



**MINISTRY
HOME AFFAIRS
REPUBLIC OF SOUTH AFRICA**

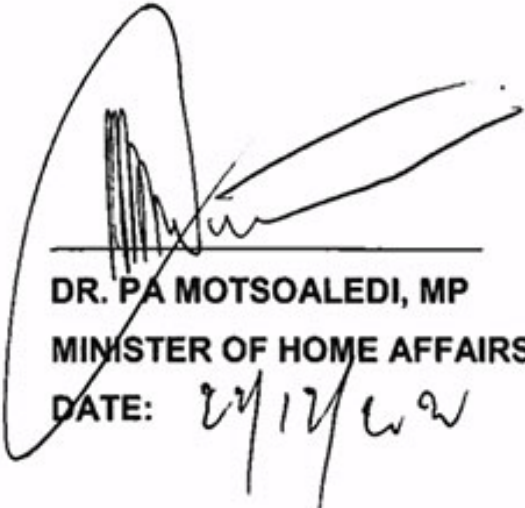
Private Bag X741, Pretoria, 0001 Tel: (012)432 6600 Fax: (012) 432 6637
Private Bag X9102, Cape Town, 8000 Tel: (021) 469 1600 Fax: (021) 461 4191

OFFICIAL IDENTITY MANAGEMENT POLICY

I, Dr Pakishe Aaron Motsoaledi, Minister of Home Affairs, intend in terms of section 85, sub-section 2 (b) of the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996) to publish the Official Identity Management policy for public comments.

Interested persons and organisations are invited to submit any substantiated comments or representation by no later than 28 February 2021. Written submissions can be forwarded to the following address:

The Director-General: Department of Home Affairs, Private Bag x114, Pretoria, 0001
For attention: Mr Sihle Mthiyane, Chief Director: Policy & Strategic Management
Alternatively via email: oimpolicy@dha.gov.za
Tel: 012 406 4353



**DR. PA MOTSOALEDI, MP
MINISTER OF HOME AFFAIRS**

DATE: 24/12/20



home affairs

Department:
Home Affairs
REPUBLIC OF SOUTH AFRICA

We Care!

DEPARTMENT OF HOME AFFAIRS

DRAFT OFFICIAL IDENTITY MANAGEMENT POLICY

PUBLIC CONSULTATION VERSION

22 DECEMBER 2020

TABLE OF CONTENTS

GLOSSARY	3
ABBREVIATIONS.....	6
SECTION A: BACKGROUND, ANALYSIS AND CONTEXT	7
Chapter 1: The Department of Home Affairs mandate.....	7
Chapter 2: Problem analysis and rationale for the identity management policy .	11
Chapter 3: Policy development approach	22
SECTION B: OVERVIEW OF IDENTITY MANAGEMENT IN SA	25
Chapter 4: Evolution of identity management	25
Chapter 5: Current policy and legal framework.....	28
SECTION C: POLICY FRAMEWORK AND OPTIONS	31
Chapter 6: Policy framework	31
Chapter 7: Policy analysis and options	34
SECTION D: ENVISIONED IDENTITY MANAGEMENT SYSTEM	51
Chapter 8: Key elements of the identity management system	51
Chapter 9: Legislative framework.....	57
Chapter 10:Funding model.....	60
SECTION E: IMPLEMENTATION STRATEGY AND ROADMAP	62
Chapter 11: Phased-implementation approach.....	62

GLOSSARY

Assigned sex: the sex category assigned to an individual by medical, legal, or other social authorities. Assigned sex is often determined to be either male or female based solely on a child's genitalia at birth, and it may not align with gender identity.

Biometric (biometric data): measurable biological or behavioural characteristic of a natural person that can be used to determine or to verify their identity; e.g. face, fingerprints and voice.

Biometric verification: automated verification of a person based on their biological and behavioural characteristics, e.g. the facial matching conducted by the FVS.

Civil registration: continuous/permanent, compulsory, universal recording of the occurrence and characteristics of vital events that could affect the legal status of individuals in a population such as birth, marriage or death. This means the State must record all the events in an individual's life, in line with decrees, regulations or laws of the country and fully respecting rules regulating the protection and privacy of individual information.

Consent: expressed or implied specific and informed permission given voluntarily by an individual with the capacity to understand their decision to offer the permission.

Credential: technology used to authenticate a user's identity (also referred to as an authentication credential). The user possesses the credential and controls its use through authentication protocols. A credential may be a username and password, cryptographic key or other form of secret used to verify a user's digital identity. To use a digital identity in requesting access to a resource, a subject presents an authentication credential. The credentials, once authenticated, are taken as proof that the subject owns the claimed digital identity, and that the subject is permitted to access the resources/services which are associated with their digital identity.

Data dump: transfer of a large amount of data between two systems, often over a network connection. For example, a database can be dumped to another network server, where it could be used by other software applications or analysed by a person.

Digital identity: a person's set of attributes that uniquely describes the person engaged in an online transaction under the identity ecosystem.

Gender: socially constructed roles, behaviours, and personal characteristics that a given society considers appropriate for men, women, and others. People whose gender is neither man nor woman may describe themselves as being in an intermediate state between man and woman, being both man and woman, being neither or belonging to another gender altogether.

Gender identity: an individual’s deeply-rooted internal sense of gender. This resource uses the term “trans” to include a diverse range of people whose gender identity is different from the sex they were assigned at birth.

Identity: a person’s set of attributes that uniquely describes the person within a given context.

Identity attribute: a piece of information relating to identity (e.g. full name or date of birth).

Identity theft: the deliberate use of the identity of another living or deceased person.

Intersex: an adjective referring to a person whose sexual anatomy, reproductive organs and/or chromosome patterns do not fit the typical definition of male or female. These anatomical differences are often perceived to be both male and female at the same time; not quite male or female; or neither male or female. These congenital differences in anatomical sex often result in physical differences in secondary sex characteristics such as muscle mass, hair distribution, breast development and stature.

Non-binary person: non-binary or genderqueer is a spectrum of gender identities that are not exclusively masculine or feminine – identities that are outside the gender binary (male and female). Non-binary identities can fall under the transgender umbrella, since many non-binary people identify with a gender that is different from their assigned sex.

Official identity: personal information including biometric data that is collected and stored by the DHA according to the established legislation.

Sex: a classification of people as male, female, indeterminate sex or intersex. Most individuals are assigned a sex at birth based on a combination of bodily characteristics such as genitals and internal reproductive organs, and less frequently based on their chromosomes.

Transgender: an adjective referring to a person whose gender identity or expression is different from their assigned sex.

Transition: the process that a trans person undergoes to live in their gender identity. It may include social gender recognition (e.g. changing one’s appearance), legal gender recognition (e.g. changing one’s name and sex / gender details on documents) and/or medical transition (e.g. hormones or surgeries that result in physical changes to a trans person’s body).

Validation (in an identity proofing context): a check that the attribute exists and is under the control of the individual (e.g. SMS activation code being sent to a mobile phone number to confirm control of the associated phone number).

Validation (in an integration testing context): testing a system under controlled conditions providing evidence that the system satisfies trust framework requirements and satisfies the intended use and user needs. Validation involves testing that functionality works as specified, designed and constructed, including intentionally making things go wrong when they should not and things happen when they should not (testing boundary conditions) to ensure that the system is robust when in production.

Verification (in an integration testing context): provides confirmation, using objective evidence, that trust framework requirements have been fulfilled. Verification involves evaluating whether a system complies with a regulation, requirement, specification, or imposed condition.

ABBREVIATIONS

4IR	Fourth industrial revolution
Abis	Automated Biometric Identification System
AU	African Union
DHA	Department of Home Affairs
EMCS	Enhanced Movement Control System
Hanis	Home Affairs National Identity System
ICAO	International Civil Aviation Organization
ID	Identity document
MCS	Movement Control System
NIIS	National Immigration Information System
NIS	National Identity System
NPR	National Population Register
POPI	The Protection of Personal Information Act 4 of 2013

SECTION A: BACKGROUND, ANALYSIS AND CONTEXT

Chapter 1: The Department of Home Affairs mandate

1.1 Overview of the DHA mandate

The Department of Home Affairs (DHA) mandate straddles a number of essential elements of all South Africans' lives, including activities carried out by the private sector. The DHA is the sole authority and has a leadership role in South Africa on identity, identity management and identity management systems across government and economic spheres.

The DHA's sole mandate includes the sole authority to affirm and regulate official identity and South African citizenship. To fully appreciate the DHA's mandate, the Constitution of the Republic of South Africa is the first and primary point of reference. The Constitution's provisions are accompanied by the concepts of sovereignty, identity, citizenship, national security interests and actively enabling citizen empowerment and economic development. In promoting and fulfilling the Constitution's provisions, the DHA is mandated to develop and manage an identification system. According to the Constitution, no citizen may be deprived of citizenship (Section 20), every child has the right to a name and a nationality from birth (Section 28(1)(a)), everyone has the right to leave the Republic (Section 21(2)), and every citizen has the right to a passport (Section 21(4)). Also of direct relevance is a just and efficient administration as defined in Chapter 10 of the Constitution.

The mandate and strategic relevance of the DHA is expressed in the *White Paper on Home Affairs* (the White Paper) as follows:

- Mandate one: Management of citizenship and civil registration
- Mandate two: Management of international migration
- Mandate three: Management of refugee protection

The DHA has a sole mandate over its services, unlike other government departments such as Health and Education whose services can be privatised. Only the DHA can affirm a person's identity, issue a South African identity document or passport and register a birth, a death or a marriage. No other department can affirm or grant citizenship. Only the DHA has the authority to allow anyone to enter or leave South Africa, and to issue a permit and a visa. Only the DHA can grant asylum seeker or refugee status.

The overarching importance of identity and identity management is evident and clear in this mandate. As observed in the White Paper, managing identity and the status of legal

persons in a society, particularly in a modern society, continues to be essential for societies to organise work, distribute resources and ensure that people's rights and identities are protected. And where those looking for economic opportunities and those who claim asylum create a movement of people, managing migration means minimising risks while maximising the benefits of migration in terms of knowledge, productivity and trade.

In realising the goals of the mandate, the DHA is structured around two pillars of its programmes and work. The first is the programme on citizen affairs, which covers the activities of the Civic Affairs branch at national and provincial levels. This involves providing and managing the identity and status services for citizens, permanent residents and persons accorded refugee status. The second is the programme on immigration affairs, which is responsible for implementing immigration legislation, managing the immigration system, functions at ports of entry, the immigration inspectorate and deportations, the visa and permitting regime, and processing asylum seekers and refugees.

1.2 DHA as a custodian of identity management in South Africa

The policy framework and laws that enable the State to establish the legal status of every individual in South Africa is the foundation of our sovereignty and the legitimate exercise of State power. Affirming the identity and status of every citizen at birth is indispensable for the State, which must respect, protect, promote and fulfil their constitutional rights.

The third clause of the founding provisions in Chapter 1 of the Constitution states, "National legislation must provide for the acquisition, loss and restoration of citizenship". Without a national register of citizens, this obligation cannot be fulfilled and there cannot be "Universal adult suffrage and a national common voter's roll..." as prescribed in the first clause.

The very notion of sovereignty and the legal status, integrity and security of the South African State, South Africans and all members of society rest, to a large extent, on the information and functions that are within the legal jurisdiction of the DHA. This is a reference to identity as a legally established concept composed of specified information.

The DHA's core functions are a fundamental part of all human societies. Throughout history, managing identity and status has been essential for societies to organise work, distribute resources and ensure that people's rights and identities are protected.

Identity refers to the unique set of identifiers that distinguishes an individual from all other individuals. In modern states the key identifier is typically a unique number allocated soon after birth, and can be linked to that person by biometrics and other means.

Status is the assigned category of persons based on shared criteria, such as being citizens of a country, married, a child, a voter or a mother. Civic status refers to criteria attributed to citizens by a state, typically including a record of vital life events such as marriage.

The DHA plays a central role in both the State and society through its mandate, responsibilities and functions as stipulated in various Acts including the Identification Act 68 of 1997.

The Identification Act makes provision for compiling and maintaining the population register for the population of the Republic. It also provides for issuing identity documents to persons (citizens and permanent residents) whose particulars are included in the population register. In 1982, the DHA established the national population register (NPR) to enable it to store biometric data (fingerprints and face image) and other data specified in the Act. This register can be used to determine a person's identity, linked to the biographical information and personal information for civil registrations, and compile and store particulars as stipulated in the Identification Act. However, as the NPR is outdated and only data stores are limited to citizens and permanent residents, it will be replaced by an inclusive and secure National Identity System (NIS). The NIS will store the particulars of all persons, citizens and non-citizens who are within the territorial jurisdiction of the country. The NIS will be the backbone of identity management and cut across the social, political and economic spheres.

The DHA is the established legal institution within the South African government mandated to carry out the responsibility for identity management. The identity management policy establishes the vision, goals and objectives, as well as the approach that the DHA adopts towards establishing a modern and secure NIS. The NIS will become the backbone for systems, networks and platforms to facilitate providing goods and services to citizens and other legal persons, in the government-wide consolidation of processes and systems to enhance national security and in the contribution to economic development and growth.

Accurate and reliable data and information on all South Africans such as birth, marriage, death records and other vital statistics is a necessity for planning and formulating appropriate policy and programme responses to cater for the needs of South Africans. All these are essential services offered by the DHA. The policy on identity management is anchored in the DHA's crucial role as part of this critical function, as demonstrated when the State provides socio-economic goods and services such as non-contributory social assistance, housing, education and healthcare services to its citizens and other legally

prescribed persons. In addition, for the economy to function to its full potential, identity management is used in various forms through multiple channels, technologies and innovations by the private sector and its markets in financial services and transactions.

Identity management, under the DHA's legal mandate as the sole provider of official identity and civic status verification in South Africa, is an important and pressing issue given the technological advances unfolding globally, especially the growth of the digital economy. Innovations and new technologies are sweeping the globe at rapid pace, including here in South Africa, and are rapidly disrupting and changing the way we all behave, live and work. This phenomenon has been dubbed the fourth industrial revolution (4IR), also known as the digital revolution, and marks a major turning point in our collective local and global development.¹

Identity management in its multiple forms is an integral part of this era of 4IR, the digital economy, e-identity, national security, global threats, and the use of technology by governments to improve the quality of life of citizens. The ever-changing, technology-driven context and environment is accompanied by demands from stakeholders within and outside government, with economic activity demanding digital automation.

The 4IR has implications for South Africa in identity management, digital identity development, cybersecurity, the digital economy and other new technology-driven frontiers. South Africa's sixth administration saw the former Department of Communications, Telecommunications and Postal Services becoming the Department of Communications and Digital Technologies², with a context-relevant mandate. This indicates an awareness of the pressure exerted by an external national and global environment that is adopting new digital technologies to which governments have to respond. For these reasons, the DHA is building an NIS that is inclusive, digital, secure, accurate, confidential and responsive.

¹ Project iKUSASA: A Digital Roadmap to a Modernised, Future-fit DHA. In this document, the DHA of the future is described as 'a digitally-led organisation that is responsive to the changing needs of South Africa's citizens and other stakeholders as well as the opportunities that digital thinking provides to promote value-for-money service delivery.'

² In South Africa the raising, at the national level, of digital technologies to the political and policy levels demonstrates the emerging appreciation by the sixth administration of the pervasive impact changes in this area will have on South Africa and its systems in government and the private sector.

Chapter 2: Problem analysis and rationale for the identity management policy

2.1 Problem analysis

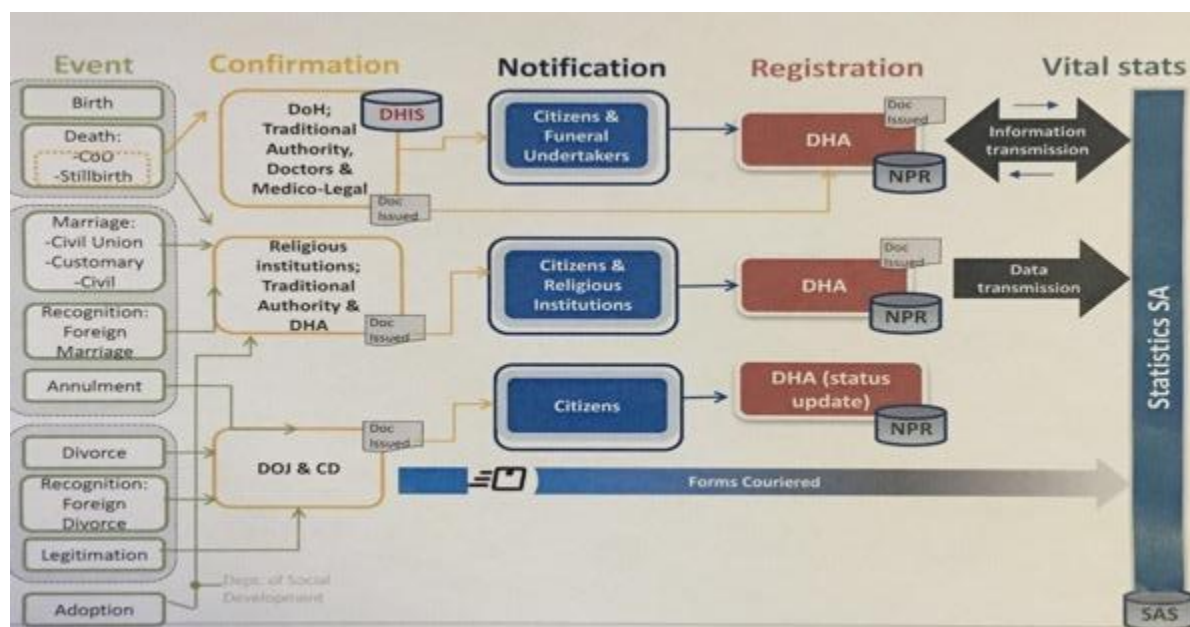
The Identification Act is now more than 20 years old. It is not based on a policy that considers key local and global developments in managing official personal information. This in part explains why the current legislation and systems are outdated, fragmented and do not fully align with constitutional principles of equality, non-discrimination and human dignity.

The integrity of the population register depends on the integrity of all the primary data systems, which must meet high standards of security, as specified in relevant Acts, and produce data that is accurate and reliable. While it is important to secure and modernise the DHA identity management system, the continued reliance on primary systems that are manual and insecure poses a serious risk to the accuracy of the population register. The following systems or processes provide primary data that is used to affirm identity or status to the applicant:

- Notification of birth from the Department of Health
- Notification of death from the Department of Health
- Notification of death from funeral undertakers
- Affidavits from traditional leaders and school principals for late registration of birth and claim for citizenship
- Abridged marriage certificates from religious marriage officers
- Divorce decrees from the Department of Justice and Constitutional Development
- Letter of non-impediment from a foreign country confirming that a non-citizen who intends to marry in South Africa is not married in the country of origin
- Police clearance form from a foreign country confirming that a non-citizen who is applying for a residence status in South Africa does not have a criminal record in the country of origin
- Bank statements from a foreign country confirming availability of the required bank balance in the account of a non-citizen who is applying for residence status in SA.

Figure 1 below illustrates some of these primary systems or processes that provide the critical information required by the DHA to affirm identity or status. These systems will continue to compromise the new population register if they are not modernised or secured.

Figure 2.1: An overview of the civic registration and vital statistics interface



Source: Statistics South Africa: South Africa's progress in civil registration

The DHA realises that the identification data at its disposal, including both civic status and immigration data, has a broader value than the core administrative purpose it currently fulfils. For instance, the DHA requires a regulatory framework for enabling e-government and e-commerce.

The DHA is currently operating without an approved identity management framework. This framework needs to address how the DHA will regulate the manner in which personal information will be processed by establishing conditions that meet the minimum threshold requirements for the lawful processing of personal information contained in the Protection of Personal Information (POPI) Act 4 of 2013. It will also be necessary for the DHA to articulate how the digital administrative datasets under its control will meet the requirements of both the contemplated privacy impact assessments in terms of POPI, and the cybersecurity audits in terms of the Cybercrimes and Cybersecurity Bill. Where the data handled by an organ of state qualifies as personal information that organ of state must establish a specific identity management policy to ensure compliance with POPI. Where an organ of state's system is classified as critical information infrastructure, a framework must be set in place to ensure compliance with the provisions of the Cybercrime and Cybersecurity Bill and independent audits of this must be undertaken from time to time.

The DHA, through both internal processes and external assessments, has confirmed and expressed the contextual, systems-related and operational problems and challenges in-house, within government and externally. The White Paper (December 2019) alludes to

the many factors constituting obstacles. It observes that, by 2016, it was evident that the DHA's existing operational, organisational and funding models were constraining the modernisation process with negative consequences for its sustainability and effectiveness. The White Paper further observes that the following three significant shifts had to happen to complete the modernisation process and deliver on the DHA's mandate:

- i. Firstly, how the DHA is perceived must shift towards an understanding that its full mandate is a key enabler of citizen empowerment, economic development, efficient administration and broadly defined national security.
- ii. Secondly, the DHA must be positioned as being central to building a capable State that can confront extreme inequality, poverty and the impact of 4IR.
- iii. Thirdly, the DHA must realise its vision of becoming a fully modernised, secure department with professional staff (in the broad sense of the term) and appropriate operating, organisational and funding models.

The DHA as an institution in the current social, political, economic and global environment has to change and adapt. The reasons behind this change are:

- historical
- related to alleviating threats to the nation and are bound, significantly so, to the unfolding future that is fundamentally shaped by the adoption of advanced technologies
- evolved identity management that now has digital technology at its core.

In this context, the **historical legacy of the apartheid systems** that separated South Africans into different geographic and separate identity enclaves in the white Republic, ethnic homelands and self-governing territories is a factor to be considered. The apartheid ideology meant that the areas where the black majority population lived were severely underdeveloped and under serviced. Some of the daunting challenges the DHA faces are rooted in South Africa's history of a system that differentiated South Africans based on race and geographic origin and enshrined them in the separation of the former Republic of South Africa from the homelands and self-governing territories. This system was pursued through laws, regulations and practices that deeply politicised and racialised the allocation of resources and infrastructure, and building systems that could adapt to a changing global context. This bequeathed the post-apartheid government and the DHA with monumental challenges in infrastructure, systems and personnel.

In the DHA circumstance, the **technological advances shaping identity management and systems** are best represented by the change over decades from South Africa's Identity books of the early 1960s, where a fading photo, typed biographical information, handwritten entries and manual ink fingerprints imprinted on paper were the totality of what constituted identity. At the moment digital platforms and networks form the

backbone of the global financial enterprise that is led by financial institutions such as banks. Central to this is biometric data, which now includes fingerprints, iris reading, facial recognition and DNA, e-identity, e-government and e-commerce. The impact of these technological advances lies in how government services are provided and how governments facilitate and enable this widening economic activity.

National security and the protection of South Africa's sovereignty, the security of the State and citizens, and the integrity of the NIS is another factor. This comes from a number of considerations including the fight against the global threats of local and international crime syndicates and global terrorism, and taking steps to ensure that government services, on which multiple trillions of rand are spent, are enjoyed by those with rights and entitlements to them.

National developments in South Africa on identity management are linked to international developments, as changes and trends at the global level directly affect and influence South Africa's position and actions on identity management. South Africa's capability to facilitate and secure the application tourist and business visas, matched with migration control through a seamless digital system that employs modern and secure technologies and systems on identity authentication, stands to boost South Africa's economy through trade and investment in the country.

In South Africa providing and accessing goods and services that citizens and residents are entitled to depend on identity instruments issued by the DHA. This leads to a substantive policy, programme, implementation and operations relationship between the DHA and other government departments and State entities, based on the goods and services from the State to citizens. There are many stakeholders and actors in the area of identity management within and outside government. In the private sector, stakeholders, especially financial institutions, operate with business systems that require real-time verification services that are provided by the DHA through its legal mandate. Because of its multiple stakeholders and actors, and in promoting e-government through platforms for data sharing and processes, the DHA categorises several service-oriented streams of its work into:

- government to government programmes (G2G) – is concerned with interaction between different levels of government and collaboration with government agencies
- government to citizen programmes (G2C) – involves an interaction between government and its citizens
- government to employee programmes (G2E) – this involves the relationship between government and its employees. This form is considered an effective way of bringing employees together and promoting knowledge sharing among them

- government to business programmes (G2B) – this is concerned with supporting business activities.

Identity management has to be considered beyond South Africa's Borders. South Africa's own national developments on identity management have to take full cognisance of the fact that South Africa is part of the Southern African Development Community and the African continent through membership of the African Union. South Africa participates in the Southern African Development Community in areas such as identity management and financial transactions, the vision and policies of the African Union and Agenda 2063, and in multiple forums that are part of the international and global community. This means that ideas, views and developments from these forums will shape in remarkable ways the national South African agenda and practices in identity management.

2.2 Root cause analysis

The objective of this section is to assess the extent to which the challenges facing a secure and inclusive population register originate from a lack or insufficiency of a policy and legislative framework, and outdated and fragmented systems or administrative weaknesses.

2.2.1 Accessibility and barriers to inclusion

There are vulnerable groups that face significant economic and social barriers to enrolling in or using the South African identity system. Unless the identity system and its implementation are designed to help people overcome these barriers, it is likely these vulnerable segments of the population will have lower rates of coverage. While South Africa has made great strides towards ensuring that no one who lives in the country is left without a legal record of existence, there are still people (including citizens) who remain either undocumented or improperly documented. This group includes non-binary persons, people who did not acquire birth certificates earlier in life and now require late registration of birth, children of non-citizens who were born in South Africa, and those who are either excluded or improperly documented for historical reasons such as the borderline communities and KhoiSan people.

Abandoned children are excluded because of the requirement for identity details for parents at registration. Children abandoned by their parents are left in the care of their relatives who often do not have the required birth registration information. This means that the absence of a parent or legal guardian poses challenges for birth registration. There is a solution to this problem, but illiteracy and affordability issues worsen the situation. Children of teenagers who have not reached 16 years and do not have parents nor informants are unable to register the birth of their children. Children of asylum seekers who are not included in the file of the asylum seeker are excluded from the identity system

because of difficulty in providing documentation or other evidence such as paternity test for identity proofing.

Gender and sexual identity minorities are excluded because the current laws and policies do not cater for changes in the gender/sex attribute of the identity system. They experience discrimination when attempting to register or update their gender in the ID system.

Poor people, rural residents and many elderly people face logistical and travel challenges. The direct and indirect costs such as fees, travel and lost wages associated with the application for, or use of, identity credentials are prohibitive to them. They also lack smartphones or other resources to access online or digital services or use credentials. The elderly also have difficulty providing biometrics and have limited access, or literacy to access, digital services. Persons with disabilities also lack mobility and/or accessible centres, which may hinder registration. The DHA may also lack trained staff and accommodating enrolment procedures. People with lower levels of literacy have difficulty completing applications as forms are either written in English or Afrikaans. These barriers constitute a root cause for exclusion of vulnerable groups.

It is currently possible for anyone who has not applied for an ID (smart ID card or ID book) to successfully claim and use the identity of another person who has also not applied for an ID. This is possible because children's biometrics were not captured. The DHA currently has no way to reliably verify that a child who presents a birth certificate as proof of identity during interactions with the department, e.g. when applying for an ID for the first time, is truly the person whose birth the certificate is meant to certify. Any child can lay claim to the identity of another child and such instances have been recorded. For instance, there is a practice, especially in borderline communities, where birth certificates of deceased children are sold to foreign nationals. This happens when the death of a child is not reported to the DHA. The DHA aims to deal with this fraud by capturing children's biometrics when their births are registered to reliably verify their identities during subsequent interactions with the department and other institutions. However, not all biometric traits captured from children shortly after birth can be used to verify their identities later in life.

2.2.2 Interoperability and integration of identity management systems

Interoperability is crucial for developing efficient, sustainable, and useful identity ecosystems. Specifically, interoperability is the ability of different functional units – e.g., systems, databases, devices, or applications – to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units. The South African identity system itself does not have standards-based

technical interoperability and therefore does not allow different components and devices to communicate with each other and work together.

The DHA, in realising its mandate, uses the following core information technology (IT) systems to record, store and/or process citizens and non-citizens' biographic and biometric data, as well as their movements into and out of South Africa:

- (a) NPR, which is used to record, store, and process citizens and permanent residents' biographic data, and limited biographic data for refugees
- (b) National Immigration Information System (NIIS), which is used to record, store and process biographic, biometric and supporting data (audio files and scanned documents) of refugees and asylum seekers
- (c) Movement Control System (MCS) and the Enhanced Movement Control System (EMCS), which are used to record and store the movement data of people across South African ports of entry. MCS is further used to record other data related to the movement of people across ports of entry, including visas, v-lists, etc.
- (d) Visa Adjudication System (VAS), which is used to record, store, and process mostly biographic data and the supporting documents of people who apply for South African temporary and permanent residence permits in South Africa
- (e) Visa system, which is used to record, store, and process mostly biographic data of people who apply for South African temporary residence permits at South African missions abroad
- (f) Home Affairs National Identity System (Hanis), which is used to store and process the biometric data of citizens and non-citizens (refugees, asylum seekers, illegal foreign nationals and permanent residents). This system will be replaced in the immediate future by the Automated Biometric Identification System (Abis), which will process and store biometric data of all persons, citizens and non-citizens.

Therefore, the data of a person is, in most cases, stored on more than one system, e.g. the data of a citizen who has travelled outside South Africa exists on the NPR, and on the MCS and/or EMCS. In addition, the systems may store the same data in different ways, e.g. names.

However, the systems are generally not linked and do not communicate directly to exchange data; e.g., an update of the common data is not automatically updated on all the relevant systems that have the same data. This means that it is possible to change a person's ID number on the NPR without also changing the ID number on MCS (and/or EMCS). This effectively breaks the link between a person's data on the NPR and their data on the MCS (and/or EMCS), giving the appearance that the person has never travelled and rendering the person's data inaccurate.

The department plans to address this challenge and other data challenges by developing the NIS, which will be the single source of all DHA client data. It will consolidate the data stored on the NPR, NIIS, MCS, EMCS, VAS and the visa system into one database, and serve as the link between other systems and Abis, i.e. insertion of and access to the biometric data stored on Abis will be through the NIS.

2.2.3 Data protection and privacy

According to best international practice, ensuring data privacy and security requires a holistic approach to system design that incorporates a combination of legal, administrative and technical safeguards. South Africa has adopted general data protection and privacy laws that apply not only to the identity system, but to other government or private sector activities that involve processing personal data. Section 14 of the Constitution protects the right to privacy. The POPI Act regulates processing personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests. In a nutshell, the POPI Act aims to promote protection of personal information; give effect to the constitutional right to privacy; and prohibit unlawful collection, dissemination and use of personal information. It further provides a framework for handling personal information.

The Identification Act and Alteration of Sex Description and Sex Status Act 49 of 2003, are key legislation that regulate how personal data that is hosted in the DHA identity management systems is handled. The legislation needs to be amended to regulate handling personal information in line with the Constitution and the POPI Act. The current practice of dumping the department's data on other government systems is contrary to the POPI requirements.

2.2.4 Institutional oversight on data protection and privacy

International best practice dictates that data protection and privacy are subjected to the oversight of an independent supervisory or regulatory authority to ensure compliance with privacy and data protection law, including protecting individuals' rights. The POPI Act established the Information Regulator, an independent body subject only to the Constitution and to the law. This body is appointed by the President on the recommendation of the National Assembly, after nomination by a committee composed of members of all the political parties represented in the National Assembly.

The powers, duties and functions of the South African Information Regulator are aligned with the international best practice powers and duties. However, the Information

Regulator is not yet fully functional and able to legally deal with some key aspects of data protection such as data leaks. This is an institutional root cause for the lack of data protection and privacy.

2.2.5 Data security

In keeping with international best practice, personal information should be stored and processed securely and protected against unauthorised or unlawful processing, loss, theft, destruction or damage. This principle becomes increasingly important for digital identity systems given the threat of cyber-attacks. In South Africa, the POPI Act requires the Information Regulator, to notify the data subjects of breaches as soon as reasonably possible after the discovery that they have been compromised, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

2.2.6 Data sharing

According to international best practice, there are potential benefits of information sharing such as better government service delivery, improved risk management and cost savings as duplication of effort is eliminated. However, information sharing between state institutions, if not well regulated, can enable circumvention of individual privacy and data protection safety measures. The POPI Act effectively grants the right to privacy as contained in the Bill of Rights and is widely regarded as being a codification of the common law position regarding processing personal data.

2.2.7 User consent and control

In accordance with international best practice, an individual's personal data should only be collected and used with the consent of that individual unless there is another basis in law for such collection and use. There must be a valid lawful basis for processing personal data. One such lawful basis is consent of the individual. Where consent is relied on, it must be freely given, specific, informed, unambiguous and signifying agreement to personal data being processed. Where the personal data being processed is special category data such as biometric data, additional conditions to processing must be satisfied, one of which is obtaining the individual's explicit consent to the processing.

Explicit consent must be provided in a clear statement – whether written or spoken. An explicit consent statement will also need to specifically refer to the element of the

processing that requires explicit consent. The POPI Act makes the provision that personal information may only be processed if the data subject or a competent person – where the data subject is a child – consents to the processing. The POPI Act also states that the responsible party bears the burden of proof for the data subject's or competent person's consent.

2.2.8 Cybercrime and cybersecurity

Cybercrime may have a wide range of meanings depending on the country, legal instrument and context in which the phrase is used, but according to best international practice, a country should have laws in place addressing criminal conduct directed against the confidentiality, integrity and availability of computer systems and networks, as well as the data stored and processed on them, and criminal acts carried out through the instrumentality of such systems, networks and data. South Africa currently does not have any legislation on cybercrime and cybersecurity. Since 2015, the government has been working on cybercrime and cybersecurity legislation with the stated aim of bringing South African law in line with international standards and creating specific offences for cyber-related crime such as online fraud, forgery, extortion and terrorism.

In 2017, Parliament began deliberations on the Cybercrimes and Cybersecurity Bill. The 2017 version of the Bill contained a provision concentrating cybersecurity powers in the hands of intelligence agencies and potentially criminalising free expression. In October 2018, Parliament began deliberations on a significantly revised version of the Bill, referred to as the Cybercrimes Bill. However, the Bill has yet to be adopted by both houses of Parliament and signed into law, which is a root cause for the lack of cybercrime and cybersecurity legislation.

2.2.9 Identity authority and governance structure

Identity authorities are specialised entities responsible for implementing and/or overseeing personal identity data collection, verification, storage and sharing; issuing credentials, and verifying and authenticating identity data. They are also typically responsible for public engagement and redressing grievances. For an identity system to succeed, this entity must be empowered by law and political will and should demonstrate the capacity to serve as a champion of identity, a convener of multiple stakeholders and an effective implementer and/or overseer.

In South Africa, civil registration and the NIS operate under the auspices of the same entity – the DHA – which is responsible for civil registration and national identification, immigration and border management, and refugee management. The DHA is therefore a

single, dedicated entity for identity management in South Africa, yet South Africa does not have a legislation that identifies and affirms the DHA as the sole provider of official identity management services. There are other entities within and outside government that are providing related services.

However, the DHA appears not to be well equipped with sufficient and capable human, financial and technological resources to efficiently carry out its mandate, implying a potential institutional root cause for not administering official identity management.

Chapter 3: Policy development approach

3.1 Scope

The policy will provide a constitutionally sound framework for regulating the following critical elements of identity management:

- Recognise equality, non-discrimination and human dignity values in managing the official identity and status of all citizens and non-citizens who interface with the DHA.
- Recognise the identity number, identification credentials (birth certificate, identity card/document and passport) and biometric data as the sole sources for verifying citizen identities.
- Recognise the passport number, identification credentials (visa and permit) and biometric data as the sole sources for verifying identities of foreign nationals within South Africa's territorial jurisdiction.
- Recognise the identity number and biometric data as the sole sources for accessing government services such as social services and for paying tax.
- Reposition the DHA as the sole provider of official identity and civic status verification services.
- Establish rules that govern accessing and processing population register data in line with relevant policies and legislation.
- Replace the NPR with an inclusive, digital population register that is secure, accurate and confidential.
- Establish the NIS to interface with other government identity management systems and generate the critical data needed by e-government and e-commerce to function.
- Apply for DHA services via multiple digital channels.

3.2 Out of scope

The Official Identity Management Policy does not deal with the following policies or processes:

- Policies and processes to attain citizenship

- Policies and processes to attain immigration status in the country
- Policies and processes to grant refugee status
- Policies and processes to determine who qualifies for which government services.

It is important to emphasise the following principles as we develop the policy:

- No one, irrespective of their status, should be left without a legal record of existence (**scandal of invisibility**)
- Being included in the population register does not translate to any status (immigration or citizenship) other than that your identity is properly documented in the country.

3.3 Policy objectives

This policy is developed with the following objectives in mind:

- Enable an inclusive digital population register that is secure, accurate and confidential
- Position the DHA as the sole provider of official documentation relating to the identity of civic and international migration status of citizens and foreign nationals within South Africa's territorial jurisdiction
- Position the DHA as the sole provider of official identity and civic status verification services
- Establish rules that govern accessing and processing population register records and data in line with relevant policies and legislation such as the POPI Act and the Cybercrimes Bill
- Establish the NIS to generate critical data needed for e-government and e-commerce to function
- Enable an application for DHA services via multiple channels.

3.4 Methodology

Globally there are a number of organisations and forums that investigate identity management and identity management systems. The World Bank, with its Identification

for Development initiative working with many global partners, has become an indispensable resource on identity management.

As part of the process of developing a policy on identity management, the DHA researched and analysed international and regional developments in identity management. The research surveyed the systems and practices of countries that are considered internationally to be advanced, intermediate or emerging in their development of secure, digital and interoperable NISs. The research collected information at international and regional levels and also explored the key documents and studies carried out in different regions and countries of the world. The approach was to look at the following seven dimensions in each of the countries investigated.

- i. Description of the national identity management system
- ii. Establishment of the national identity management system
- iii. Management of the national identity management system
- iv. Digitalisation of the identity management system
- v. Maturity of the national identity management system and integration with other services
- vi. Data sharing and processes or procedures governing access to national identity
- vii. Statistics on coverage of the identity management system.

The international and regional analysis demonstrated the complex, evolving social, economic and technology-driven environment with multiple stakeholders and actors in identity management systems.

The seven dimensions were then applied to the South African context.

The research was complemented by a comprehensive consideration of national developments in South Africa on identity management and related challenges. The outcome pointed to the current status at DHA and the multiple challenges that have to be addressed on the path to a modern and secure NIS and an identity management policy. National developments highlighted the need for integration and building synergies within government, and for enhancing and strengthening the interface with private sector institutions by exploiting modern secure technology. This process culminated in the first draft of the Identity Management Policy being developed.

SECTION B: OVERVIEW OF IDENTITY MANAGEMENT IN SA

Chapter 4: Evolution of identity management

4.1 Introduction

This section considers the interplay between national, regional and international developments on identity management. Under these circumstances, the DHA has to respond to broader national and international issues and global developments on identity management. This translates into the DHA adapting, adopting, using and exploiting that which serves South Africa's national interests.

In the post-apartheid period since 1994, the DHA has undergone several phases in terms of its strategic goals, focus of functions and operations. The historical legacy of the apartheid systems with the then Republic of South Africa, the TBVC states and self-governing territories meant that the attention was on building a unitary State with one single central authority. Consequently, the years 1994 – 2007 saw the DHA driven by the imperative to bring all South Africans into a single NIS by registering all citizens of the new Republic South Africa into one NPR. This critical initiative was accompanied by extending and expanding DHA services to areas that were historically underserved in terms of both infrastructure and services. Today, the DHA has mobile units that reach areas without infrastructure and is a remarkable and innovative method for taking services to all South Africans and advancing the agenda and principle of inclusivity.

4.2 Modernisation programme

The current DHA systems are not integrated and many processes are largely paper-based. Changes to identity and status that are made in immigration systems are only partially reflected in the NPR, using lengthy manual processes that are not reliable. The NPR was designed in the 1980s and data is often inconsistent or missing. Biometric and biographical data are stored on a mixture of paper and digital records that are neither reliable nor sufficiently secure. The existing operating model is based on one used before 1994 by "white" Home Affairs, characterised by clients queuing before a front office clerk to complete forms.

The DHA initiated a modernisation programme in 2012 with the aim of integrating and digitising its systems, and transforming its delivery systems to achieve the strategic objectives of inclusivity, national security, service delivery and meaningfully contributing to the government-wide agenda of a growing, inclusive economy. The goal

of the modernisation programme is to build a Home Affairs that has replaced its legacy systems with multiple channels and integrated digital systems. The assumption is that these systems will be very secure, professionally managed and appropriately funded.

The new DHA systems and operating model will be built around the new NIS and linked to the systems for the civil registration of birth, nationality, citizenship, marriage and death. It will also be linked to the MCS and other immigration systems. The NIS will enable the DHA to manage all its functions efficiently and responsively, as the NIS will link the identity of all citizens and other persons in a country to their civil and immigration statuses. Interfaces between systems will mean that data is accurate and continually updated in real time.

The modernisation programme consists of multiple projects: short-, medium- and long-term. Elements that are being rolled out include the smart ID card, fully digital ID and passport processes, online capture of biometrics at ports of entry and upgrades to the movement control and biometric systems. An automated system for asylum seekers to make appointments was designed and installed by the DHA at the newly opened Desmond Tutu Refugee Centre, greatly reducing fraud and human rights abuses and increasing efficiency. An in-house contact centre was opened in 2015/16, which was one of the key elements of the new operational model.

Given its limited resources, the DHA has entered into partnerships to improve access by creating new channels. A partnership agreement with the major banks allows their clients to access a DHA service point. They apply and pay for a smart ID card or passport online and make an appointment to complete the process at a bank. An SMS advises them when to collect the document at the bank. A partnership with a visa facilitation service led to the company creating service points in several countries abroad and in major South African cities. Applications are sent digitally to the DHA, where adjudicators complete the process. Together with local development agencies, the DHA has extended the service to create one-stop centres for businesspeople in major cities.

This third phase of the DHA's transformation promises a clear path towards digitisation and attaining a paperless environment. In a nutshell, the achievements of the modernisation programme include the following:

- Automated ID and passport processes into Live Capture
- Rolled out the Live Capture system to 193 offices
- Integrated and updated the payment system into the Live Capture system
- Enabled online services through the new eHomeAffairs portal
- Rolled out capturing smart ID cards and passports with the banks
- Rolled out smart ID cards, with the milestone of more than 12 million cards reached in March 2019
- Established a new contact centre

- Implemented online verification, resulting in birth, marriage and death certificates and temporary IDs being issued on the spot
- Deployed the Queue Management System at Live Capture offices
- Implemented the EMCS at 70 ports of entry
- Implemented a paperless process at Marabastad, now Desmond Tutu Refugee Centre
- Abis to replace Hanis
- Launched the e-visa system.

4.3 Repositioning programme

Repositioning the DHA from administration to key contributor to strategic national security came about in March 2017, with Cabinet approval. Central to this new security-related mandate is the capability of the DHA to protect South Africa's people, systems and data. The DHA has identified the following overriding strategic objectives:

- Establish and maintain a secure, comprehensive and reliable register of the identity and status of all citizens, as well as all foreign nationals in South Africa.
- Establish and maintain a secure and efficient system of immigration management that is used strategically to minimise risks and maximise the benefit of immigration.
- Establish and maintain world-class standards in delivering secure and reliable identity, civil registration and immigration services by patriotic, professional and caring staff.
- Establish a Home Affairs that has the policies, people, processes and infrastructure required to secure its systems and deliver world-class services.

Chapter 5: Current policy and legal framework

A number of policies and legislation have an impact on official identity management.

5.1 Policy framework

- **Constitution of South Africa 1996:** The Constitution of South Africa provides for the right to privacy in terms of the common law and section 14.
- **White Paper on Home Affairs 2019:** Through this proposed White Paper, the DHA is positioning itself to deliver effectively against its mandate as a critical enabler of citizen empowerment, economic development, national security and an efficient State.
- **White Paper on Science, Technology and Innovation 2018:** This White Paper focuses on using Science, Technology and Innovation to assist in solving problems that, among others, are associated with rapid technological advancement, geopolitical and demographic shifts, and 4IR.

5.2 Legal and regulatory framework

5.2.1 DHA internal:

- **Alteration of Sex Description and Sex Status Act 49 of 2003:** This Act provides for altering the sex description of certain individuals under certain circumstances, amends the Birth and Deaths Registration Act 51 of 1992 as a consequence, and provides for matters incidental to this.
- **Births and Deaths Registration Act 51 of 1992:** This Act provides for the compulsory registration of births and deaths for both South Africans and non-South Africans.
- **Citizenship Act 88 of 1995:** This Act provides for the acquisition, loss and resumption of South African citizenship.
- **Identification Act 68 of 1997:** This Act regulates compiling and maintaining a population register of the population of the Republic, for issuing identity cards and certain certificates to persons whose details are included in the population register.
- **Immigration Act 13 of 2002:** This Act provides for regulating the admission of persons to, their residence in, and their departure from, the Republic.

- **South African Passports and Travel Documents Act 4 of 1994:** This Act provides for issuing passports and other related travel documents to South African citizens.
- **Refugee Act 130 of 1998:** This Act gives effect within the Republic of South Africa to the relevant international legal instruments, principles and standards relating to refugees. It also provides for the reception of asylum seekers into South Africa, regulates applications for, and recognition of, refugee status and provides for the rights and obligations flowing from such status.

5.2.2 DHA external:

- **Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000:** This Act provides for the prohibition of unfair discrimination based on race, gender, sex, pregnancy, family responsibility or status, marital status, ethnic or social origin, HIV and AIDS status, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth.
- **Cybercrimes Bill 2019:** This Bill will create offences that have a bearing on cybercrime, will criminalise the distribution of data messages that are harmful and provide for interim protection orders. The Bill will regulate jurisdiction for cybercrimes, regulate the powers to investigate cybercrimes and impose obligations to report cybercrimes. In addition, the Bill will provide for capacity building, will provide that the executive may enter into agreements with foreign States to promote measures aimed at detecting, preventing, mitigating and investigating cybercrimes, and will provide for deleting and amending the provisions of certain laws.
- **Electronic Communications and Transactions Act 25 of 2002:** This Act provides for facilitating and regulating electronic communications and transactions. It provides for the development of a national e-strategy for the Republic. It also promotes universal access to electronic communications and transactions and the use of electronic transactions by small, medium and micro-sized enterprises. In addition, the Act prevents abuse of information systems and encourages the use of e-government services.
- **Promotion of Access to Information Act 2 of 2000:** This Act gives effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for to exercise or protect any rights. The Act also gives effect to the constitutional right of access to any information held by the State, and any information that is held by another person and that is required to exercise or protect any rights.
- **Promotion of Administrative Justice Act 3 of 2000:** This Act focuses on

ensuring that administrative bodies act reasonably and procedurally fairly. It stipulates that any decisions by an administrative body can be challenged in court if such an action is, among other things, procedurally unfair, not within an entity's powers set out in law, biased "or reasonably suspected of bias". It also allows for administrative bodies to be taken to court for "failure to take a decision".

- **Protection of Personal Information Act 4 of 2013:** This Act promotes the protection of personal information processed by public and private bodies. The Act gives effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information. This Act also provides persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act. The Act establishes voluntary and compulsory measures, including establishing an Information Regulator, to ensure respect for, and to promote, enforce and fulfil, the rights protected by this Act.
- **Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002:** This Act regulates the interception of certain communications, monitoring certain signals and radio frequency spectrums and providing certain communication-related information. The Act regulates making applications for, and issuing, directions authorising the interception of communications and the provision of communication-related information under certain circumstances. It also provides for prohibition of manufacturing, assembling, possessing, selling, purchasing or advertising certain equipment, and creates offences and prescribes penalties for such offences.
- **State Information Technology Agency Act 88 of 1998:** This Act provides for establishing a company that will provide information technology, information systems and related services to, or on behalf of, participating departments and regarding these services, act as an agent of the South African government.
- **The Public Services Act 1994:** This Act empowers the minister of public services and administration to develop and establish norms and standards related to, among others, information management and electronic government in the public service.

SECTION C: POLICY FRAMEWORK AND OPTIONS

Chapter 6: Policy framework

Vision

The Official Identity Management Policy is one of the founding policies that give effect to the vision of the DHA: a South Africa where identity, status and citizenship are key enablers of citizen empowerment and inclusivity, economic development and national security.

Principles

The shared principles³ outlined below are influenced and derived from the World Bank principles on identification for sustainable development. They are also informed by the Constitution and other transversal legislation such as the POPI Act. These principles set out considerations for developing a regulatory framework that maximises the benefits of an identity management system while minimising its risks. They are intended to maximise the benefits of an identity management system.

In this regard, it is recommended that a policy and legislative framework should, at a minimum, incorporate **10** principles under the following **three** themes:

- Inclusion (universal coverage and accessibility)
- System design (robust, secure, responsive and sustainable)
- Governance (building trust by protecting privacy and user rights)

These three themes are discussed and expanded into the principles as follows:

6.1 Inclusion

The identity management system should recognise all persons and should not discriminate on any specific grounds, such as gender, race, religion, political affiliation,

³ Principles on Identification for Sustainable Development: Towards the Digital Age (2017), facilitated by the World Bank and Centre for Global Development

etc. Inclusion means treating citizens and non-citizens fairly. For the identity management system to be inclusive, it must ensure integration of all users.

Inclusion entails the following principles:

- Ensuring universal coverage for individuals from birth to death, free from unfair discrimination
- Removing barriers to access, usage and disparities in the availability of information and technology.

6.2 System design

Identity management systems should be robust, context appropriate, and interoperable. While they should respond to user demand and long-term needs, they should collect and use only the information necessary for the system's explicit purpose. Open standards and vendor neutrality help to ensure financial and operational efficiency and sustainability.

The data or information and privacy of individuals must be protected in the country's Constitution. The identity management system should be designed with the privacy of the end-user in mind. No action should be required on the part of the individual to protect his or her personal data. Information should be protected from improper use by default. The right to privacy should be protected by law. The law should ensure that the collection and use of personal data or information is protected. The design of the regulations should ensure that the data subject is informed of the purpose and intended use of the data that is collected. To ensure prevention of leaks and loss or theft of data or information, the regulations should require physical, technical and administrative protection of data or information.

Design entails the following principles:

- Establishing a robust, unique, secure, and accurate identity
- Creating a platform that is interoperable and responsive to the needs of various users
- Using open standards and ensuring vendor and technology neutrality
- Protecting user privacy and control through system design
- Planning for financial and operational sustainability without compromising accessibility

6.3 Governance

Consent is the basis for good governance of the identity management system. There should be regulations that specify consent as the basis for collecting and using personal data or information. Therefore, it is a recognised general rule that personal data or information should only be used on receipt of consent from the owner. The regulations should provide for the right to access, rectify and/or delete personal data about the owner held by third parties. Furthermore, there should be at least one administrative authority that has a responsibility to protect personal data/privacy.

Governance entails the following principles:

- Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework
- Establishing clear institutional mandates and accountability
- Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

The above principles will guide the department in developing the new identity management policy and legal framework.

Chapter 7: Policy analysis and options

This chapter is the backbone of the Official Identity Management Policy. It introduces policy options that will be translated to a policy proposal when the policy paper has been approved by Cabinet. Policy options are discussed under each principle.

7.1 Principle 1: Ensuring universal coverage for individuals from birth to death, free from unfair discrimination

The universal coverage principle requires countries to **fulfil their obligations to provide legal identification to all residents—not just citizens—from birth to death**, as set out in international law and conventions and their own legislative frameworks. This includes the commitment to universal birth registration for those born in their territory or jurisdiction. It also includes **linking civil registration and identity systems**, which is an essential part of ensuring the accuracy and sustainability of identity systems. In addition, identity systems should be **free from unfair discrimination**.

This requires practitioners to identify and mitigate legal, procedural and social barriers to enrol in and use identity systems, with special attention to poor people and groups who may be at risk of exclusion for cultural, political or other reasons (such as women and gender minorities, children, rural populations, ethnic minorities, linguistic and religious groups, persons with disabilities, migrants, the forcibly displaced and stateless persons). Furthermore, identity systems and identity data should not be used as a tool for discrimination or infringe on individual or collective rights. While **secure and inclusive identity systems** are essential for ensuring that no one is left behind without a legal record of their existence, they are not a **guarantee for a change of status such as citizenship and immigration status**.

7.1.1 Lack of birth registration for all

Finding and cause: In South Africa, inclusion is high with near universal coverage of all persons in the Republic. A gap was identified in the **registration of all** births onto the NPR. This is caused by the **absence of a clear policy and legislation that governs the registration of all different categories of persons** in the NPR and other immigration systems.

The Identification Act, which establishes the NPR, only caters for issuing birth certificates and ID cards to citizens and permanent residents. As a result, the personal information (identity and status) of other people such as international migrants is not stored on the NPR but on other immigration systems that are not linked to the NPR. The

current practice is that children born to non-citizens are issued with birth notification forms that are not included on the NPR and, thus, cannot be tracked and traced.

The Identification Act and Births and Deaths Registration Act do not cater for the birth registration of children who are born intersex. Such children are assigned either a male or female sex status at birth. Some social groups are discriminated against in the current identity management system. This is because the identity number that we use is not gender neutral. The identity number recognises and accommodates only two categories, namely, male and female. The ID system does not differentiate between the distinct concepts of sex and gender. The World Health Organization defines sex as “the different biological and physiological characteristics of males and females” and gender as “the socially constructed characteristics of women and men”⁴. Whereas gender is traditionally thought of as a binary attribute (male vs. female), a third gender is now being increasingly considered (intersex). If an individual transitions to a new gender, the ID system should be updated. In fact, the Identification Act refers to gender and not sex.

The following **observations and policy options** apply under the principle:

- i. Every birth that takes place in the country, irrespective of the status of the parents, must be registered. If technology and medical conventions allow, the biometrics of children must be captured at birth. Where impossible, the biometrics of a parent must be linked to the birth certificate of a child.
- ii. The NIS must enable the creation of sub-database systems for registering births of citizens and non-citizens.
- iii. The new legislation and NIS must enable the registration of births for intersex children.
- iv. The identity number of a child must be processed on the basis of biographic information and linked to their parents’ identity numbers and mother’s biometric data.
- v. When possible, the biometrics of a child must be collected at birth. A facial photograph must be taken for manual identification when needed. Children must be reregistered when they reach age five with ten fingerprints and iris and facial photographs.
- vi. A combination of different biometric data for children should be considered with options such as the photograph of the ear. This depends on availability of proven technology.

⁴See World Health Organization, Gender equity and human rights, Glossary.

- vii. The new legislation and population register must make a provision that enables the establishment of a category that is neither male nor female. That is, a sex category that caters for biological males with feminine gender identity or expression or biological females with masculine gender identity or expression in the identity system.
- viii. The sex category must cater for transgender that will enable updates of sex information in the population register.
- ix. The other option is to issue a random unique identity number that is not linked to or founded on a person's sex, date of birth, place of birth or any other marker.

Unintended exclusion of birth registrations is also caused by the lack of coverage, resource capacity and constraints of the systems, and weak cooperation between the Department of Health and the DHA. The following **observations and policy options** apply under the principle:

- i. There has to be a stronger cooperation between the DHA and the Department of Health on birth notification and birth registration, with a reasonable presence of the DHA services at the facilities of the Department of Health where births occur.
- ii. Securing of the Department of Health information system is very crucial since it is the main feeder system to the birth registration records held on the NPR. This can make significant contributions to enhancing the security and authentication of births.

7.1.2 Lack of death registration for all

Finding and cause: There are still cases of **unintended exclusion of death registrations**. Some communities **fail to notify the appropriate authorities** when death occurs and burials are undertaken without an official death certificate issued. Law enforcement of the mandatory process in the instance of death and burial is absent in some instances. The consequence of not registering deaths is that a person's record remains on the NPR as if the person is still alive. Thus, the NPR has a record of people who are more than 140 years old who are still recorded as alive. The other consequence is that a birth certificate of a deceased person can be sold to another person; this is enabled by the fact that the birth certificate is not linked to the biometrics of either a parent or a child.

The following **observations and policy options** apply under the principle:

- i. In terms of law, death must be registered within 72 hours. Burying a person without a death certificate will be illegal to protect the integrity of the population register, ensure an accurate death register and prevent fraudulent use of birth and ID documents of the deceased.

7.2 Principle 2: Removing barriers to access and use of IDs, and removing disparities in the availability of information and technology

To ensure universality, principle 2 advocates eliminating barriers to accessing and using an ID. This includes removing or reducing direct and indirect costs for identification. Civil registration and first birth and death certificates should be free of charge to the individual, as should the initial issue of any identity credential that is mandatory – de jure or de facto – to possess or to access basic rights and services. If fees are charged for certain additional services (such as reissuance of lost credentials), rates should be reasonable, proportional to costs incurred, and transparent to the public. Consideration should be given to subsidising or waiving fees for poor and vulnerable persons. The indirect costs of obtaining identification – including fees for supporting documents, travel costs, and cumbersome administrative procedures – should also be minimised. For example, ID-related services should be available online and should routinely visit remote communities.

Furthermore, practitioners should **mitigate information disparities and the digital divide** by working to ensure user literacy regarding ID systems, fostering a culture of understanding and trust, and reducing information asymmetries that might prevent individuals from accessing identification-related services or benefits. With the rise of digital systems, no one should be denied identification or associated services because they lack mobile or internet connectivity or digital literacy. Stakeholders should work together to ensure both online and offline infrastructure can be extended to provide “last-mile” access and connectivity, particularly for those in rural and remote areas.

7.2.1 Removing barriers to access and usage

Finding and cause: Individuals that **cannot afford** registration services face a barrier that excludes them from the identity management system. The **cost barriers** (cost of identity cards, documents, etc.) lead to exclusion of individuals from the ID management system.

The following **observations and policy options** apply under the principle:

- i. Citizens carry a duty and responsibility to protect identity documents/cards and keep them safe.
- ii. Fees should only be charged for non-mandatory identity credentials such as passports. Replacements for lost or damaged cards should be charged on a sliding scale based on the number of replacements, with exemptions being available to persons with disabilities, the poor, senior citizens, children below age, victims of

natural disasters and persons who lost their cards as a result of being a victim of crime.

- iii. The DHA must develop an indigent policy as part of a costing model. This policy must also cater for those who already hold green ID books but cannot afford to pay for the new secure smart ID cards.
- iv. No one, irrespective of their status, should be left behind without a legal record of existence.
- v. Being included in the population register will not translate to any status other than that your identity is properly documented in the country.

7.3 Principle 3: Establish a robust, unique, secure, and accurate identity

Principle 3 highlights that **accurate**, up-to-date information is essential for a trustworthy identification database and credentials used for authentication. Foundational identity systems should provide a **unique identity** that is verifiable over the course of a person's life, from birth to death. That is, within a foundational identity system, each person should have only one identity, and no two people should have the same identity. In addition, identity systems must have safeguards against tampering (alteration or other unauthorised changes to data or credentials), identity theft, data theft and misuse, cybercrime and other threats occurring throughout the identity lifecycle).

Finding and cause: Under this principle a number of gaps were identified and several findings were made.

- i. The continued use of paper-based green ID card books increases risk of identity theft.
- ii. Issuing paper-based birth certificates that cannot be linked to a child increases the risk of fraud.
- iii. The legal age at which a person can apply for an identity documentation is 16 years. This is a serious risk since a person's biometrics are only collected when they apply for an ID. This situation has been exploited by criminals who steal the birth certificates or use minors as accomplice in criminal activities.
- iv. The current identity system contains duplicate ID numbers and ID numbers that change when a date of birth is corrected or sex alteration takes place.
- v. Identity credentials in different formats transact on multiple platforms are lacking.
- vi. The address details on the NPR are outdated.

This situation arises from the continued use of manual and paper-based processes, systems and documents. The current application process for ID books and birth certificates at outdated offices, and fraud and corruption, add to the challenges. Undocumented unregistered South African child deaths are abused. Inadequate proofing measures prevail that lead to duplicate registrations. The systems are not integrated in the absence of digital platforms for multiple formats of credentials and the Identification Act not being enforced.

The following **observations and policy options** apply under the principle:

- i. The department must intensify its strategy implementation for phasing out green barcoded ID books.
- ii. The department must intensify its strategy implementation for modernising all its offices (frontline and back-office) to enable automation of all application processes.
- iii. Once identity data has been collected through the registration process, it must be proofed to determine its veracity. The identity proofing process is fundamental to ensuring accurate and trustworthy identities are created.
- iv. The two fundamental processes for identity proofing registrations are:
 - **Validation:** Checking the validity, authenticity and accuracy of supporting documents or evidence provided and confirming that the identity data is valid, current, and related to a real-life person.
 - **Deduplication:** Using biometric recognition (using biometric identification to identify other identities already registered that could be a match) and/or demographic deduplication algorithms to ensure that a person is unique.
- v. In any identity system, identifying numbers are the most basic type of identifiers. In the context of foundational systems, ID numbers are considered to be unique when:
 - The number-generating process ensures that no two people within the system share the same number.
 - A deduplication process ensures that the same person does not have multiple identity records or numbers (that they are unique in the database).
- vi. The **structure of an ID number**, including its format and length, require careful consideration of country context and privacy concerns. Policy options guiding the number structures to be used could include the following:
 - A random number generated using mathematical algorithms and containing no

information about the person.

- A serial number assigned based on the order of entry into the system, with the highest number assigned to the most recent enrollee.
 - A coded number that contains information about the person, with certain digits coded based on attributes such as birth year, sex, nationality, and location of application. That is, retain the current ID number but have three sex categories – male, female and intersex.
 - The format of the new ID number must be as inclusive as possible, especially when it comes to intersex and transgender persons.
 - The seventh digit of the ID number is a gender marker that indicates whether the ID holder is a female or a male – (0-4 means the holder of the ID is a female while 5-9 means the holder of the ID is a male). This is the most contentious digit for non-binary or transgender persons as it does not reflect their sexual orientation or gender. To accommodate non-binary, transgender and intersex persons, it is recommended that an alternative digit or letter “X” be used for this population. This will be a subject of further consultation with the affected population. This change will not affect the current composition of the ID number for males and females.
- vii. In the digital era, however, randomised numbers are the preferred choice for enhancing privacy and security. Connectivity between registration points, along with the centralised nature of deduplication and advanced computing power, mean that it is now possible to assign unique, random numbers to every person in the ID system. Random numbers offer three primary benefits over coded numbers:
- They reveal no personal information. By definition, coded numbers reveal information about a person.
 - They are more secure. Coded numbers make it easier for fraudsters to guess an ID number by narrowing down the possible combinations based on a few known facts about a person.
 - They are immutable. In some cases, coded numbers contain information, such as nationality, place of residence, or gender, which may be subject to change over an individual’s lifetime, requiring the numbers to be updated.
 - The legal age for smart ID card application must be lowered to enable biometrics to be captured earlier and to curb identity theft. It is recommended that 10 years should be a new legal age for ID applications – this can be lowered further, but this age will mitigate a risk of having matriculants who write matric examinations

without smart ID cards.

7.4 Principle 4: Creating a platform that is interoperable and responsive to the needs of various users

Principle 4 highlights the need for identification and authentication services to be **flexible, scalable, and meet the needs and concerns of people (end-users) and reliant parties** (e.g. public agencies and private companies). The value of identity systems is highly dependent on their interoperability with multiple entities, both within a country and across borders. Domestically, this includes the ability of different databases or registries (e.g. foundational and functional databases) to communicate with each other, exchange data, and facilitate identity queries in a timely and low-cost manner, subject to appropriate privacy and security safeguards. It also includes **interoperability across borders** to facilitate mutual recognition of physical or digital IDs issued by one country in other countries, which can increase trade and enable safe and orderly migration.

Finding and cause: The finding was that there are no linkages between database systems within the civic services and immigration branches and little interlinkages and integration with other databases and systems within the DHA. Developing different identity systems (silo or fragmented identity systems) by different government departments leads to process duplication, increased costs and inefficiencies within government. Citizens are registering in different identity systems at various government departments and institutions.

This is because the approach to digital transformation adopted by different branches and government departments is not synchronised. Most existing systems were not designed to share information across branches and government departments.

The following **observations and policy options** apply under the principle:

7.4.1 Interoperability

Interoperability is crucial for developing efficient, sustainable, and useful identity ecosystems. Specifically, interoperability is the ability of different functional units such as systems, databases, devices, or applications to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units. Interoperability occurs at three levels:

- **Between identity subsystems.** Within the identity system itself, standards-based technical interoperability allows different components and devices to communicate with each other and work together.
- **With other domestic systems.** Identity systems must be interoperable with other

systems such as the civil registry and service providers that are reliant parties of the system to exchange data or facilitate queries. Communication with other systems may be provided through various interoperability layers, web services and APIs, or direct connections.

- **With identity systems in other jurisdictions.** Cross-border frameworks for interoperability and mutual recognition allow credentials from one country to be accepted in other countries. This includes, for example, accepting standards-compliant passports across the globe and regional frameworks for mutually recognising identity credentials.
- Legal, policy and regulatory frameworks should define the scope of interoperability, particularly with regard to data exchange and requirements for privacy and data protection.

The following **observations and policy options** apply under the principle:

- i. Adopt one official identity management system across all government departments to store biographic and biometric information for citizens and non-citizens.
- ii. Integrate all identity management databases in the new identity management system, the NIS.
- iii. Create an e-government platform that will allow electronic verification and authentication services.
- iv. Maintain separate identity management systems and create linkages between different identity management systems.

South Africa should constitute a focal point for identification services to help coordinate the approaches and activities of the several government entities that constitute the system as well as support from funding institutions. The focal point could be complemented by a user group representing several of the system's major customers such as the Department of Health, the South African Police Service, the Department of Social Development, etc.

7.4.2 Integration across borders

South Africa's identity management systems are not integrated and interoperable with those of neighbouring countries, as is the case with the Economic Community of West Africa States countries and the European Union. This is because there is a lack of cross-border integration and interoperability frameworks. Cross-border frameworks allow for interoperability and mutual recognition of countries' identity management systems.

7.5 Principle 5: Using open standards and ensuring vendor and technology neutrality

Principle 5 emphasises the need for **vendor and technology neutrality** to increase flexibility and avoid a system design that is not fit for purpose or suitable to meet policy and development objectives. This requires robust procurement guidelines to facilitate competition and innovation and prevent possible technology and vendor “lock-in,” which can increase costs and reduce flexibility to accommodate changes over time. In addition, open design principles enable market-based competition and innovation. They are essential for greater efficiency and improved functionality in identification systems, and for interoperability.

Finding and cause: Identity databases are duplicated and there are large-scale system incompatibilities within government departments. A number of government departments are using diverse applications, platforms, software and databases that are vendor or product locked. Most of the existing ICT systems were not designed to share information across departments. This arose because common standards were not adopted within the DHA and among government departments.

The following **observations and policy options** apply under the principle:

- i. Adopt open standards to ensure vendor and technology neutrality.
- ii. ISO 29794-part 5: The new expanded standard on facial biometrics.
- iii. ISO/IEC JTC/1 SC/17 SG/2: A special group on standards for virtual identity.
- iv. Digital travel credential: Looks at both policy and technology and is coordinated between the International Civil Aviation Organization (ICAO) and ISO.
- v. Standards-based (“plug and play”) procurement model.
- vi. XML advanced electronic signatures standard (XAdeS).
- vii. ICAO identity applet.

7.6 Principle 6: Protecting user privacy and control through system design

Principle 6 emphasises that identity systems must protect people's privacy and control over their data through system design. Designing with people's privacy in mind means that **no action should be required on the part of the individual to protect his or her personal data**. Information should be protected from improper and unauthorised use by default, through both technical standards and preventative business practices. These

measures should be complemented by a strong legal framework (as emphasised in principle 8).

For example, data collected and used for identification and authentication should **be fit for purpose, proportional to the use case**, and managed in accordance with norms for data protection. Credentials and numbering systems **should not unnecessarily disclose sensitive personal information**.

Finding and cause: Presently, user privacy is not protected in compliance with some sections of the POPI Act and there are no control mechanisms to ensure that users have access to the data contained in the ID system. This is a management issue as full compliance with the POPI Act is mandatory. The non-protection of user privacy is linked to the fact that some provisions of the POPI Act are not yet effective.

The following **observations and policy options** apply under the principle:

- i. Privacy-enhancing technologies and security measures should be built into every aspect of the NIS by adopting a privacy by design approach that adheres to the foundational principles of privacy by design.
- ii. Maintain user privacy and secure systems that process, collect, store, use, and disseminate personal data as this is a fundamental concern for ID systems. In addition to adhering to international data protection and privacy principles in the development of the legal framework, privacy-enhancing technologies and security measures should be built into every aspect of the NIS. Privacy assurance must become an organisational norm.
- iii. Individuals must be informed whenever their data is processed, for what purpose, and by which means. The system must be enabled to send transaction notifications and data breach notifications to the data subject.

7.7 Principle 7: Planning for financial and operational sustainability without compromising accessibility

Principle 7 recognises the importance of designing systems that are **financially and operationally sustainable** while still maintaining accessibility for people and reliant parties. This may involve different business models, including reasonable and appropriate service fees for identity verification, offering enhanced or expedited services to users, carefully designed and managed public-private partnerships, recuperating costs through efficiency and productivity gains and reduced leakages, and other funding sources.

Finding and cause: The DHA does not have a defined model to sustain its ID management system through revenue generation.

The following **observations and policy options** apply under the principle:

7.7.1 Financial and operational sustainability

In many cases, particularly where ID authorities report to line ministries, ID systems will be financed out of the national budget. However, digitising ID systems in particular has created the potential for new business models, including generating own revenue by charging fees for identity-related services, as well as public-private partnership models. The following revenue generation streams must be considered:

- Develop policies and a regulatory framework that make provision for revenue generation streams for identification and verification services
- Lower pricing or free services for government agencies
- Market-related fees for the private sector users
- Bulk pricing discounts for frequent users of identity services
- Pricing based on the type of data requested
- Pricing based on whether authentication and verification services are performed online or through hardwired database connection
- Phasing in pricing through initially waiving fees or setting prices extremely low, and later increase them based on demand
- Consider public-private partnerships

7.8 Principle 8: Safeguarding data privacy, security and user rights through a comprehensive legal and regulatory framework

Principle 8 sets out the requirements for a comprehensive legal framework: identity systems must be underpinned by policies, laws and regulations that promote trust in the system, ensure data privacy and security, mitigate abuse such as unauthorised surveillance in violation of due process, and ensure provider accountability. This typically includes an enabling law and regulations for the identity system itself as well as laws and regulations on data protection, digital or e-government, electronic transactions, civil registration, cybersecurity and cybercrime, functional identity systems, etc. The enabling law and regulations for an identity system should clearly describe the purpose of the identity system, the identity system's components, roles and responsibilities of different stakeholders, how and what data is to be collected, liability and recourse for ID holders and reliant parties, the circumstances in which data can be shared, correcting inaccurate data attributes, and how inclusion and non-discrimination will be maintained. Laws and

regulations on data protection and privacy should include oversight from an independent body with appropriate powers and should protect ID holders against inappropriate access and use of their data by third parties for commercial surveillance or profiling without informed consent or legitimate purpose. At the same time, these frameworks should not stifle competition, innovation, or investment and can include regulatory and self-regulatory features.

In addition, the identity-related laws, regulations, and policies should give people genuine choice and control over the use of their data, including the ability to selectively disclose the attributes that they want. Users should be given simple means to have inaccurate data corrected free of charge and to obtain a copy of data held about them. Personal information should not be used for secondary, unconnected purposes without the user's informed consent, unless otherwise required under the law. Identity providers should be transparent about identity management, develop appropriate resources to raise users' awareness of how their data will be used, and provide them with tools to manage their privacy. Identity providers should ensure that the process to correct errors is administrative rather than judicial to increase the speed of resolution and reduce costs. Data sharing arrangements should also be transparent, fully documented, and only agreed to in the best interest of the individual(s) concerned.

7.8.1 Safeguarding data privacy, security

Finding and cause: Legal framework provisions to safeguard data privacy and security have not come into legal effect, leading to personal data being compromised. Some of the provisions of the POPI Act are not yet enforced and the legal framework is currently weak. The ownership, and therefore control, access to and management of the data systems is an issue. The DHA's Information Systems Security Policy is outdated and not aligned to the POPI Act.

The following **observations and policy options** apply under the principle:

- i. Government needs to own critical information infrastructure. The technological sovereignty principle must be observed when designing the NIS. That is, the information and communications infrastructure and technology must be aligned to the laws, needs and interests of the country.
- ii. NIS must be built on a foundation of trust and accountability between government agencies, individuals, and the private sector, both within countries and across borders. A cornerstone of this foundation are the laws, codes, regulations, and practices that govern and support the ID system, commonly referred to as legal framework.
- iii. In general, the policies, laws, and regulations that will support an identity system can be divided into two categories:

- Enablers: directly define and govern the NIS stem, including its design, management, operation, and relationships with stakeholders and other systems.
 - Safeguards: address potential risks surrounding the NIS, including those related to data privacy, security, and non-discrimination.
- iv. Data dumping to public and private institutions would be discontinued or minimised, and be regulated in accordance with the POPI Act.
- v. A legal framework should be established to build trust and accountability in the NIS.

7.8.2 No documented and transparent identity data sharing arrangements between the DHA and identity system users

Finding and cause: There are no documented and transparent guidelines that regulate sharing identity data between the DHA and other ID system users (third parties that have access to either the NPR or Hanis) leading to an unregulated exchange of personal information between parties.

The following **observations and policy options** apply under the principle:

- i. Because linking information across databases intensifies privacy and data protection concerns, legal frameworks can mitigate risks by stipulating all the purposes for which personal data in an identity system is shared, by both government and non-government entities. In addition, public and private entities may be limited to obtaining specific information justified by their functions (the “need-to-know” principle).
- ii. Personal data collected for other purposes, which could be for an identity system or for civil registration, can be processed by the same or another controller for crime-related purposes only in so far as there is legal authorisation for this and such processing is necessary and proportionate to the purpose for which the personal data was collected.
- iii. Disclosure of information, excluding core biometric information, is pursuant to an appropriate court order, which can be made only after the DHA has been given an opportunity to give input on the disclosure. Disclosure of information, including core biometric information, is permitted in the interest of national security on the approval of the director-general or delegated officials.
- iv. Personal information about an individual collected for a particular purpose must not be used or disclosed for another purpose without the individual’s consent. However, there is an exception for situations where the use or disclosure is reasonably necessary to enforce related activities conducted by, or on behalf of, an enforcement

body. This includes disclosure by police for prevention, detection, investigation, prosecution or punishment of criminal offences, as well as an exception for uses and disclosures authorised by law or by court order. Use for enforcement-related activities must be noted in writing as a mechanism to promote accountability.

7.8.3 User control of identity data

Finding and cause: Sharing personal data of clients occurs without their consent. This arises because some provisions of the POPI Act are not yet implemented.

The following **observations and policy options** apply under the principle:

- i. One widely accepted privacy principle is that an individual's personal data should only be collected and used with the consent of that individual unless there is another basis in law for such collection and use. Where consent is the basis for collection, transparent disclosure to the individual of the nature of their personal data collected and the intended uses of such data is essential for consent to be meaningful.
- ii. Where the personal data being processed is special category data such as biometric data, additional conditions must be satisfied, one of which is that the individual's explicit consent to the processing should be obtained.
- iii. At the point of information collection, consumers must receive notice as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.
- iv. Clients must be notified when there are changes effected on their records and identity profiles.

7.8.4 Cybercrime and cybersecurity

Finding and cause: There are risks and weaknesses in the legislative framework that lead to identity theft, such as e-identity theft, and cybercrime. South Africa does not have a comprehensive and effective cybercrime and cybersecurity legislative framework. Legislation on cybercrime and cybersecurity is still a Bill.

The following **observations and policy options** apply under the principle:

- i. For each kind of crime in the analogue world, there is an equivalent in the digital world. For instance, theft of property or identity can occur digitally. The occurrences that amount to crime in the real world have a cybercrime parallel in the virtual world. Cybercrime laws provide enforcement powers against such violations.
- ii. Cybercrime law should criminalise unauthorised access to the NIS or other databases holding personal data.

- iii. Cybercrime law should criminalise unauthorised monitoring/surveillance of the NIS or other databases holding personal data, or unauthorised use of personal data.
- iv. Cybercrime law should criminalise unauthorised alteration of data collected or stored as part of the NIS or other databases holding personal data.
- v. Cybercrime law should criminalise unauthorised interference with the NIS or other databases holding personal data.
- vi. Cybercrime law should clearly state adequate penalties for cybercrime violations, but also for breach of obligations by critical information infrastructure holders.
- vii. Cybercrime law should establish clear powers for a computer emergency response teams to prevent and investigate cybersecurity breaches.

7.9 Principle 9: Establishing clear institutional mandates and accountability

Principle 9 highlights the need for institutional mandates and accountability in governing ID systems. Ecosystem-wide trust frameworks must be established and regulate governance arrangements for ID systems. This should include specifying the terms and conditions governing the institutional relations among participating parties, so that the rights and responsibilities of each are clear to all. There should be clear **accountability and transparency** around the roles and responsibilities of identification system providers.

Finding and cause: South Africa does not have legislation that affirms the DHA as the sole provider of official identity services: that is personal data collection, storage and processing. There are other entities outside of government that provide identity verification; however, the DHA cannot challenge these entities as there is no legislation that prevent them from providing this service in any way they see fit..

The following **observations and policy options** apply under the principle:

7.9.1 Clear institutional mandate

- The Home Affairs White Paper alludes to the lack of legislation that declares the DHA the sole provider of identification.
- The legislation must reaffirm and reposition the DHA as the sole provider of official identity and civic status verification services.
- The Home Affairs Bill is part of the process towards a Home Affairs Act to declare, reaffirm and reposition the DHA as the sole provider of official identification.

- The administration of the NIS, including the organisations, staff and procedures involved in its management, operations and oversight, is critical to ensuring that the system is trusted and sustainable.

7.10 Principle 10: Enforcing legal and trust frameworks through independent oversight and adjudicating grievances

Principle 10 emphasises that the identity system should include clear arrangements for the **oversight of these legal and regulatory requirements**. The use of identity systems should be **independently monitored** (for efficiency, transparency, exclusion, misuse, etc.). This will ensure that all stakeholders use identification systems appropriately to fulfil their intended purposes, monitor and respond to potential data breaches, and receive individual complaints or concerns regarding processing personal data. Furthermore, disputes regarding identification and personal data use that are not satisfactorily resolved by the providers – for example a refusal to register a person or to correct data, or an unfavourable determination of a person’s legal status – should be subject to a rapid and low-cost review by independent administrative and judicial authorities with the authority to provide suitable redress.

Finding and cause: There is no independent oversight for the identity management system and some of the provisions of the POPI Act have not yet come into effect.

The following **observations and policy options** apply under the principle:

- i. To ensure compliance with privacy and data protection laws, the following options are recommended:
 - The **Information Regulator** (South Africa) could be declared an independent oversight authority to monitor the use of official identity information.
 - Establish an independent body that is legally empowered and has the capacity to oversee official identity processing and to hold responsible parties accountable.
 - Establish a semi or fully autonomous agency or directorate within the DHA that is legally empowered and has the capacity to oversee official identity processing and hold responsible parties accountable.

SECTION D: ENVISIONED IDENTITY MANAGEMENT SYSTEM

Chapter 8: Key elements of the identity management system

8.1 Introduction

The identity management system consists of the following key elements:

- Single digital population register of all people who live and have lived in the country
- Biometric-based NIS that enables a single view of a person, e-government and e-commerce
- Policy that provides for a constitutionally sound framework to manage personal information that will be collected and stored in the NIS
- Legislation that establishes clear rules to govern accessing and processing the population register records in line with relevant policies and legislation such as the POPI Act and Cybercrimes Bill.

The DHA can only carry out its constitutional commitments if it is the sole custodian of the official identity of all citizens and all persons in South Africa. In a digital age, this requires building a population register that can affirm, secure and verify e-identity corresponding to the register of identity of natural persons.

8.2 The new population register

The new population register will incorporate the civil registration of citizens, data from the immigration system and aspects of the current population register. Each item included in the population register will be specified in a new Population Register Act. In a digital age that is data-dependent, the data specified in the Act will have major implications for citizens, the State and the economy.

The population register, as conceptualised in the White Paper and supported by the NIS, is an instrument that the State will use to keep and process legally specified records and data on every citizen and every person in South Africa. It will be a central feature of a digital society and globalised economy, and the backbone of e-government. To play this role, population register records and data must be digital, accurate, current and secure. This, in turn, depends on establishing enablers to ensure that the systems producing the

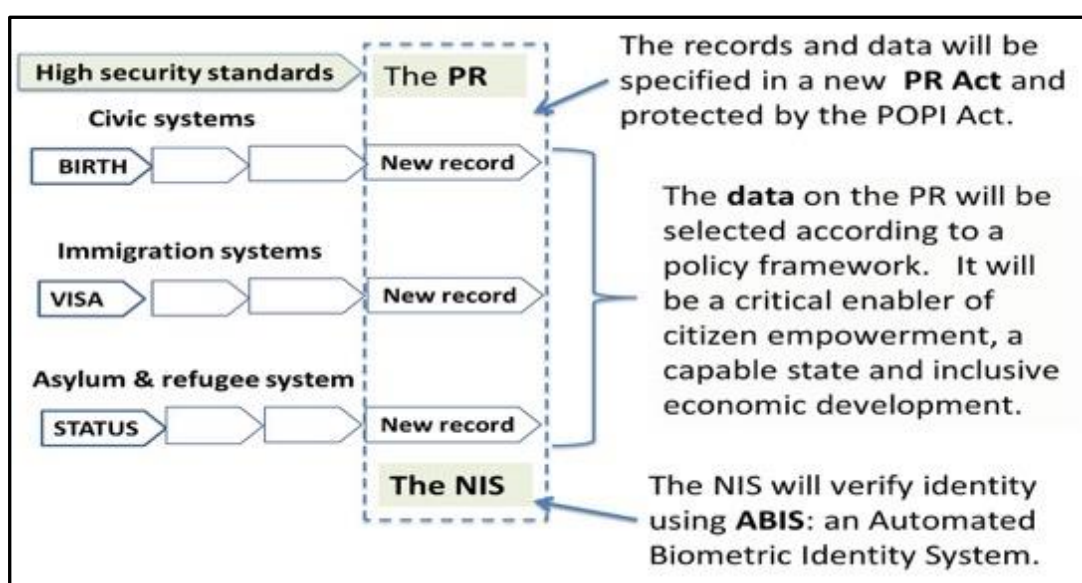
records have a firm policy and legal foundation, with up-to-date technology. They must operate within an environment that is secure and well-governed.

The argument for South Africa to invest in the kind of population register outlined above is made in the 2017 version of the Mandate Paper, published annually by the DPME as a guide to government budgeting approaches and priorities:

Improved operational and information systems will help fight crime and corruption but also government efficiency generally. Ongoing technological change is driving down the cost of effective administrative, information and monitoring systems. A bedrock of such administrative systems is an effective identity system for citizens and visitors. It is therefore critical to ensure that the population register of the Department of Home Affairs and the electronic and card Identification system include all citizens and be of the highest integrity. Obstacles to a more rapid rollout must be investigated and a comprehensive integrated approach developed about how this system can be integrated with other government programmes and systems. (The views expressed above were elaborated in the 2018 Mandate Paper).

The basic model of the NIS as demonstrated in Figure 8.1 shows how the model will work. The civic, immigration and refugee systems have outputs that result in creating a new or updated record. In the examples, these would respectively be a birth certificate; a visa such as a tourist, work or study visa; and a decision to grant or deny refugee status to an asylum seeker. The population register is part of the same digital platform and is the database where the records and data specified in a Population Register Act reside. The integrity of the population register depends on the integrity of all the systems, which must meet high standards of security as specified in relevant Acts and produce data that is accurate and reliable.

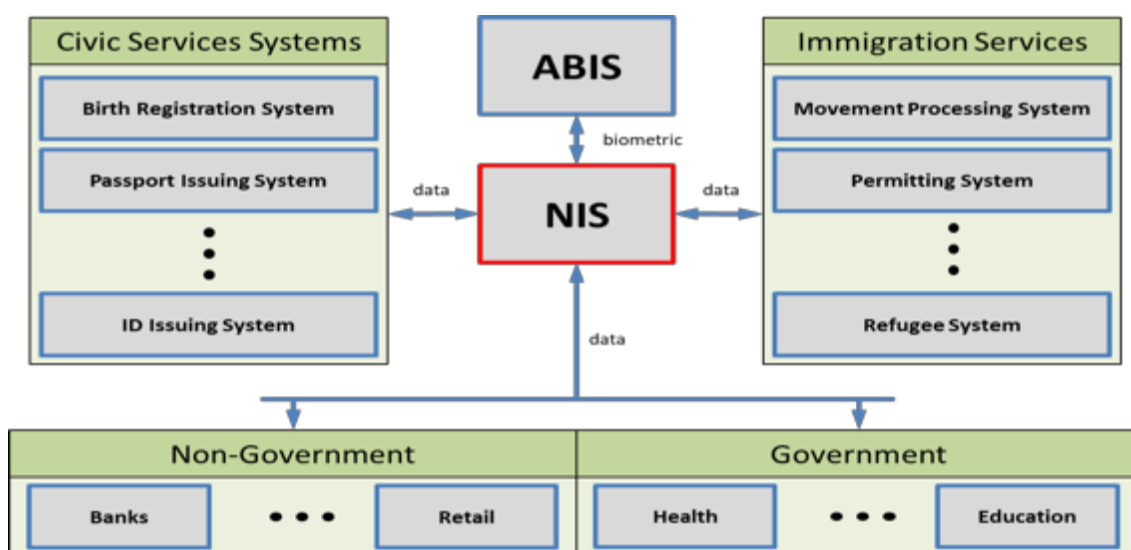
Figure 8.1: The new population register supported by a National Identity System



8.3 The envisaged NIS

The NIS will be an integrated system built around a multi-modal Abis. The NIS will support identification searches to establish the identity of a person with a given biometric, and verification searches to confirm whether the identity document belongs to the person whose biometric is presented. It will be scalable and expandable to include additional biometrics such as iris scans, palm prints and footprint and facial recognition. Figure 8.2 illustrates how such an interface will be enabled.

Figure 8.2: NIS interface platform



The NIS will be developed in phases based on open standards to ensure seamless integration of all government IT systems. All modules will be developed as required and will be based on the functional and technical specifications that are based on re-engineered business processes. Developing the NIS modules will be fully implemented once the information from the legacy systems (NPR, Hanis, EMCS and NIIS) have been cleaned up. Every case requiring data clean-up should be tracked through a case management system to investigate and report on the nature of challenges encountered and progress made towards resolution of the cases detected.

The NIS is the envisaged single source of all DHA client data. It will consolidate the data stored on the NPR, NIIS, MCS, EMCS, VAS and the visa system into one database. The NIS will serve as the link between other systems and Abis; i.e., insertion of and access to the biometric data stored on Abis will be through the NIS. The NIS has the following objectives:

- i. Record the department's interactions with clients (i.e. travellers and all persons that are resident in South Africa).
- ii. Ensure accuracy and integrity of the client data.
- iii. Ensure that all client records are linked uniquely to each client.
- iv. Record all changes to a client record and store historical data.
- v. Link all transactions (data insertions, data requests, and data updates) to DHA officials who perform the transaction in such a manner that the official who performed the transaction cannot dispute the transaction.
- vi. Provide interfaces for systems of organisations outside the DHA to access client data.
- vii. Ensure that data stored in the NIS is available in real time.

The main function of the NIS will be to ensure the storage and integrity of client data. All data that is concerned with the identity of a DHA client, citizen and non-citizen, will reside in the NIS. The DHA's business processes will be executed in front-end systems, such as Live Capture, and the NIS will only store the data generated from those front-end systems. The NIS will provide access to its data via a catalogue of services, which in turn will be used by the interfacing systems to perform their functions. The services that the NIS will provide can be broadly grouped as follows:

- i. Query: all interactions where data residing in the NIS is only being retrieved; i.e., the data from the NIS is merely used to accomplish some desired function, but remains unchanged after the interaction. This is inclusive of verification and identification, which entail more than the simple retrieval of data.
- ii. Modify: all interactions where data residing in the NIS is only being updated or changed from its current value.
- iii. Create: all interactions resulting in the genesis of a new record. Once a record is created, all subsequent interactions with it will be modify interactions.
- iv. Insert: this is not a fundamental interaction type of the NIS but it is used to represent all interactions involving new information being entered into the NIS. This consists of both modify and create interactions.
- v. Retrieve: this is not a fundamental interaction type of the NIS, but it is used represent all interactions involving existing information being requested from the NIS.

- vi. Push: this involves the automatic propagation of data from the NIS to any of its interfacing systems. Push services provide the capability to send data to external systems without necessarily being initiated by an external system to the NIS. These services are typically initiated when specific “trigger” events occur within the NIS, where it has been determined that an external system should be updated automatically upon occurrence. An example of this is when the NIS receives information about a v-listed individual. The NIS in turn will automatically push this information to relevant systems such as the risk engine, so that it too has the latest and most accurate version of the v-list.
- vii. Deactivate: this is an interaction whereby the data of a record or the record itself is removed from the active set of the NIS and placed in an inactive set, which is only accessible with the requisite authorisation.

Given the pivotal nature of the NIS to the operations of the State and society, and the sensitive nature of the personal information contained in it, proper privacy and security measures will be put in place to protect it from unauthorised modification and external tampering or hacking. Key security measures will include biometric access control including non-repudiation measures for officials and audit logging of any transaction processed on the NIS. The NIS will also ensure the secure issuance of enabling documents to eligible applicants. Key enabling documents will be secured by including security features. The introduction of the smart ID card and the new secure passport (an ICAO-compliant machine-readable travel document) are part of the security improvements that form part of the NIS rollout.

All access to digital data and records will be rule-based and governed by appropriate legislation. Rules that ensure security and the rights of citizens and residents will derive from cyber security and privacy legislation. The new population register will be comprised of legally mandated records that are accurate, highly secure and linked to biometric data that relates to a unique individual. It will be the basis of a trusted official e-identity that will be the backbone of the digital platforms, State and private, that all our lives will depend on. The population register will enable all communities to access responsive and integrated digital services and information. The following security components are needed for the NIS:

- i. Identity and access management refers to the processes and tools used to grant or deny access and authorisation to the NIS. It will be realised by the following services: identity management, access control services, authentication services and privilege usage management service.
- ii. Data governance refers to management and control of data to ensure that high-quality data exists within the NIS over the lifecycle of the data.

- iii. Data security and privacy ensures that policies, procedures, functions and tools are provided to classify data and protect it from unauthorised disclosure, modification, theft and leakage.
- iv. Threat and vulnerability management refers to the continuous or cyclic practice of monitoring, identifying, classifying, remediating, and mitigating of system security weaknesses.
- v. Secure infrastructure hardening ensures that all the NIS infrastructure components, and the associated software and platforms for both, are continuously secured.
- vi. Centralised logging ensures that all the activities such as user access, transactions, user permissions, transaction patterns, etc. are stored centrally and that the storage is protected from any modifications by either authorised or unauthorised users of the NIS.
- vii. Business continuity / disaster recovery refers to the policies, procedures, facilities, tools and functions that ensure that there will be no loss of NIS data following a disaster of any kind.
- viii. Information security governance refers to the tools, policies, personnel and business processes that ensure that security is continuously carried out to meet NIS-specific needs in line with relevant legal and regulatory frameworks.
- ix. Risk analysis and management refers to the tools and processes needed for identification, analysis, monitoring and mitigating system risks during the lifecycle of the NIS.
- x. Device management refers to securing (such as securing file systems) of all devices that connect to the NIS to avoid tampering with these devices.

Further modernisation and integration of systems mean the DHA must introduce Abis, which will enable further biometrics capturing. The Abis project will be rolled out in phases, over a five-year period. Among others, implementation will entail migration of the current Hanis data (fingerprints and facial recognition) to the new Abis, with improved functionality, installation and configuration of Abis infrastructure (hardware), and building system functionalities. The current Hanis only records two biometrics; that is, photos and fingerprints. Abis will record at least five biometrics; that is, fingerprints, palmprint, facial, iris and photo recognition. It is envisaged that, in future, the DNA and child footprint will be added to Abis.

Chapter 9: Legislative framework

The White Paper contends that the DHA rules that govern access to, and processing of, population register records and data, including verifying identity, will be based on a new legislation, regulations and operating procedures. The legislation will replace the current Identification Act that dates back to the 1980s, although it was deracialised post-1994. The new legislation will specify the mandatory records and data that must be in the population register, according to a policy and legislative framework aligned to the Constitution of a sovereign, democratic South Africa.

The current Identification Act establishes a population register and specifies its scope in the mandatory records that are captured on it. In terms of categories of persons, the current population register covers all South Africans, including those residing abroad, and foreign nationals who are permanent residents. The Identification Act also covers the biometric and biographical data captured on the population register and the specifications of the identity documents that are issued.

The Identification Act's objectives specifically include (among other things) compiling and maintaining a database in respect of the population of the Republic of South Africa and the issuing identity cards, birth certificates, marriage certificates, death certificates or passports to persons whose details are included in the database. The director-general of the DHA, according to section 5 of the Identification Act, is responsible for ensuring that:

- the database is compiled and maintained
- the particulars required for compiling and maintaining the database are obtained, in accordance with the provisions of the Identification Act.

The Identification Act only refers to the population register and does not distinguish between the underlying systems or their purposes. The population register is implemented through the following systems:

- the NPR managing biographical information
- Hanis managing biometric information, notably fingerprints, facial photographs and signatures.

The new legislation will provide for the following key policy changes:

- i. Provisions that reaffirm the DHA as the sole provider of official identity services; that is, collection, storage and processing of personal data (biographic and biometric data).
- ii. Provisions for the establishing the population register as the only official record or database for all people who live or lived in the country.

- iii. Provisions for collecting new biometrics such as iris scans, palmprints and footprints and facial recognition.
- iv. Provisions for collecting, storage and processing official identity data for all people (citizens and non-citizens) who live/lived in the country, or international visitors.
- v. Provisions for collecting storage and processing official identity data for people that are currently discriminated against on the basis of their sex.
- vi. Provision for registering all births (citizens and non-citizens) in the population register.
- vii. Provisions for capturing biometrics of children at birth or, where impossible, biometrics of a parent or informant.
- viii. Provisions for reconfiguring the ID number to accommodate excluded minority groups, including intersex persons.
- ix. Provisions for establishing a single digital NIS that enables a single view of a person, e-government and e-commerce.
- x. Provisions for securely sharing official identity data with public and private institutions in line with the POPI Act and Constitution (realisation of the privacy principle).
- xi. Provisions for establishing an institutional capacity for independent oversight of the NIS and processing personal data.
- xii. Provisions for hefty penalties for those who aid identity fraud and theft, and illegal processing of personal data (including amendments to personal data without the consent of the affected person). This should also cover cybercrimes.
- xiii. Provisions for criminalising burying a person without a death certificate that is issued by a relevant authority.

Other legislation that will be amended include the following:

- Births and Deaths Registration Act 51 of 1992
- Regulations made under the Births and Deaths Registration Act 51 of 1992
- Regulations made under the Identification Act 1997
- Alteration of Sex Description and Sex Status Act 49 of 2003.

The South African population register will be among the most integrated, comprehensive and connected systems globally, with significant benefits for the State, the economy and

citizens. The centrality of data in a digital world will mean enabling legislation that aligns with Acts dealing with areas that include privacy, copyright, cyber security, national statistics, archives and records. Population register records will eventually need to be archived indefinitely for two main reasons: to preserve a record of who constituted the nation for future generations and as a database that is a crucial resource in a digital knowledge-driven society.

Chapter 10: Funding model

The DHA's budget of just R8 billion (2019-20 financial year, inclusive of the IEC transfers) is based on the incorrect assumption that it does not require modern systems, professional staff and a secure environment. The consequences of the funding deficits have been very costly for South Africa, leading to deprivation of constitutional rights to citizens and eligible non-citizens. This has also contributed to the increase of illegal migration since the inspectorate capacity and budget have shrunk over the years. A secure, modernised DHA that is funded at an appropriate level by the State would be a key enabler of economic development and would generate new revenue streams and investments.

Given the fiscal pressures, it will be impossible for the State to fully fund the repositioning programme. The project for a detailed design and cost projection of the new model DHA will be launched in the 2020/2021 financial year.

Other (current and future) revenue streams:

- Tariffs for civic and immigration services: this revenue stream is current but tariffs remain very low especially for passports, visas and permits.
- Self-financing (revenue collected through the tariffs is returned from the NRF to DHA): this revenue stream is current; however, it is dependent on the National Treasury approval.
- Charges for verification of identity and status in official transactions: this revenue stream is current but the automated billing system is not operational (manual invoicing is being used).
- Charges for verification of identity and status in commercial transactions: this revenue stream is current but the automated billing system is not operational (manual invoicing is being used).
- Additional charges for premium services: this revenue stream is at a conceptualisation stage.
- Fees for interfaces with the NIS: this revenue stream is at a conceptualisation stage.
- The successful implementation of the NIS will lead to a substantial reduction in fraudulent transactions across the State and society. The reduction in social grant fraud alone will more than pay for its development over the medium term; new revenue streams could be generated; and many forms of partnerships developed.
- As part of removing barriers for accessing DHA services, the department will

develop an indigent policy to cater for the poor who are not able to pay for reissued mandatory enabling documents. This will include first-time applicants for smart ID cards who already have green ID books.

SECTION E: IMPLEMENTATION STRATEGY AND ROADMAP

Chapter 11: Phased-implementation approach

The identity management system will be planned according to the following horizons:

- Three-year horizon (April 2019 – March 2022): The focus is on putting in place the policy and legal framework for the population register and NIS.
- Five-year horizon (by March 2024): All core elements of the new population register and NIS are fully functional, including basic administrative and core business systems, and required security standards are maintained. That is,
 - integration of DHA systems completed
 - the NIS interfaces with critical government systems
 - a single database for government and e-government platform is operational
 - the NIS interfaces with private sector systems
 - the NIS interfaces with systems of neighbouring countries – piloted through the one-stop border post initiative
 - The population register is generating substantial revenue through large-scale verification of identity.
- Ten-year horizon (by March 2029): The envisioned end-state is achieved with the legacy model fully replaced, world-class standards maintained and funding assured.

The department is undertaking deep-dive studies that will enable the development of clear and realistic implementation strategies. The focus areas include:

Human resources management and development:

- The new model DHA requires officials who understand policy, law and processes and can investigate and solve problems while securing systems under constant threat from criminal syndicates. As a result, the recruitment and training of an employee that is security aware is critical to establishing the kind of secure environment needed.
- The DHA will not be able to reposition to a secure and modern department with the current competences of its employees. It is envisaged that the results of the study will determine the readiness of the department and will further enable the DHA to take firmer control of key functional areas in preparation for a

comprehensive implementation of the repositioning programme. The strategy is to capacitate the Learning Academy as a college that will help the department to retrain employees for a repositioned DHA

Information communication technology

- The current repositioning programme is the most critical factor in transforming the DHA as a modern and secure department and an integral part of the security apparatus of a capable State. The DHA vision for its systems is to build one integrated digital platform with a single NIS at its centre that serves both civic and immigration functions and enable a single view of a person. Such a platform requires a new operating model, with highly trained officials guided by appropriate values and legislation within a secure environment.
- It is imperative that a diagnostic study be conducted to assess the state of ICT in the department as this is one of the critical enablers of successfully implementing the repositioning programme. It is envisaged that the results of the study will determine the readiness of the department and outline all the necessary measures that need to be put in place prior to implementing the repositioning programme.

Security and enforcement

- In executing its mandate, the DHA plays a very critical role in protecting the integrity of the country as a sovereign State through securing and managing the official identity and status, international migration, refugee protection and population register. As it is, the DHA will not be able to reposition to a secure and modern department with the current security and enforcement capacity.
- With the DHA being repositioned as a modern, secure department located within the security system of the State, there is a need to enhance its capability to mitigate risks, deal with threats and respond to national security demands. This requires building and maintaining a security system around its people, systems, data and infrastructure. Therefore, prior to the DHA embarking on the actual implementation of the repositioning programme, an organisational assessment of the security and enforcement capabilities will be undertaken through a deep-dive study.
- It is envisaged that the results of the study will determine the readiness of the department and will further enable the DHA to take firmer control of key functional areas in preparation for a comprehensive implementation of the repositioning programme.

Funding/revenue generation model

- One of the key arguments for repositioning is that financial constraints are preventing the DHA from continuing with its transformation and threatens to undermine the progress it has made thus far.
- Although the DHA is a critical enabler of citizen empowerment, inclusive development, efficient administration and national security, it is currently not fully funded to deliver its mandate efficiently while its mandatory services to the public remain the same.
- A secure, modernised DHA that is funded at an appropriate level would be a key enabler of economic development and would generate new revenue streams and investments. To address this gap, an appropriate funding model for the DHA is of necessity and will contribute to ensuring that the DHA reposition itself to fulfil its vision of being a fully modernised and secure department, with professional staff and appropriate operating, organisational and funding models. There is a clear need for a new funding model for a repositioned DHA that is located within the security of the State.

It is envisaged that the deep-dive studies will be finalised during the 2020/2021 financial year, and they will enable the finalisation of a detailed (short-, medium- and long-term) implementation plans for repositioning the department; this includes the full operation of the population register and the NIS.

The department is in the process of establishing a programme management office (PMO) that will oversee the implementation of the repositioning programme. The strategic vision of the DHA PMO remains “A programme management office that is internally institutionalised and positioned as a catalyst to successfully deliver special projects of the department. DHA PMO strategic mission is to provide a solid foundation for the projects of the Department of Home Affairs by creating an environment of measurable, disciplined project management professionalism.”

Change management and communications are core elements of the repositioning programme. The shape of the repositioned DHA will inevitably be different; and will require an extensive change management programme over seven to 10 years.

The change management directorate has developed a change management strategy that includes the following elements:

- Awareness campaign on the repositioning programme
- Appointment of youth as change agents for the repositioning programme
- Appointment of senior managers as champions for the repositioning programme

- Training change agents on the repositioning programme and its implications for employees
- Preparation for a future-fit DHA.