online with the TRN and this sometimes results in issues when the customers attempt to do other transactions immediately after being assigned or have updated their TRN information.

Applications within the GOJ and private enterprises have access to TRN validation via Web services.

All access to TRN validation services by applications external to the MOF are granted by eGovJa upon provision of written approval from the Minister through the office of the Director General of TAJ.

- Applications for Departments within the MOF that are constructed by eGovJa may have direct access (query only) to the TRN database for TRN validation.

No Death information is provided directly to TAJ.

Web service allows verification of a TRN:

- Pass a TRN and the system returns name and other details.
- TAJ recognize that this as a privacy issue so are switching to a new methodology where the TRN and other data is passed and a “Match” or “No Match” message is the only response.

Web service also allows verification of a Driver’s License:

- Fee for service.
- Revenue goes to eGovJa, not TAJ.

Companies Office registers businesses and organizations.

- Are able to issue TRNs directly.
- Systems are “kind of” linked through eGovJa

D.3 NETWORK SECURITY

The visit to the Tax Administration Jamaica took place on Wednesday, January 15, 2014. eGovJa runs/hosts the Tax systems and a number of upgrades to the Tax systems are in the pipeline including a database "cleanup". There are 29 Tax Registration Offices throughout the country, plus the Head Office that also accepts applications. Data entry is performed at the point of registration utilizing a 2-person enrollment – both have to review/sign-off on the application. Note there is no hashing of the data in the database to insure integrity of the data.

TAJ clearly has processes, procedures and policy in place to handle network security as the systems are provided through eGovJa.

D.3.1 NETWORK AND SECURITY ANALYSIS

Because TAJ utilizes eGovJa's backend systems, the bulk of the network security follows eGovJa's capabilities. Protection of the user client side of the system does require some effort by TAJ to make sure this side of the system is properly protected.

D.3.2 DOCUMENTED EXISTING INFORMATION SECURITY POLICIES

Information regarding security polices fall mainly under the same guidelines as eGovJa as stated by TAJ. The table below lists some of the common policy utilized by TAJ. These policies are provided through eGovJa.

Policy Name	Current Version	Revision Date
eGovJa - Physical Access Control Standards & Procedures (Nov 2013)	0.3	20.11.2013
eGovJa - Remote Access Usage Policy (Nov 2013)	0.3	20.11.2013

TABLE 4: TAJ SUPPLIED POLICY DOCUMENTATION

D.3.3 DOCUMENTED COMPLIANCE STANDARDS

TAJ utilizes the same base set of national and international standards that are being utilized by eGovJa.

Specific details of Compliance Standards were not available to the Consultant Team at the time of this report and will be updated when available.

Appendix E: ELECTORAL OFFICE OF JAMAICA

E.1 BUSINESS PROCESSES

E.1.1 ENVIRONMENTAL ANALYSIS

The EOJ has implemented an Elector Registration system (ERS) to provide accurate information to all eligible electors and from which to compile a voters list every six months.

The basis for the ERS is the collection of elector's demographic data, his/her photograph and fingerprints. Fingerprints are cross matched to ensure that there are no multiple registrations and to ensure that each registered elector has only one opportunity to vote.

The Representation of the People Act (1996 and amended several times) governs election law: what can/cannot be done with data and biometrics is included in that legislation.

A voter's list is now produced and published every six months, May 31 and November 30

- They are posted in Post Offices and the public can object to anyone in the list, in which case that person is asked to provide proof of eligibility.

EOJ operations have been collecting and using fingerprints since 1997

- Currently the EOJ database has 1.7 million eligible voters but it is estimated that the database contains more entries than eligible voters.
- Many young people register when they turn 18 simply to get an ID card.

Registration:

- Have 79 registration offices across the island:
    - There are 63 constituencies island-wide:
    - Have at least one registration office in each of the constituencies.
- EOJ does not require a birth certificate for proof of eligibility unless the person looks obviously under age (18 is the voting age).
- No card is issued immediately – the registration pends until after the next posting on the Voters List.

Issuance:

- If no objection is received, the applicant is registered and a Voter Registration card is issued on the 6th month anniversary of the publishing of the list:

  - Informally known as the National ID Card.
  - This is a photo ID card with biographic information and 2D Barcode (contains fingerprint templates).
  - Use a watermark and other security features in the card to help prevent fraud - but there is still some fraud.
  - Use Data card MX6000 card printer.
- In-person card delivery.

Select polling stations have systems to read fingerprint and pull up data from the database.

- Expensive so not yet island-wide.
- Checks 4 fingerprints.
- Not online with main database - database is replicated and distributed to each station.

Even if no fingerprint reading capability is available, polling station requires a voter to show the Voter ID card to vote.

The Law limits how the database can be used:

- For voting purposes only.
- Fingerprint data cannot be shared.
- Receive “countless” requests from the Police for access to biometric information but cannot grant under current law.

Death list provided to the Electoral Office by the RGD every 3 months

- It is extremely difficult to reconcile the lists because there is no unique number to relate them together - NIDS would be ideal for solving this challenge.

70,000 voters were taken off the list following a 'manual' verification exercise in 2005-6. Also manually there is a periodic look at people over the age 81 and EOJ subsequently deleted another 32,000 by removing people who have died.

- NIDS data would provide a way to triangulate ID information and be very valuable and save money and resources.

EOJ currently operates a 3M Cogent AFIS:

- EVABIS - Electronic Voting and Ballot Issuing System
- Frequent upgrades from Cogent.
- Reportedly happy with the system and the support.

EOJ is presently exploring iris and facial biometrics also but no firm changes are made or planned.

EOJ has skills and staff that are able to share experience and knowledge in AFIS with other organizations (and even other countries) so could assist in the stand-up of NIDS.

- Proven experience of transferring knowledge to Antigua, Barbados and others.

EOJ would be willing to consider (subject to legal review) to cross-check identities against their data base both demographic and biometric for NIDS adjudication purposes.

- This would potentially result in significant time and cost savings and improve the precision (and cross linking) of EOJ identities to NIDS.

Next Election will be held not later than June 2016.

E.1.2 Documented Existing Business Processes

Specific details of the existing business processes were not available to the Consultant Team at the time of this report and will be updated when available.

E.2 ICT Architecture

E.2.1 Documented Existing ID System Data Models

eGovJa (as FSL) performed an analysis / mapping of database designs / data models in EOJ and mapped the fields against other databases and the proposed NIDS data structure. Details of this analysis is available to the Consultant Team and is being analyzed. It has not been replicated in this report.

E.2.2 Database Designs

Using a 3M Cogent AFIS:

- EVABIS - Electronic Voting and Ballot Issuing System
- Exploring iris and facial biometrics also.

Capture / store 10-prints but only scan for 4 (index/middle on each hand).
Currently have 1.7 million eligible electors in the database.
Can't say exactly how many actual entries they have in the AFIS but greater than 1.7million; entries are not purged from the AFIS data base.

Database Security:

- Database backups made onsite then taken offsite
- Database is not encrypted
- 2-man rule applies when making any changes to the database.
- 3 month process is required to change an address in the database.
- Requires a sign-off from both political parties.

Further details of the Database Design were not available to the Consultant Team at the time of this report and will be updated when available.

E.2.3 ID System Architectures

A number of polling stations have fingerprint readers and pull data from the database for matching purposes.

- Not online with the main database - database is replicated and manually distributed to each station.

EOJ have established relationships with financial institutions:

- Provide a web service that allows verification of the Voter ID number and DOB and returns a match if found.
- Subscription fee based service.

Further details of the System Architecture were not available to the Consultant Team at the time of this report and will be updated when available.

E.3 Network Security

E.3.1 Network and Security Analysis

The visit to the Electoral Office of Jamaica (EOJ) took place on Wednesday, January 15. The EOJ has been collecting/using fingerprints since 1997 and not all the polling stations have systems to read fingerprint and pull up data from the database. Present Law limits how the database can be used and fingerprint data cannot be shared. The system is produced by 3M and utilizes their Cogent AFIS. The data stored in the database is not encrypted and both iris and facial biometrics are being considered as upgrades. Web services allow entry of Voter ID number and DOB and will pull up data if a match is found. The web services are mainly

utilized by the financial sector. Presently there are 79 registration offices across the island and as stated earlier not all the stations have systems to pull up data from the database.

E.3.2 Documented Existing Information Security Policies

During the writing of this assessment report no documentation has been received by the Network Security Consultant regarding network security policy documentation. The visit to the facility showed that EOJ had carefully considered best practices relating to network security. Based strictly on the onsite visit it appears that EOJ does have both policy and procedures to handle IT Network and security areas. Access to the server systems required PIN codes and were only available to authorized individuals.

Specific details of Information Security Policies were not available to the Consultant Team at the time of this report and will be updated when available.

Policy Name	Current Version	Revision Date

TABLE 5: EOJ SUPPLIED POLICY DOCUMENTATION

E.3.3 Documented Compliance Standards

AFIS systems by their nature adhere to best practices and international standards for image quality and data exchange formats. Upon visual inspection physical security, logical security and auditing procedures and processes do seem to be in place.

Specific details of Compliance Standards were not available to the Consultant Team at the time of this report and will be updated when available.

Appendix F: MINISTRY OF HEALTH

F.1 BUSINESS PROCESSES

F.1.1 ENVIRONMENTAL ANALYSIS

In the National Health Information System and e-Health strategic plan 2014-2016 developed by MOH, the vision is presented as an "an integrated National Health Information System supporting timely an efficient data management to produce quality information ". The use of an electronic health record is a core initiative and one of the 4 key priorities. This initiative will be implemented through a first component called the Patient Administration System (ePAS) which will make information electronically available at multiple locations. ePAS will be developed based on a Free and Open Source (FOS) software system which is currently under development with an open source developer community specialized in patient care systems.

Currently MOH do not provide a unique identifier for their patients and use a manual algorithm (through questioning) to try to determine identity (based on the biographic information provided). This can lead to legal issues through misidentification.

- TRN or other "national" identifiers are not routinely collected

A key requirement for the new HMIS is a unique patient identifier. As documented in the strategic plan: "the proposed national identifier holds promise in linking health information across diverse data stores to ensure the portability of patient information to support continuity of care." **The strategic plan includes an initiative to ensure that the design of a national identifier is aligned with the development of e-Health solutions** and will support truly NHIS. As they cannot wait for NIDS (starting their pilot in April 2014), the Patient Identifier will be randomly generated by the system upon registration:

- Not linked to a person by a biometric.
- Alphanumeric - 9 digits

The new system is being designed to maintain all the current ID numbers (including TRN, Health Records Number, Government of Jamaica Health Card Number, others) and will create/maintain a data location for the NID number.

In the NHIS strategic plan there is a performance improvement indicator calling for 25 % of the patients registered in the PAS will use a national ID number by 2017- 2018.

The system will be sharing data on a monthly basis with RGD. A medical record is not created immediately for a new baby but the new system will generate a new identifier for the baby (linked to the Mother's record).

MOH Have made a cabinet submission requesting to be able to capture/store pictures in GENUHEALTH (the new FOS software) as a temporary measure until NIDS allows tracking by biometric.

NHF – National Health Insurance

Was formed in 2003 and is used for pharmaceutical services. An identifier was required to uniquely identify individuals and a decision was made to use the TRN (considered the most robust). However, this required anyone participating in the program to have a TRN and the TRN at the time was only issued to people over 18 at the time. The Tax Authority agreed to relax that age restriction to allow TRN assigned from birth.

The NHF member number is a 10-digit number derived from the TRN and created by an algorithm that ensures it is unique.

- Currently have >500,000 cards issued
- Approx. 330,000 of those have the unique identifier.

It is understood that the system is open enough that it can be modified to support the NIDS:

- May decide to keep existing member number.
- May create a new algorithm to create a member number based on the NIDS number.

Cards are mailed to recipients already activated and no other ID is obligated at the pharmacy.

The use of the system is limited (and closely controlled) to a list of items available using the card - and the amount of each item.

GOJ Card

This scheme has about 108,000 members and provides for general health services.

- Some people (estimate 25,000) may have both the GOJ card and the NHF card

PATH information is collected as part of the GOJ registration process.

- Use the TRN to match identities.

Child Health Development Passport (CHDP)

Issuance began in September 2010. This is a Paper Booklet which maintains health and educational records up to age 18, including:

- Birth information.
- Immunization information.
- Educational achievements.
- Nutritional record.
- Screening tools to monitor health and development.

It has a sequential numbering system for a Document identifier – this is not a person identifier. A record of the Passport number is made in the clinical record.

It is mandatory that each child is issued one but it is a procedural mandate, not a legal one. It is issued at birth if in a hospital, at time of first medical visit if not. >90% of babies since 2010 have the passport.

NIDS could be used to reconcile Passports numbers with patients.

F.1.2 Documented Existing Business Processes

Specific details of the existing business processes were not available to the Consultant Team at the time of this report and will be updated when available.

F.2 ICT Architecture

There are 13 Health Departments and 24 hospitals that collect patient data. The information is integrated at a national level.

Network connectivity is not always reliable so each Health facility must be able to operate offline – they are still identifying the best way to resolve this. The biggest challenge this creates is with the generation of the unique patient number. If the system is offline, a temporary ID must be issued until uniqueness can be established when connectivity is restored.

Patient records are still primarily paper-based. Are considering a Document Management and Imaging System – only for digitizing, not digitalizing.

F.2.1 ID Numbers

The Consultant Team identified multiple ID numbers in use across the MOH.

There is not currently a unique Patient identifier:

- Use a manual algorithm (through questioning) to try to determine identity (based on the biographic information provided).
- Can lead to legal issues through misidentification.

The TRN or other "national" identifiers are not routinely collected so unique identification is a problem. A key requirement of the new MHIS system is generation of a patient identifier. MOH would use the NIDS number but cannot wait for NIDS – they are starting their ePAS pilot in April 2014. For this program, a patient Identifier will be randomly generated by the system upon registration.

- 9-digit alphanumeric number.
- Not linked by a biometric.

The system is being designed to also maintain other patient identifiers numbers (including the Health Records Number, Government of Jamaica Health Card Number, others) and includes a location to store / maintain a NIDS number.

Other numbers identified within MOH include:

1. Health Records Number
   - Number is generated manually.
   - 6 digit – sequential.
   - Unique to the facility but not country-wide.
   - Need to maintain this number - cannot replace this with the new number - used in too many places - especially for filing (current procedures require a sequential numbering system for filing).

2. NHF Member Number.
   - Is a number derived from the TRN.
     - Created by an algorithm that ensures it is unique - 10-digit number
   - May keep the existing member number moving forwards or may devise a new algorithm to create a member number based on the NIDS number.

3. GOJ Card
   - Uses the TRN as an identifier to match identities with PATH.

4. CHDP
   - Has a sequential numbering system.
   - Document identifier only - not a person identifier.

F.2.2 ID DATABASE & APPLICATIONS

MOH has a contract with eGov Jamaica Limited for the hosting and maintenance of the MOH Trade Facilitation system.

The new ePAS system is being developed in Free and Open Source (FOS) software system.

- Sustainable and affordable for over 340 facilities.
- Have an MOU with the FOS community (for 2 years).
- They will assist with software development

There is one core legacy ICT system but this is a proprietary system and "has to go".

- System is only presently supported in 10 of 24 hospitals and 1 of the other 316 health facilities.

MOH requires access to a broad range of data sources in order to develop a complete patient picture. These include:

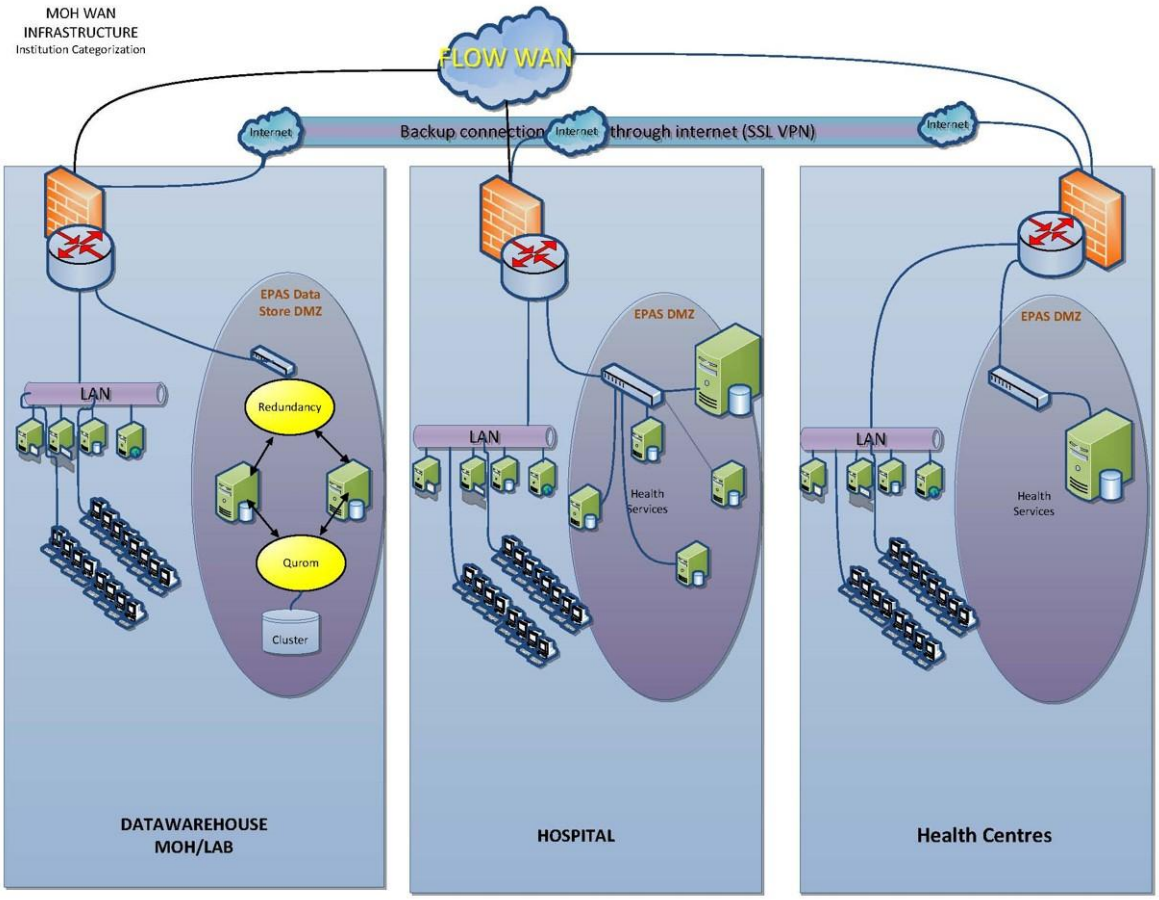
- PIOJ
- RGD
- Statistical Institute of Jamaica
- National Security
- University of West Indies
- Others

There is a good existing relationship with RGD, covered under a collaborative MOU. They will be sharing data on a monthly basis with RGD.

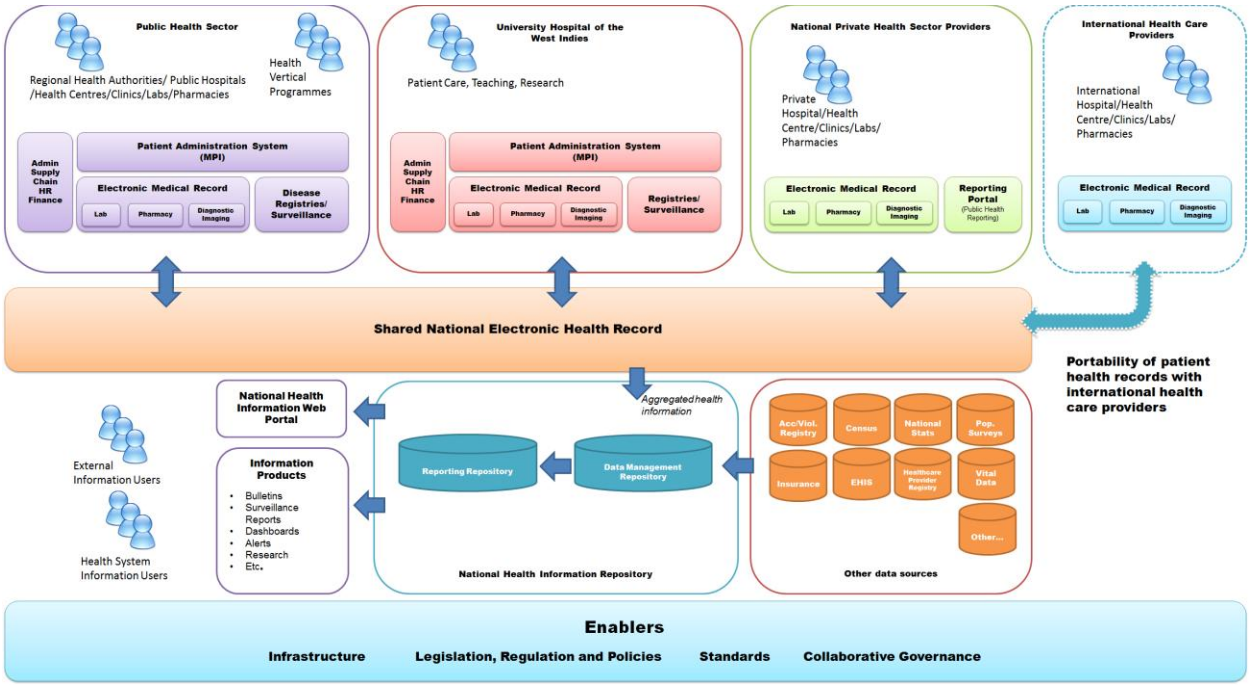
Further details of ID Databases and Applications were not available to the Consultant Team at the time of this report and will be updated when available.

F.2.3 CONCEPTUAL SYSTEM ARCHITECTURES

The following diagram shows the MOH WAN Infrastructure for the ePAS Patient Administration System.

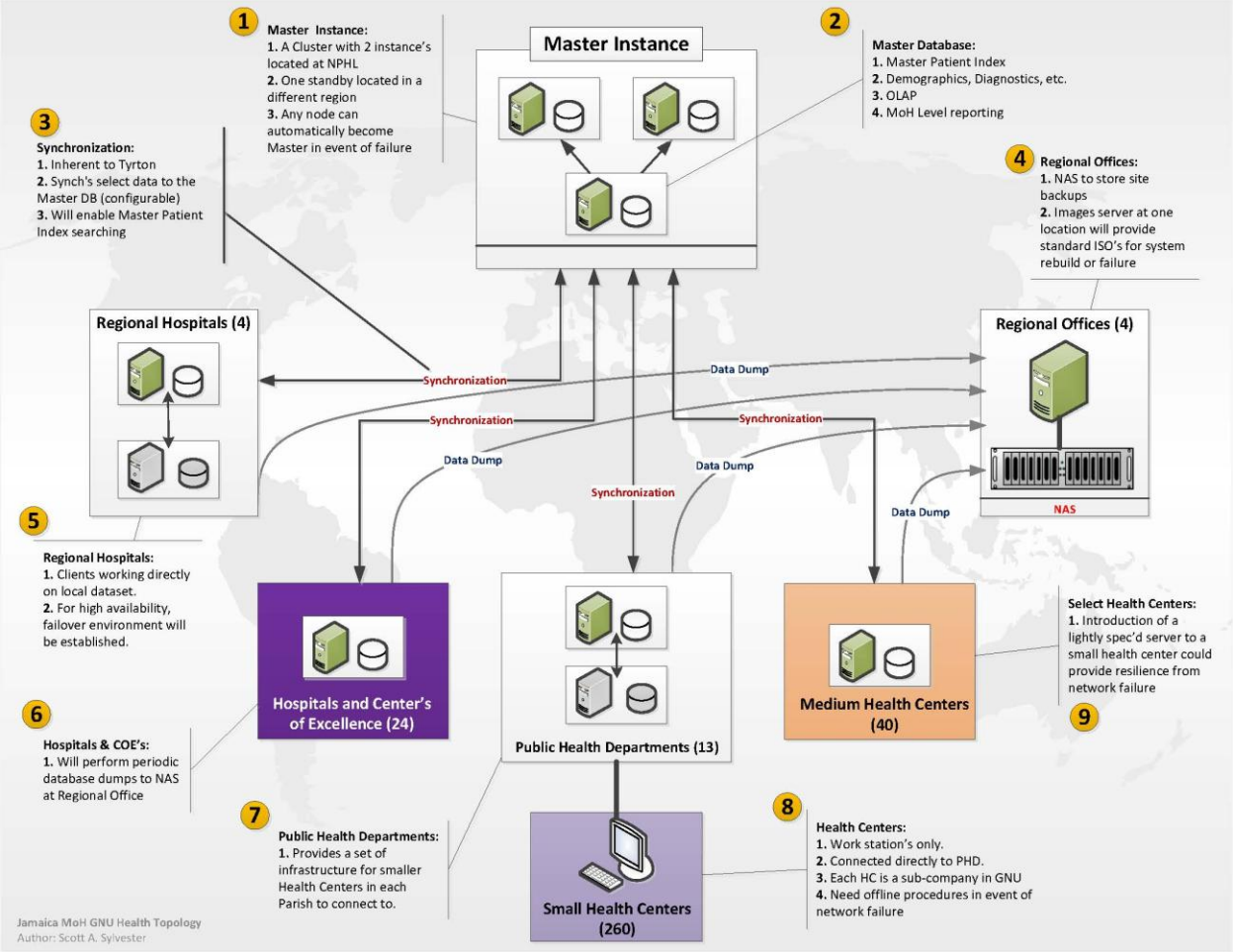


The following diagram provides a graphical representation of the vision for a National Health Information System and e-Health for Jamaica. This is not a technical architecture, but rather a conceptual view of how the various envisioned components may work together.



Source: *National Health Information System Strengthening and e-Health Strategic Plan 2014 to 2018, Ministry of Health, October 2013*

The following diagram is an illustrative network topology for the proposed National Health Information System:



F.3 NETWORK SECURITY

F.3.1 NETWORK AND SECURITY ANALYSIS

The visit to the Ministry of Health took place on Wednesday, January 15, 2014. The consultants did not get the opportunity to see any of the networked systems due to time constraints. There are many different data sources that need to come together to provide a complete picture. The Primary information source is patient care data and supporting information comes from finance, HR, etc. The Patient Administration System is using a Free and Open Source (FOS) software system. The MOH has made a cabinet submission requesting to be able to capture/store pictures in GNU Health (the new FOS software).

The GNU Health server system is composed of the following components:

- Attachments, Images, links to PACS
- Tryton and GNU Health kernel
- Database and PostgreSQL engine
- Linux Operating System components (kernel, users, network, ...)

Presently 13 health departments along with 20+ hospitals collect data, which is integrated on a national level. Network connectivity is not always reliable so each Health facility must be able to operate offline. MOH has also contracted with eGovJa for the design of the national Health Information Network, i.e. the MOH WAN, and has intention to acquire a document management and imaging system.

F.3.2 Documented Existing Information Security Policies

The visit and discussion with the stakeholders provided the vision for the eHealth system. The vision for the system has been carefully considered and will utilizing best security practices along with cost considerations. Based on the site visit it was hard to determine what policy and procedures are used to handle IT Network and security areas.

Specific details of Information Security Policies were not available to the Consultant Team at the time of this report and will be updated when available.

Policy Name	Current Version	Revision Date

TABLE 6: MOH SUPPLIED POLICY DOCUMENTATION

F.3.3 Documented Compliance Standards

Specific details of Compliance Standards were not available to the Consultant Team at the time of this report and will be updated when available.

Appendix G: REGISTRAR GENERAL'S DEPARTMENT

G.1 BUSINESS PROCESSES

G.1.1 ENVIRONMENTAL ANALYSIS

The Registrar General's Department (RGD) was established in 1879 with the mandate to ensure the registration of births, deaths and marriages in Jamaica and its territorial waters through the General Register Office. The Island Record Office, which is another arm of the RGD, is responsible for the safe keeping of public records such as: Deeds, Liens, Resident Magistrate and Supreme Court wills, Certificates of Citizenship and Naturalization as well as Acts of Jamaica. Certified copies of birth registration are the primary identifiers for all vital events occurring in Jamaica. The RGD was made into an Executive Agency on April 1, 1999 as part of the Government of Jamaica's agenda to transform the public sector to be more customer-centric. It is the authoritative repository of over 70 million records dating back to 1660s.

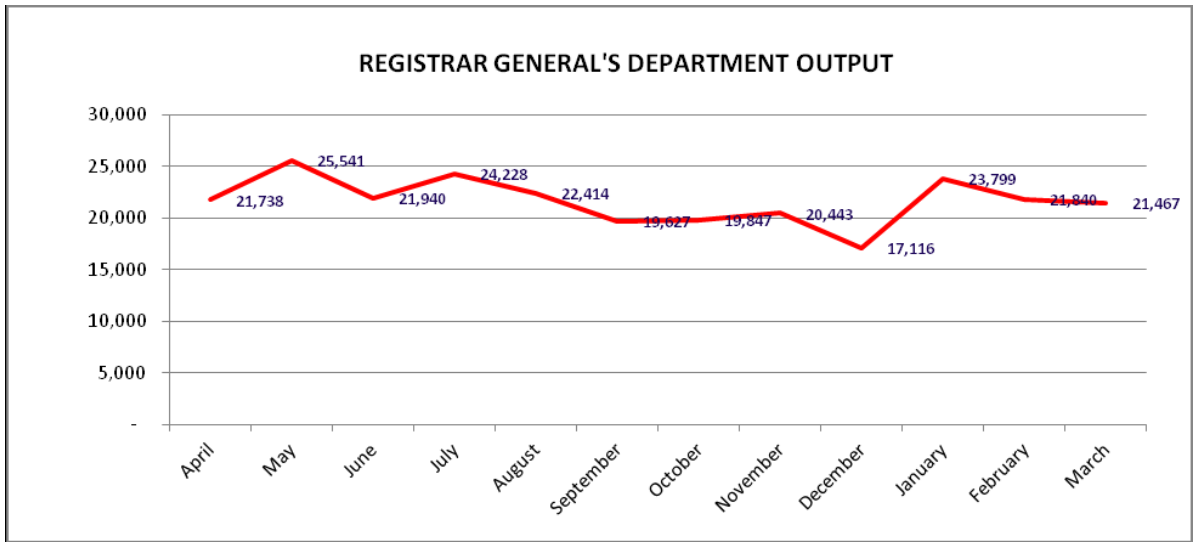
RGD is self-funded with no-appropriation from Government.

This is a customer service cultured and service innovation focused organization taking advantage of their branch office network (10 branch offices) and online facility.

One critical area was the implementation of ICT in its processes to increase efficiency, economy and effectiveness. On May 7, 2001 an in-house application system was implemented known as the Birth, Death, and Marriage System (BDMS) from which certificates were printed on Security Paper. To further improve the system in April 2003 an in-house Application Tracking System (ATS) was implemented and integrated with the BDMS. The ATS allowed for electronic tracking through each step of production and to add commentary by internal users agency-wide. Further developments to the system included: point of sale transactions through a retail management system, online payment interface, application process updates through interface via the internet by customers. The latest system developments include the provision of application updates through Automatic Voice Response (AVR) facilitated through the Voice over IP.

Not all the RGD business processes are computerized resulting in a high-interdependency on manual labour which is still inadequate and a major challenge to be funded. The RGD staff complement includes 345 personnel. Approximately 260,000 applications are processed annually which include approximately 40,000 free first copies of birth certificates

provided to fully registered newborns. Additionally over 260,087 sheets (160 words are equivalent to 1 sheet) of documents are recorded annually. There are several non-core services such as 1,665 registry weddings which are facilitated annually and 1,349 deed polls drafted. Identified below are the basic output of applications processed annually and an indication of peak periods.



It is not mandatory to name baby at birth but since the implementation of bedside registration on January 1, 2007 a free first copy of the birth certificate is issued within three months if the baby is named during the process. As a result of this incentive, 90% of birth registrations now contain a baby name and nearly 70% now include the father's particulars.

Once registered, the RGD is able to produce a birth certificate and requires the following information:

- Birth entry number
- Full name of parents
- Place of Birth
- Date of Birth
- Name of Child

A child cannot enter school without a birth certificate.

The Agency, through its own efforts, developed new software to conduct online registration. This is ready to go but not yet implemented as it is not currently funded. The Agency is considering a phased introduction with it being introduced to hospitals in major

population centers first. Online registration will be available for use by the RGD staff in the hospitals.
There is an ongoing NHIS (National Health Information System) initiative to implement good internet connectivity at all locations: RGD hope to piggy back off that initiative to allow the online registration systems to be connected at all times. If the systems are not online, a number is not assigned until connectivity is re-established with the main database.

The RGD has not audited its database or business processes due to a lack of financial resources. As a way forward, a committee was recently established to review and document processes and recommend changes.

An Online Verification system has been developed and is slated to be implemented by March 2014. The system will allow the following:

- Allows external subscribers to query the registry.
- Will return an image of the certificate if available.
- Uses https (or equivalent) for secure communication.
- Operated on a Fee-for-Service basis

RGD is “not close” to digitalizing all the records yet as funding is limited and it was not possible to provide an estimate of when they will have all digitalized.

They are interested to see if NIDS could help clean their records and feed updates back into their system.

RGD use an Internal Registration Tracking System developed in house:

- A tracking number is generated for each application for a birth certificate.
- The processing of each application is updated and can be retrieved using the tracking number.
- The record includes a copy of the receipt provided to the cashier.
- 100% audit trail is maintained.
- The system links to the online query system.
- Customers can track progress via a web portal.

RGD also has an electronic index system “IRIE” which facilitates the search for electronic indices of vital records.

RGD do not have life events reconciliation software – some software was developed in house but is not implemented.

Birth certificates are produced on high end security paper from one of the best designer and manufacturer of this type of documents (Giesecke and Devrient, Germany). Processes used to authorize and control the production of such birth certificates are best in class and would certainly meet the ICAO breeder documents production guidelines.

A number of MOU have been signed with other MDA's:

MOUs with the Police: - Not obtaining adequate and timely data on sudden and violent deaths including police shootings. This negatively affects the completeness and quality of data submitted to STATIN annually.

Electoral Office of Jamaica: regarding the provision of death data. Additionally within recent times data has been requested on deed polls.

Discussions have taken place regarding the provision of death data to Accountant General's Department regarding pension arrangements.

MOUs with JSIF and PATH – provision of birth certificates to persons in receipt of social benefits.

Charter – Citizen's charter which informs on the service standards of the Agency.

The RGD has over the years embarked on several initiatives geared at modernizing the Civil Registration and Vital Statistics system in Jamaica as well as improving its processes. Despite the efforts so far, there still exists the need for further modernization to take place to support the implementation and maintenance of the National Identification System. The existing systems at the RGD include both manual and computerized processes. To support the NIDS, it will require an electronic system with all vital records since at least the year 1910, capable of integration and interfacing to enable the ease of assignment of a unique identification number. This system should be capable of facilitating linkages between relevant vital records whether the birth, marriage, death, deed poll or adoption event.

The Agency is at a crossroad where further improvements can only be achieved through the following improvement initiatives:

- Comprehensive electronic, real time data capture of all vital events occurring within Jamaica which would inform National Planning and support the Government's thrust

of implementing a National Identification System. RGD states that the first phase will be achieved through the implementation of e-registration of births by March 2014.

- Conversion of all vital records and supporting documents through the electronic population of the BDMS. This will allow for better cross referencing/matching of vital data life events - that is their birth, marriage, death and instances of name change through a deed poll;
- Business process re-engineering to assess all major areas of operations.

G.1.2 Documented Existing Business Processes

All key workflow processes have been provided and will be integrated at a later date.

G.2 ICT Architecture

G.2.1 Data Models

The entry number for birth / death registrations is alphanumeric:

- The first letter – Parish
- Second and Third letters – Registration District
- Number – sequential event number (note: Numbers not necessarily unique)
    - This sequential number goes from 1 to 9999 and after this the number starts over. As a consequence, it is possible for a certificate number to be repeated in a year in a larger district such as Kingston.

eGovJa (as FSL) performed an analysis / mapping of database designs / data models in RGD and mapped the fields against other databases and the proposed NIDS data structure. Details of this analysis are available to the Consultant Team and is being analyzed. It has not been replicated in this report.

A data field has already been established in the Civil Registry database to store a NIDS number when it is assigned.

G.2.2 Databases and Applications

<u>Birth, Death, and Marriage System (BDMS)</u>

- In-house application

- First implemented in 2001
- Database is SQL Server 2008
- Visual FoxPro application programming
- Enables printing of Certificates on Security Paper
- Provision application updates through Automatic Voice Response (AVR) facilitated through a Voice over Internet Protocol (VoIP) system

Application Tracking System (ATS)

- Integrates with BDMS
- SQL Server 2008
- Adobe ColdFusion 5 application development
- Tracking number is generated for each application for a birth certificate
    - Other steps in the process key off that number
- Record includes a copy of the receipt provided to the cashier
- 100% audit trail is maintained
- Includes support for point-of-sale transactions through a retail management system and an online payment interface
- Links into the online query system
    - Customer can track progress through a web portal
- Upgrade and modernization program in the planning phase.

Online Registration System:

- Developed in ColdFusion.
- SQL database.
- Written for a laptop but working on tablet conversion
    - Signature capture is the biggest issue due to the new OS of the tablet).
- Other issues to overcome include battery power limitations and wireless communication availability in the hospital – coverage is inconsistent from one area of the hospital to another.
    - Hoping to 'piggyback' off the ongoing NHIS initiative to implement good internet connectivity in hospitals and medical facilities.
    - Will allow the systems to be online at all times.
    - Number is not assigned until connectivity established with the main database.
- Use VPN for data transfer.
- Estimate a March 2014 launch date.

eServices online verification system:

- Will be online in March 2014.
- Allows external subscribers to query the registry.
- Provides authentication services for external subscribers for documents/certificates
    - Currently being implemented to provide this service online to stakeholders including PICA, TAJ, Embassies, EOJ, etc.
- Will return an image of the certificate if available.
- Uses https (or equivalent) for secure communication.

Index Rebuilding Implementation Exercise (IRIE) database:

- Record search system (internal use only)
- Electronic index of "most" records

Proprietary, in-house developed software to track cross-events:

- Creates/assigns a unique number for each person.
- Tracks descendant information.
- Is not able to touch all databases (e.g. divorce)
- Described as "a work-in-progress with challenges"

Bedside Registration database and the BDMS database are currently independent but have software (in-house) ready to integrate once in-house records are digitalized.

G.2.3 ICT System Architectures

There is no electronic linkage or data sharing yet established with external MDAs

- Information / data is exchanged manually

The systems and networks infrastructure at RGD currently includes:

Wide Area Network (WAN) - External

- Connects 10 regional locations using Digicel WiMAX Broadband.
    - 10Mb connection between each location.
- 3 x T1 lines from Digicel input to PBX
- 6Mb dedicated internet access with 10 usable IP address
- 1 x T1 line from Lime input to PBX
- 2MB Lime ADSL

Local Area Network (LAN) - Internal

- Connects workstations, servers, printers, photocopiers and other devices within the Head Office.
- 19 x Switches (Cisco and Dell)
- 3 x Hardware Firewalls (Cisco)
- 2 x Servers acting as a software firewall (running Ubuntu Server 12.04)
- 5 x Power over Ethernet (PoE) Midspan devices
- 1 x fiber connection which connects the telephone and server rooms.

27 x Virtual LANs (VLANs)

Servers & Storage

- 18 x Physical servers
- 15 x Virtual servers
- Network Attached Storage (NAS) contains all the virtual disks for all the servers on the virtual machine.
    - Concern it is a single point-of-failure within the system.
    - Require software to operate an Active-Active High Availability Storage Architecture.

Workstations

- 79 at the Regional Office
- Approximately 173 at the Head Office
- 25 x Thin Clients

Data Backup

A full back up of RGD's data is done daily, including databases, file servers and mailboxes. The backup is scheduled to run automatically after working hours (after 5:00 pm daily) and on weekends. Log backup of several of our databases are also done throughout the day. Duplicate backups and media storage are maintained offsite.

Network Redundancy

The current configuration is of such that any server installed in the virtual environment can easy be migrated between servers. Therefore, if there is an issue with a virtual server, hardware failure or maintenance required, all servers can be easy migrated to another virtual server. This provides redundancy from down time and data losses in the event of virtual server failures.

Software Updates

USE Windows Server Update Services (WSUS) to deploy Microsoft product updates to computers/servers on the network that are running the Windows operating system.

G.3 NETWORK SECURITY

G.3.1 NETWORK AND SECURITY ANALYSIS

The visit to the Registrar General's Department took place on Thursday, January 16. The consultants were presented with a PowerPoint presentation along with a Demo –E-Registration, tour of the RGD (Print Room, Data Center, Vital Statics, Production, IRO and Customer service areas) and a chance to observe a bedside registration process.

The data center is composed of both electronic and paper based records and the system was created by the RGD team. The system is called the Birth, Death, and Marriage System (BDMS). In 2003 the Application Tracking System (ATS) was implemented and integrated with the BDMS. The latest system developments include the provision of application updates through Automatic Voice Response (AVR) facilitated through the Voice over Internet Protocol (VoIP) system.

Logical access to the network systems includes the following access control methods:

ROLE-BASED ACCESS CONTROL for our Active Directory environment:

- Username and Passwords for workstation access
- Username and password for sub systems
- Electronic access cards and PIN for access to secured areas

ACCESS CONTROL LIST for remote access

- Specific ports are enabled for communication
- Username and password and encryption for VPN users
- VLAN and access list for connection to the regional offices

VPN Tunnel to access branch network

ROLE-BASED ACCESS CONTROL and ATTRIBUTE-BASED ACCESS CONTROL for ID systems

The RGD has clearly thought out its systems as well as its policies, procedures and processes. Compliance for the network security policy is being handle through audits done over the years.

G.3.2 Documented Existing Information Security Policies

RGD has an IT Policy, a Password Policy, a Remote Computer User Policy, a Computer Use Policy, System Administrator and an IT Code of Ethics Policy.

In addition, the following policies are currently being evaluated for updates:

- Physical Record Management Policy, including:
  - Secure vaults fully furnished with a fire retardant system
  - Records stored in acid-free storage
  - Bar coding of records to track usage
  - Other
- Digital Record Management Policy:
  - Governed by the Systems Management and Network Security Policy
- IT and Network Security Policy:
  - Governs general IT operations, security procedures, redundancy plans, business continuity plans, access control protocols, etc.

The Consultant Team were made aware of these policies but had not reviewed them at the time of this report.

Policy Name	Current Version	Revision Date
IT Policy		
Password Policy		
Remote Computer User		
Computer Use Policy		
System Administrator		
IT Code of Ethics Policy		
Physical Record Management Policy		
Digital Record Management Policy		
IT and Network Security Policy		

TABLE 7: RGD SUPPLIED POLICY DOCUMENTATION

G.3.3 Documented Compliance Standards

Specific details of Compliance Standards were not available to the Consultant Team at the time of this report and will be updated when available.

Appendix H: MINISTRY OF EDUCATION

H.1 BUSINESS PROCESSES

H.1.1 ENVIRONMENTAL ANALYSIS

The current system was designed to facilitate the registration of approximately 750,000 students with an incremental increase of 42,000 new students each year at grade 1. Registration at grade 1 is mandatory.

The student population is distributed as follows:

- Approx. 500,000 primary and secondary children.
- Approx. 750,000 total student population if you include pre-school and adult learners.

Currently MOE is cleaning its registration data (examination registration) and recognize they need a better capability to track students. They do have some electronic databases – but they are neither fully accurate nor reconciled. They have attempted to develop a unique identifier for students - not ready yet as they want to be able to track from entry into school through University. MOE would welcome NIDS identifier – both for tracking students and teachers (especially those that may teach across more than one school).

MOE operate an in-house registration system with a centralized data entry of completed forms returned from schools. It would be a big help if NIDS could pre-fill much of the biographic data in the forms.

MOE would prefer data entry performed at the schools as it would make QC easier if done at the source.

Of notable concern is education and training for 15-24 year olds. The unemployment rate for this age group is estimated to be more than 3 times that of the adult unemployment rate (Vision 2030 - Social Welfare and Vulnerable Groups Sector Plan, June 2009). The unique identification provided by NIDS would better allow the MOE to deliver and monitor specific programs for training and education for employment.

MOE has made allowance in their database for a NIDS number. A concept paper for their own registration number was developed but not yet implemented.

Other stakeholders who could benefit from NIDS for registration:

- Home schoolers and applicants for virtual schooling but not determined yet.
- Jamaican Foundation for Lifelong Learning serves adult learners - those who never completed secondary education.

Strictly speaking these participants are outside of MOE jurisdiction but MOE is still responsible for the monitoring of such education and curriculum.

Also MOE has a need for better teacher identification as there is a need to better track teacher movement as well as qualification/certifications:

- Currently use the TRN.
- A number of teachers are in the database with the same TRN.
- Working to clean up the database.

Approximately 25,000 teachers are in the public school system. MOE is also responsible for private schools.

H.1.2 Documented Existing Business Processes

An outline of current business processes has been provided in the Concept Paper. Further details were not available to the Consultant Team at the time of this report and will be updated when available.

H.2 ICT Architecture

H.2.1 ID System Data Models

2010 decision made to create a unique student identifier.

- First 4 are year of registration.
- Next 5 are a school code.
- Final 6 are sequential.
- Not yet implemented.

TRN currently used as the ID number for Teachers.

- Have identified duplicates in the database.
- Working to correct this.

Further details of Data Models were not available to the Consultant Team at the time of this report and will be updated when available.

H.2.2 ID DATABASE & APPLICATIONS

MOE has an in-house registration system - JSAS

- Centralized data entry of completed forms returned from schools.
- Data entry clerks follow a process to help try to catch duplicates.
- Would prefer data entry performed at the schools.
    - Would make the QC process easier if done at the source.

The database is a MySQL database; applications are developed in PHP5.6. Provision has been made in the database to store a NIDS number.

The database is required to support a minimum of total student population of 750,000.

- Approx. 500,000 primary and secondary children.
- Approx. 250,000 pre-school and adult learners.
- Planning for an annual incremental increase of 42,000 at Grade 1.

The existing database(s) are not considered accurate and have not been reconciled.

In addition, eGovJa hosts and maintain the Bank Reconciliation System (BRS) for the MOE. This is a Powerbuilder app that uses an Informix database.

Further details of Databases and Applications were not available to the Consultant Team at the time of this report and will be updated when available.

H.2.3 DOCUMENTED EXISTING ID SYSTEM ARCHITECTURES

Being able to data exchange/share with other agencies would simplify their processes and avoid duplication of effort.

- Not presently able to do
- NIDS would help facilitate

Specific details of the ICT System Architectures were not available to the Consultant Team at the time of this report and will be updated when available.

H.3 NETWORK SECURITY

The visit to the Ministry of Education took place on Thursday, January 16. MOE has a Service Level Agreement (SLA) between the Management Information Systems Unit (MISU) and the employees of MOE. The agreement establishes their commitment for internet, laptops, desktops, servers, networks, telecommunications, approved applications and technical support. This document clarifies both parties' responsibilities and procedures. The MOE application was developed using PHP5.6 with a MySQL backend database.

The following areas are supported by the IT Department under the agreement:

- Network Connectivity & Infrastructure
- Server Hardware & Software Support (availability, backup, restores, etc...)
- End-User Desktop, Laptops, printers (troubleshooting, break/fix, helpdesk/hotline, etc...)
- Telecommunications (desk phones, remote access, etc...)
- Hardware and Software standards, compliance, inventory & purchasing
- Uninterruptible Power Supplies (UPS)
- Fire Suppression System
- Biometric Devices

H.3.1 NETWORK AND SECURITY ANALYSIS

The Network Security Consultant did not get the opportunity to physically see the data center due to time constraints but documentation provided by MOE described some of these details as follows:

- Access to the MOE data center is done via a Fingerprint reader
- Access to the datasets is controlled by credentials tied to the application security roles. The user roles are defined by the application owner (Educational Services).
- User authentication is done via the google openID platform
- Software updates and patches are developed and tested locally, then deployed to an online staging server for further testing, and finally implemented on the production server
- The system does not have any direct data sharing methods
- The server room is equipped with HVAC (inrow) and a fire suppression system.

MIS Responsibilities:

- Adhere to the SLA.
- Log and track all employee requests for service via the Business Support Portal (BSP).
- Communicate ticket IDs to customers/staff.

- Maintain an effective level of communication with Ministry of Education employees.
- Review MIS request metrics reports to insure resolution times are being met.
- Work to exceed the current SLA and adjust resolution times accordingly.
- Maintain appropriately trained staff.
- Be courteous and friendly to all customers/employees.

Employee Responsibilities:

- Be aware of and adhere to the Ministry of Education – IT Security Policy and Service Level Agreement (SLA).
- Be willing and available to provide time to support the resolution of your work order and offer feedback.
- Be courteous and friendly to all MIS staff.

H.3.2 Documented Existing Information Security Policies

Specific details of Information Security Policies were not available to the Consultant Team at the time of this report and will be updated when available.

Policy Name	Current Version	Revision Date

TABLE 8: MOE SUPPLIED POLICY DOCUMENTATION

H.3.3 Documented Compliance Standards

Specific details of Compliance Standards were not available to the Consultant Team at the time of this report and will be updated when available.

Appendix I: OTHER NIDS STAKEHOLDERS

TRADE BOARD LIMITED

The Trade Board is the Digital Certificate authority within the Jamaican Government.

- Experience in using digital certificates to secure online transactions
- Has a Vision for the application of PKI across government.
- Has developed a Certificate Policy and Certificate Practice Statements.
    - Approximately 5 years old.
- Operates an Ultimaco Certificate Authority and PK based digital certificate system per IETF X.509v3 specifications.

The Electronic Transactions Act was passed in 2006:

- Identifies the Trade Board as the Certification Authority for PKI.
- Also covers digital signatures.

Some infrastructure was put in place following the passing of the Act but not nearly enough.

- Current system is from Utimaco.
- Considered good equipment but has limited capacity
    - 1,000 certificates actively in use.

Digital Certificates are being used to secure transactions for Customs and the Tax Authority.

- Trade Board is the Certificate Authority

Trade Board has also reviewed / evaluated possible forward paths for PKI in the private sector as well.

The PKI system / capability is a consideration for NIDS to build on.

PASSPORT IMMIGRATION & CITIZENSHIP AGENCY

The Team conducted an initial, short telephone interview with PICA to understand high level features and capabilities. An in-person meeting and high level business process walk-through was then conducted during a subsequent visit.

High-Level understanding from the telephone conversation:

- Passport Issuance
    - In person visit / interview at the Passport office with required documentation:
        - Birth certificate.
        - Photo ID.
        - Two passport photographs (one certified).
        - Application form, signed by same certifying officer.
        - Also any proof of change of name (deed poll, marriage certificate, etc.) if applicable.
    - Reception officer reviews and checks the documentation.
        - Search for duplicates - almost 2 million records.
    - Make payment.
    - Application goes to data entry.
    - Production:
        - Image capture (scan of provided photo).
        - Scan signature on form.
        - QC by a supervisor - double check data entry and flag any other info required from the customer if required.
        - Print.
        - Lamination.
        - QC check.
    - Employees involved can only complete a single stage in the process.
        - Not possible for one person to do more than one process.
    - In person delivery.
        - Check picture and signature.
- Currently provide a 7 day turn-around for Kingston.
    - 14-day turn-around for Montego Bay and other outside locations.
- Co-located Passport offices with other Government agencies.
- Expedited services available (next day or 3 days).
- Process applications from Embassies in other countries.
    - 20-day turn-around from receipt of application.

- General Information
    - Average 400 applications per day (with a peak of 800 per day).
    - Follow ICAO guidance – document validity of 10 years for adults, 5 years for children.
    - Estimated 1 million valid (non-expired) passports in the database – to be verified.

- Estimated 15-20% of passport holders live off island.
- Currently only capture a photo - no other biometric.
  - No facial recognition currently but looking to implement.
- Passport number is different from the application number.
- Application number is not a unique person identifier.
  - Each application has a new application number.
- NIDS could help uniquely identify an individual - and also help to validate the documents being presented as proof-of-identity.
- Verification of source documents is their biggest issue today.
- Do not have access to the RGD system to authenticate a birth certificate.
  - Similarly don't have access to online verification of a Driver's License or Electoral Card.
- Try to verify manually.
  - Often hard to get someone on the phone so must sometimes send the applicant back to the authoritative source to resolve any issues.
- Have an internal investigative team to look at suspicious cases.
- Law allows for "Citizenship by Doubt":
  - If no birth certificate or record of birth is available, can produce other documents to prove they have been living on the island for life (school records, medical records, etc.).
  - Doesn't happen very often - maybe 2 or 3 cases per year.
- Passport system provided by Canadian Banknote:
  - Customized from their standard offering.
- Has an offsite backup system.
- Also operates a separate Border Management system from a different supplier (3M).
  - Has a real-time link to the Passport System.
  - Next big project is to integrate the 2 systems.
- Emergency Travel Certificates can be issued if a passport is not available.
  - Also issue travel permits for foreign nationals who are temporary residents.
- CARIPASS not currently accepted.
  - They are aware of it and are open to accepting it once agreement is reached.

Additional understanding from the in-person meeting and walk-through:

Agency mission consists of three sub-missions all on different platforms:

- Passport issuance and management
- Border management
- Visa issue and management

  - PICA is receptive to NIDS and see it bringing benefits to their present processes in both in cost savings and increased accuracy/fidelity/precision of mission.
    - Using a biometrically enabled NIDS would mitigate the current challenge of more than one passport being issued to the same individual (under different names) – and would make it easier to detect existing situations where that has occurred.
  - PICA currently issues over 10,000 passports per month.
  - PICA does not presently collect nor use biometrics, however is exploring the ICAO MRTD ePassport facial recognition biometric as part of the agency evolution/roadmap
  - A tender for an integrated Border Management, ePassport and Visa system is in the process of being finalized.
    - Present systems are independent with challenges in cross-checking between them.
    - Visa issuance is presently a manual process.
    - Indicates anticipated RFP will have a provision to capture and maintain NIDS unique person identifier
  - NIDS would provide a common linkage to enable efficient and accurate cross-checking.
  - Existing passport printers were procured to be forward upgradeable to support forthcoming ePassports.

Intake and processing is a highly manual and stepwise process. There are significant levels of fraud in the system (inherited) that are actively being pursued and mitigated by a robust investigative and oversight process.

There is both primary (face to face) intake as well as secondary (questioned documents) evaluation. These are manual in person processes that require significant training and resources and does have potential for single point failures.

The post-adjudication backend processes are robust and well managed – including random assignment of work orders and multiple steps/stages in quality control/production. NIDS can provide significant savings and mitigate the front-end intake and adjudication risks. This would allow questionable passport applications/applicants better assessment and case management.

Potential for passport fraud is low, but not impossible due to the highly manual processes in place. Camera systems are in place, but could be improved for security monitoring.

Servers on site and off site backup. Operations in Montego Bay back-up primary Kingston facility.

Security and controls are tightly managed.

NATIONAL HOUSING TRUST (NHT)

- Reports into the Office of the Prime Minister.
- Enthusiastic and supportive of the introduction of NIDS.
- Have a competent and knowledgeable ICT staff.
- Expressed a preference for a 9-digit NIDS number similar to the TRN.
- There are currently over 400,000 people served by NHT.
- Presently have an issue validating that an applicant meets eligibility requirements.
    - Have 'field officers' to perform a manual, in-the-field validation.
- Major initiatives to further move services online
    - Online payments
    - Online viewing of status
- Would like to add additional services including mobile services in the future.
- See NIDS as a critical factor in being able to uniquely and unambiguously identify participants.
    - Supportive of NIDS as a digital identity in support of the delivery of online services as well as a physical identity.
- Would like to be able to better utilize existing offices.
    - Provide multiple services from each office.
- Views itself as an early adopter and first mover agency.

NIDS solves a number of outstanding crucial business process challenges including age verification for eligibility to NHT programs, de-conflict and provide greater precision for related party eligibility – such as joint ownership for homes.

Business process meeting(s) only – NHT is a consumer stakeholder of NIDS process.

Discussed data sharing, authoritative versus derived data sourcing and framework(s) for operation (akin to current sharing of TRN and NIS linkages). Data is currently shared/sourced via DVD (not in real time) on a periodic – as produced – basis.

FIREARM LICENSING AUTHORITY

- Standalone Executive Agency.
- Maintains an AFIS (Fingerprint)
- Issues a secure ID card – details to follow.

The Consultant Team has not yet had an opportunity to meet with the Firearm Licensing Authority to discuss details of the enrollment, issuance and management processes associated with Firearm Licensing. This report will be updated when specific details are available.

MINISTRY OF SCIENCE, TECHNOLOGY, ENERGY AND MINING (MSTEM)

A meeting was held with The Honourable Julian J. Robinson, Minister of State in the Ministry of Science, Technology, Energy and Mining and key support staff to understand the top-of-government priorities, issues and challenges. NIDS is a cross-cutting capability that can benefit all of Government – and as well enable private industry to provide better service to its stakeholders.

- eGovJa now reports into MSTEM.
- Mr. Robinson is supportive of NIDS and the objectives, concerned at the rate of implementation due to the challenges of coordinating across all of government.
- A Chief Information Officer (CIO) will be recruited as part of MSTEM.
    - Will have government-wide responsibility for ICT standards, including security and data protection. This would include NIDS.
- Legislation for Data Protection and to enable Data Sharing between Government organizations is in development but is not expected to be passed in the near future.
- Crime prevention is a big issue that NIDS could support.

PRIVATE SECTOR ORGANIZATIONS THAT COULD LEVERAGE THE NIDS FRAMEWORK

- Banks and other Financial Institutions
- Insurance Companies

- Private Educational Institutions and Universities
- Private Hospitals and Healthcare providers
- Employers
- Contract overseas employers
- Other to be determined

Appendix J: STAKEHOLDER QUESTIONNAIRE

The following Needs Assessment Questionnaire was submitted to stakeholders in advance of meetings and on-site visits.

NEEDS ASSESSMENT QUESTIONNAIRE

1. PROJECT PURPOSE

The overall objective of the project is the design and development of the ICT architecture for the planned implementation of a National Identification System (NIDS) for Jamaica. In order to arrive at the optimal identity framework, due consideration must be given to existing, relevant identity systems and the needs of the relying parties. A crucial initial step is to perform an information gathering exercise that will inform the Project Team of current capabilities, needs and requirements. These data points will form the foundation for ongoing analysis to ensure the developed ICT architecture provides a best-fit solution to present and future needs.

2. BACKGROUND DOCUMENTS:

The Consultants request that, as appropriate, each participating agency / registry / identity stakeholder to be interviewed provides any relevant background documents that will help the team better understand the structure, function, interdependencies, and processes used to manage those systems by their respective organizations. The team requests provision of such documents in soft copy (PDF, DOC, PPT, etc.), in advance if possible.

3. QUESTIONS / DISCUSSION TOPICS FOR STAKEHOLDERS:

The following baseline areas of discussion will help the Consultants develop a comprehensive understanding of the present status and forward developments, investments and ROI for a modern, interoperable National Identification solution.

Baseline areas for discussion (adjusted as appropriate for each stakeholder):

1. **Historical Perspective and Background on the Evolution of Identity Processes**
   - Evolution of the present system(s) and requirements
   - Understanding of critical constraints, including:
     - Volume requirements, including peak period production support
     - Business continuity

    - Service Level Agreements / Charter
- Perspectives on current evolution and previous initiatives

2. Legal Framework for Identity

- Legal and legislative mandates
- Policy
- Constraints and / or issues

3. Present Identity System(s)

- Rationale and criteria for selecting / implementing the present system(s)
- System description
    - Vendor and supply chain
        - Product release version
    - Hardware description
    - Software description (applications, databases, data models, etc.)
    - Technical standards used by the systems
    - Access control models (including remote access)
- Performance and results achieved
    - Performance shortfalls / issues
    - Data security, confidentially, integrity and availability (breaches, duplicate entries, etc.)
        - What audits (if any) have been undertaken, results (if known) – missing records, incorrect records, exception processing
        - Steps taken to prevent multiple applications / entries for a single identity
- Backups, redundancy and disaster recovery
- Environmental Controls (Fire suppression, HVAC, etc)
- Connectivity and communications infrastructure
    - Is there already some data sharing and/or intra-governmental links between stakeholders (e.g. registrar and electoral offices, etc.)
- Issues identified related to the system, including training, support, operations, location and dependencies of the system to other systems

4. Present Business Processes

- Current approach
- Business processes, including:
    - Enrolment
    - Identity vetting
    - Document production / printing

  - Identity management
  - Security Polices
  - Authentication
  - Software updates / patch managemect
  - Configuration management
  - Business continuity plan
- Identity numbering scheme structure and approach
- Current costs and charges (if any)
- Digitization of records
- Connectivity to other government systems and systems of record (for identity vetting and verification, delivery of e-government service, other)
- Challenges encountered and concerns
  - Enhancements needed / wanted
  - Counterfeit / fraud

5. Evolving Requirements and Challenges in the Design and Implementation of New ICT and ID Systems

- Pipeline – and timeline(s) – of ID system upgrades / updates / modernization
  - NIDS solution must support the current AND future environment
- Support for legacy systems and interdependencies
- Single points-of-failure

6. Inventory of Other Relevant Data Registries/Resources:

- Other identification used and accepted as an authoritative identity document

Appendix K: SOURCE REFERENCES

Ref #	Description
1	NIDS 2013 Draft Policy *Office of the Prime Minister, August 29, 2013*
2	NIDS 2012 – 3 Day Seminar – Civil Identification System Presentation *Nag Yeon Lee, March 29, 2012*
3	Case Study: The South Korea Civil Identification System *National Information Society Agency, February 2012*
4	Technical Committee Workshop Report *NIDS, October 6, 2011*
5	Comparative Data Schema *eGov Jamaica Limited, Undated*
6	Proposed Data Elements for NIDS *eGov Jamaica Limited, Undated*
7	A Comprehensive Review Document of Each Stakeholder Agency's (i) Existing Policies and Procedures, and (ii) Legal Framework that Guides Stakeholder Agencies *Lucretia Deean Fontaine, December 13, 2011*
8	Proposal for Technological Platform to Allow Interconnectivity and Interoperability Across Each of the Agencies' Systems *José Antonio López, Iván Alvarado, January 13, 2011*
9	A Methodology To Track An Individual's Vital History From Birth To Death Across Each Agency Collecting Vital Data, Given Each Agency's Respective Mandate, Roles And Functions. *John Louis Campbell, March 2012*
10	Detailed Report Outlining Legislative Requirements And Amendments Needed To Facilitate The Issuing of a Lifetime Identification Number. *John Louis Campbell, Lucretia Fontaine, September 2011*
11	Audit of Vital Registration and Vital Statistics Systems, July 20-July 29, 2005 Report of Findings and Recommendations *Vital Statistics Commission of Jamaica, August 31, 2005*
12	Vision 2030 Jamaica, National Development Plan *Planning Institute of Jamaica, 2009*
13	Vision 2030 - Social Welfare and Vulnerable Groups Sector Plan *June 2009*
14	Identification Management in Jamaica; Challenges Solutions and Lessons Learnt *Mrs Deirdre English Gosse, CEO, Registrar General's Department, July 2013*

Ref #	Description
15	NIDS Project Status *Presentation to NIDS 2012 Seminar, Denzil Plummer, March 2012*
16	NIDS & MLSS Social Services: Where Have You Been All Our Life? *Presentation to NIDS 2012 Seminar, Denzil Thorpe, March 2012*
17	NIDS Border Management & Control *Presentation to NIDS 2012 Seminar, Orlando Williams, March 2012*
18	Registrar General's Department *Presentation to NIDS 2012 Seminar, Gregory Gordon, March 2012*
19	MOH - GNU Topology Final With Map_15Jan2014 *Ministry of Health, January 2014*
20	MOH - WAN Drawing *Ministry of Health, January 2014*
21	MOH – GNU Health Components *Ministry of Health, Undated*
22	National Health Information System Strengthening and e-Health Strategic Plan 2014 to 2018 *Ministry of Health, October 2013*
23	eGovJa - Email Acceptable Usage Policy (EAUP) *February 2013*
24	eGovJa - Internet Acceptable Usage Policy (IAUP) *March 2010*
25	eGovJa - IT Acceptable Usage Policy *November, 2013*
26	eGovJa – Password Policy *March 2010*
27	eGovJa - Physical Access Control Standards & Procedures *November 2013*
28	eGovJa - Remote-Access Usage Policy *November 2013*
29	MOE – Unique Identification Number Concept Paper *MOE MIS Department, February 18, 2010*
30	MOE – The Unique ID Coding Structure *Ministry of Education, Undated*
31	MOE Management Information Systems (MIS) - Service Level Agreement (SLA) *Warren Vernon, Director Technical and User Support, February 6, 2011*
32	Role of the Trade Board Ltd. as Certification Authority *November 2008*

Ref #	Description
33	Overview of the Electronic Transactions Bill, 2006 *C. Earle, August 30, 2006*
34	The Electronic Transactions Act, 2006 *December 8, 2006*
35	The Representation of the People Act *As amended December 7, 2011*
36	Enhancing Border Security and Traveller Facilitation Using Advanced Passenger Information *Presentation to ICAO Ninth Symposium and Exhibition on MRTDs* *Biometrics and Border Security, Jennifer McDonald, October 2013*
37	Information Technology Diagnosis of the Jamaican National Insurance Scheme *C.C.R. Busby-Earle PhD, IDB Project Reference Code: JA-T1076, January 3, 2014*
38	RGD – NIDS Consultants Meeting Hand-out *Registrar General's Department, January 16, 2014*
39	RGD - Jamaica Flow Charts - Births Deaths Marriages *Registrar General's Department, October 2013*
40	RGD - Revised Registration Forms *Registrar General's Department, September 2010*
41	Responses to Needs Assessment Questionnaires *MOH, MLSS, TAJ, MOE, RGD, January 2014*