Terms of Reference

Digital ID Legal Framework Support

Technical Advisory Services for the Digital ID System

Ministry of Interior, Federal Affairs and Reconciliation

Federal Government of Somalia

A. Project background

The Federal Government of Somalia (FGS) has received financing from the World Bank through the Somalia Capacity Advancement, Livelihoods and Entrepreneurship, through Digital Uplift Project (SCALED-UP) to support a series of reforms to create stability, and to foster sustainable economic and social development in Somalia (Project). As part of the reforms contemplated in the Project, the FGS, under the leadership of the Ministry of Interior, Federal Affairs & Reconciliation (MoIFAR) is in the process of introducing a robust, inclusive, and responsible foundational digital identification system that is envisioned to provide each resident of Somalia with unique and verifiable proof of identity. The digital ID system is expected to, *inter alia*, help increase access to and use of financial services, pave the way for effective public service delivery, and foster the formalization and digitization of the economy.

The envisioned digital ID system will be implemented in alignment with the recently adopted FGS Digital Identification Policy (Policy)[1], the implementation approach described in the Project's SCALED-UP project appraisal document [2] and the Principles on Identification for Sustainable Development[3]. The Policy sets out the objectives of the ID system and provides guidance on the nature of new legislation required to support it. All residents of Somalia will be eligible for enrollment, irrespective of citizenship status or ability to produce any prior documentation. The ID system will strive to provide a unique identity from birth to death, with close linkages to civil registration. In line with the data protection principles on proportionality, minimal disclosure, and non-discrimination, only minimal data will be collected, including biometrics. A unique and random ID number and other credentials, as necessary to facilitate access to services, will be issued free of charge to successful registrants.

As a foundational ID system, the digital ID system is intended to underpin 'functional' ID systems and registries (for particular sectoral purposes, e.g. social protection, financial services, etc.) and will strive for interoperability with other existing and future registries. MoIFAR will establish a dedicated ID authority with the mandate to implement and continuously manage the digital ID

[1] [Add citation to new Policy]

[2] http://documents.worldbank.org/curated/en/267241552269666297/pdf/Project-Appraisal-Document-PAD-SCALED-UP-P168115-revised-February-26-2019-02262019-636878520441412199.pdf

[3] World Bank. 2018. Principles on Identification for Sustainable Development: Toward the Digital Age. Available from: http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age.

system. Until the ID authority is established by law, an interim Task Force, operating under the aegis of the Ministry of Interior, will oversee the implementation of the FGS' Digital ID Policy, including the operationalization of a robust and secure ID system, as well as oversight of the process of developing legislation for both the ID system as well as data protection, referred to below

The foundational digital ID system is expected to enable the issuance of over 1 million unique IDs to the population within the next three years, including to at least 500,000 women, as well as to enable and promote the widespread use of the digital ID in the financial sector.

A review of the existing legal framework has revealed gaps in the supporting legal framework for the ID system, including in areas such as data protection, electronic authentication, and cyber security, to name a few. As contemplated under the Policy, a new, independent institution will be established to implement and operate the digital ID system. Likewise, the Policy contemplates a new, independent institution to be established to administer data protection in the country. The Task Force will initially coordinate activities regarding these areas, as provided in the Policy. The Chairperson of the interim ID Task Force – and its institutional successor, the ID Authority, once established – will liaise with the firm or consortium of firms to be procured with respect to the services covered in this TOR

B. Objectives

While the Ministry is in the process of procuring and developing a national digital ID system, Somalia currently lacks the enabling laws and regulations to support an effective, robust, inclusive and well-governed digital ID system. Accordingly, the Ministry is now procuring the services of a firm or a consortium of firms (Consultant) to support the Ministry in the preparation of the supporting legal framework based on international best practice for the Digital ID System to conduct public stakeholder consultations with both the public and private sectors and generally undertake the tasks and provide the deliverables contemplated in these Terms of Reference (ToRs).

C. Scope of work

In order to meet these objectives, the Consultant will undertake the following tasks:

1. Familiarization itself with the Project, the Policy, the outputs of other consultancies (including, without limitation, the gap analysis already produced), the current legal and regulatory framework, the views of major stakeholders and conduct such other necessary due diligence with respect to the elaboration of the supporting legal framework for the FSG digital ID;
2. Based on, *inter alia*, the findings from the due diligence phase of this engagement, the Project, the Policy and the Principles, prepare initial draft versions of the required legislation, reflecting best practice, including without limitation, (a) a draft ID enabling law (taking account of the issues reflected in Annex 1 attached to these ToRs and the need for a coordinated legislative approach between civil registration and identification) and (b) such other enabling legislation addressing issues of data protection, legal recognition of on-line

transactions, documents and signatures, and cyber-security/cybercrime (taking account of the issues reflected in Annex 2 attached to these ToRs), including recommendations regarding the institutional arrangements for any commissions, agencies or authorities overseeing the activities contemplated in these new laws;

3. Support MoIFAR to conduct public consultations with government and non-governmental stakeholders in Somalia and on-line on the draft laws;
4. Based on the comments received from the public consultation process, prepare final draft version of the laws in both English and Somali language; and
5. Throughout the conduct of its assignment, the Consultant will coordinate with other consultants working in civil registration and cybercrime legal reform.

D. Deliverables & Timing

The expected deliverables, and indicative timeline and payment schedule are set out below:

Deliverable	**Timing (Contract Signature +)**	**Contract Amount (%)**
1. Signing of Contract	n/a	10%
2. Inception Report (covering the issues described in § C.1, above, including any proposed changes to these ToRs)	4 weeks	25%
3. First draft of laws (covering the issues described in § C.2, above)	12 weeks	20%
4. Report on Public Consultation (covering the issues described in § C.3, above)	18 weeks	20%
5. Revised/Final Draft Laws (covering the issues described in § C.4, above)	24 weeks	25%

E. Administrative Arrangements

The Consultant will report to Chairperson of the interim ID Task Force – and its institutional successor, the ID Authority, once established - and will also liaise with other FGS and external stakeholders of the digital ID system, as needed. The stakeholders include FGS line ministries, Federal Member States, development partners, private sector entities, civil society organizations, and NADRA (as a technology provider). The consultants will be based in Mogadishu at the Ministry of Interior. The Consultant shall treat all documents and communications under this engagement confidentially.

The Consultant will be expected to prepare succinct and relevant documentation to support all recommendations, and to discuss recommendations with stake holders in-country. Except as otherwise provided in these Torus, all deliverables and reports will be in English language, and in Word, Excel and PowerPoint format, or equivalent. Draft versions of deliverables will be submitted electronically, and successive versions of reports will be marked to show changes from the previous draft. Copies of all deliverables will be provided to Task Force and the World Bank.

F. Firm Qualifications

The Consultant shall be a firm (or consortium of firms) whose team consists of legal specialists of high international repute with relevant international experience (minimum 12 years) in legal aspects of digital identification, e-commerce, digital authentication, cyber-security, data protection, access to information, and related issues, particularly in developing countries. The Consultant team will have a thorough understanding of the requirements and detailed knowledge of all key areas of policy and law with respect to the laws. Knowledge of and experience in the legal system in Somalia is highly desirable. The Consultant's team will include a lawyer knowledgeable of the Somali legal context and qualified to practice law in Somalia.

Annex 1
ID System Law Requirements[4]

The Consultant will draft legislation specific to the ID system, consistent with the Policy that is expected to include, *inter alia*, the following:

Purposes

- The broad policy purposes of the ID system
- A description of any identity verification, authentication, authorization or other capabilities
- The specific tasks and services for which the ID system may be used

Basic design and architecture

- Description of the basic technical architecture and key systems and features of the ID system, including issuance of an ID card and a unique "Tirsi" number
- Description of the ID card (format, technology to be used, information to be stored or displayed) and the Tirsi number (number of digits and how they are generated)
- Description of the types of personal data to be collected by the ID system, upon enrollment and throughout usage
- Limitations on personal data shown or readable on the ID card
- Establishment of interoperability with other ID systems and mutual recognition of ID credentials
- Limitations on information sharing between the ID system and other GoS entities (e.g., law enforcement) and third parties
- Requirements for vendor neutrality and use of open standards
- Requirements for use of privacy-enhancing technologies
- Credentialing or other requirements to ensure the security of information shared with third-party entities performing outsourced functions

Inclusiveness and non-discrimination

- Eligibility criteria, including specifying that all residents are eligible regardless of citizenship status
- Documentation and/or other requirements to prove eligibility (minimal and flexible to prevent exclusion)
- Clarification that enrolment is voluntary and a requirement that alternative means of accessing essential services are available for those who choose not to enroll
- Prohibition on collection of "sensitive personal data" (or equivalent category) that may subject the ID holder to discriminatory treatment (religion, ethnicity, gender, marital or socio-economic status, etc.)

[4] The issues described in this Annex may be in addition to those requirements described in Annexes 1, 2 and 3 of the Policy, all of which should be addressed.

- Prohibition on charges to individuals for normal enrolment (excluding premium services)
- Express protections against discrimination on the basis of race, religion, ethnicity, gender, sexual orientation, disability and other similar attributes

Institutional design

- Establishment of the powers, functions and competencies of the Ministry of Interior, Federal Affairs & Reconciliation with respect to the ID system, including:
    - setting ID system policy
    - interpreting ID system legislation
    - issuing regulations and other secondary legislation
    - establishing, overseeing and approving the budget (subject to Cabinet review) of the Federal Identification and Registration Authority (FIRA)
- Establishment of the powers, functions and competencies of FIRA, including:
    - responsibility for implementation of the ID system, including:
        - enrolment of individuals
        - setting standards, protocols, and policies, including certification of third parties, for data collection and oversee the enrollment and registration process
        - ensuring the secure storage of personal data
        - management of the federal identity database
        - issuing ID cards and Tirsi numbers
        - provision of identity verification and authentication services for public and private entities
    - conducting information, education, and communication activities to ensure universal accessibility and widespread use of the ID system and credentials
    - carrying out research on best practices and innovative identification approaches
    - coordinating with and supporting capacity building for civil registration authorities, including to facilitate data exchange and the use of shared technical infrastructure, where appropriate
- Establishment of governance arrangements of FIRA, including:
    - requirements for functional and administrative independence and accountability
    - appointment of a Board of Directors to provide oversight
    - establishment of a Stakeholder Consultative Working Group to provide inputs to the Board of Directors
    - requirements for diversity in management, reflective of Somali society
- Establishment of the budget and sources of revenue of FIRA including:
    - annual public budget
    - support from local and international donors
    - fees

Annex 2
ID supporting Legislation Requirements[5]

The Consultant will draft general data protection and privacy legislation, consistent with the Policy that includes the following:

- Applicability to public and private entities
- Requirements for collection and use of personal data, including:
  - fair, lawful and transparent collection and use of personal data, including setting out specific and limited grounds for such collection and use
  - limitation of collection and use and retention of personal data to the minimum necessary for a specified, explicit and legitimate purpose
  - requirement that personal data be accurate, complete and kept up to date
  - requirement that personal data be protected by reasonable security safeguards
  - limitations on cross-border transfers of personal data subject to approved cross-border identification purposes
  - accountability of entities that collect or use personal data for demonstrating compliance with applicable requirements
  - requirements for notifications in case of breaches
  - limitations on the use of automated decisions (i.e., without human intervention) about individuals based on personal information
- Individual privacy rights, including:
  - right to information about and access to personal data about a person
  - right to rectify, block or erase personal data
  - right to object to processing of personal data
  - right to data portability
  - right to object to profiling or automated decision making
  - right to an effective remedy
- Establishment or designation of an independent supervisory authority to enforce the legislation, including:
  - powers, functions and competencies, including complaint-receiving, investigative and enforcement capacities
  - governance arrangements
  - budget and sources of revenue

[5] The issues described in this Annex may be in addition to those requirements described in Annex 4 of the Policy, all of which should be addressed.

Electronic transactions and cyber security legislation

The Consultant will draft electronic transactions and cyber security legislation, consistent with the Policy, that includes the following:

- Establishment of legal recognition of electronic signatures, documents and contracts
- Establishment of a governing framework for electronic transactions
- Requirements and mechanisms to support identification and sharing of information regarding cyber threats within and between the GoS and private sector
- Designation of and establishment of cyber security requirements for critical infrastructure
- Criminal penalties for cybercrimes