Deployment of a Device Management System (DMS)

Project Information Memorandum

Submitted to:
Nigeria Communications Commission (NCC)

Prepared by:
Weircapacity Consortium

April 2022

Disclaimer

This Project Information Memorandum (PIM) is intended to provide interested parties with information on the Deployment of the Device Management System (DMS) (the Transaction), developed by the Nigerian Communications Commission (NCC) with the support from the project Transaction Adviser (TA), Weircapacity Consortium, and the approval of the Infrastructure Concession Regulatory Commission (ICRC), of the Federal Republic of Nigeria (FGN)

This PIM is presented for information purposes only and does not present a sales offer. No representation or warranty expressed and implied is made, or responsibility of any kind is, or will be, accepted by any of the NCC, TA, ICRC or any other member of the FGN with respect to the accuracy and completeness of the PIM. The information contained herein may be amended or replaced by NCC at any time without giving any prior notice or providing any reason. Any liability in connection with the use by any recipient of the information contained in this document is hereby disclaimed.

This PIM is provided to facilitate recipients in appraising the Transaction and in deciding whether to make a proposal, and for recipients to provide feedback, on the proposed Transaction. However, it is not intended to serve as the basis for an investment decision in the Transaction, and each recipient is expected to make such independent investigation and to obtain such independent advice as he or she may deem necessary for such decisions.

Deployment of a Device Management System Solution

This Project Information Memorandum (PIM) is presented in fulfilment of the requirement by the Infrastructure Concession Regulatory Commission (ICRC) for the Pre-Qualification of firms or consortium of firms, as part of the procurement of projects through Public-Private Partnership (PPP). It has been prepared by the Transaction Adviser (TA) engaged by the NCC for the delivery of the transaction services for the deployment of a Device Management System (DMS) Solution under Public-Private Partnership (PPP) model. The PIM document is to provide information for interested firms on the deployment of the DMS through PPP.

Contact

All questions and comments relating to technical issues in the Information Memorandum (IM) should be directed to:

Engr. Bako Wakil
Director, Technical Standards and Network Integrity
Nigerian Communications Commission (NCC)
Email: wakil@ncc.gov.ng

Table of Contents

Executive Summary 6
1. Policy and Strategic Objectives 7
2. Project Scope 8
3. Device Management System in Nigeria 9
4. Device Market Assessment in Nigeria 10
5. Legal and Regulatory Environment 11
6. Institutional Framework 12
7. Technical Solution 14
8. Transaction Structure and Project Risks 15

List of Figures

Figure 1: DMS Enablement 9
Figure 2: Unique device management penetration by population 10
Figure 3: Laws and regulations applicable to the DMS project 11
Figure 4: Institutional framework for the implementation of the DMS 12
Figure 5: CDOT DMS Modules 14

List of Tables

Table 3-1: Subscriber Data from NCC 11
Table 6-1: Risk Sharing Between Public and Private Partners 15

Acronyms/Abbreviations

Acronym	Meaning
ATU	African Telecoms Union
BPP	Bureau of Public Procurement
CDMA	Code Division Multiple Access
CDOT	Centre for Development of Telematics
DBFOM	Design Build Finance Operate Maintain
DMS	Device Management System
ECOWAS	Economic Community of West African States
EIR	equipment identity register
FBC	Full Business Case
FEC	Federal Executive Council
GDP	Gross Domestic Product
GSM	Global System for Mobile Communication
ICRC	Infrastructure Concession Regulatory Commission
ICT	Information Communication Technology
IMEI	International Mobile Equipment Identity
IM	Information Memorandum
IT	Information Technology
ITU	International Telecommunication Union
LTE	Long Term Evolution
MNOs	Mobile Network Operators
MWF	Mobile Wireless Forum
NBS	National Bureau of Statistic
NCA	Nigerian Communications Act
NCC	Nigerian Communication Commission
NCS	Nigeria Customs Service
NITDA	National Information Technology Development Agency
OBC	Outline Business Case
OEMs	Original Equipment Manufacturers
PPP	Public-Private Partnership
SIM	Subscriber Identity Module
SMS	Short Message Service
SON	Standard Organization of Nigeria
SOCCAP	Standard Organization of Nigeria Conformity Assessment Program
WATRA	West African Telecommunications Regulators

Executive Summary

The Nigerian Communications Commission (NCC) is exploring options to implement a Device Management System (DMS) to monitor, manage and secure the telecommunications sector in the country. DMS are a type of central remote management software used to monitor, manage, and secure mobile devices that are deployed across the various mobile service providers, and across the various mobile operating systems in Nigeria. The DMS system will create a single window for telecom devices enabling the NCC to proactively identify illegitimate or substandard devices that are not permitted on the Nigerian telecommunications network. The NCC intends to achieve the deployment of this DMS system using a Public-Private Partnership (PPP) arrangement. In this arrangement, the private partner will establish, operate, and manage a DMS for the estimated 200 million telecommunications subscribers in Nigeria.

The DMS is expected to have the capability to address the proliferation of fake, counterfeit, substandard and cloned mobile devices in the telecommunications industry in Nigeria. The DMS will enable NCC to collect International Mobile Equipment Identity (IMEI) data and integrate it into NCC's type approval process, so that stolen, illegal mobile phones and other smart devices are blacklisted and rendered inoperable. This solution is expected to reduce mobile phone theft, protect consumers' interests, and enhance national security.

The consumer market for telecommunication devices in Nigeria is far reaching and expanding rapidly. According to data from the NCC, there is an estimated 200 million subscribers of various telephony services currently in Nigeria. The opportunities a digitally literate population pose economically, socially, and developmentally are immeasurable. Conversely, the risks posed, especially coupled with a youth unemployment rate estimated by the National Bureau of Statistics (NBS) at about 45%, are severe. The NCC reports that cybercrime alone, one of such risks, contributes to 0.08 % of the GDP loss, about $500 million. Tax evasion, terrorism, and health and safety violations are other risks associated with an increasingly digitally literate, mobile dependent economy. All these potential risks necessitate the need to have adequate tools and resources, backed by conscientious regulatory measures, to manage the growing mobile economy.

To this end, a primary aspect of NCCs mandate, as stipulated in the Nigerian Communications Act 2003, is to; establish and enforce standards for all telecommunications equipment in operation, to ensure that they operate seamlessly and safely within the Nigerian telecommunications ecosystem.

This Information Memorandum (IM) presents a high-level summary of the business case and rationale for the DMS system. The document outlines result of a technical and legal assessment of the DMS project and presents a basic outline of the business case for the project.

1. Policy and Strategic Objectives

1.1. A considerable number of counterfeit ICT devices have found their way into global markets, including in Nigeria. The proliferation of these devices is raising concerns about national security, performance, quality of service delivery and potential revenue losses for all stakeholders. This has led to the call by ITU Member States, particularly those in developing countries to address the issue, especially its negative effects and to study the impact of measures taken to address it. Counterfeit mobile devices pose security and health risks to the consumer as well as economic risks to the brand that is being counterfeited. In the background of Boko Haram in Nigeria and other terrorist groups using cloned cell phones many key security concerns relating to counterfeit electronic devices arise. Additional issues involved are:

a. **Ransomware**: ransomware, a malicious software known to be designed to deny access to an electronic system until a ransom is paid and this may be included on counterfeit devices and may travel between devices on a network causing broader contamination.

b. **Keylogging**: some devices log keystrokes to capture usernames, passwords and any sensitive information that could be useful to criminals; and

c. **Data Theft**: personal or business data may be stolen given the low levels of security by design on counterfeit devices.

1.2. The NCC in collaboration with Mobile Wireless Forum (MWF) held an Industry Stakeholders Forum in 2015 and 2017. The objective of the engagement was to work towards developing recommendations that could influence decisions and policy directions, leading to solutions for combating counterfeit and substandard ICT devices in Nigeria.

Consequently, the government of Nigeria through the NCC, immediately constituted a Standing Committee to develop the required regulatory framework for identifying and isolating fake and counterfeit / non-type approved mobile devices in Nigeria. Accordingly, the Committee came up with an action plan, that ultimately led to the following proposed actions:

a. Effective Regulation and efficient enforcement of the Equipment Type Approval processes.

b. Strategic collaboration with all stakeholders within Nigeria and other international / Regional bodies such as the African Telecoms Union (ATU), ECOWAS, WATRA, GSMA, Mobile & Wireless Forum (MWF), Vendors, OEMs etc.

c. Protecting consumer rights and enhancing cooperation with the industry.

d. Deployment of empirical solution, the Device Management System (DMS).

2. Project Scope

The proposed DMS will provide a single control point for comprehensive device management for mobile and network devices. It will also support capabilities for the tracking of telecommunication devices to eliminate fake and substandard devices, provide detailed statistical information for stakeholders use, and support the fight against cybercrime and insecurity.

The scope of the DMS deployment project is Design, Build, and Finance, Operate, Maintain and Manage the deployment of a DMS solution within the terms and conditions that will be prescribed in a PPP Agreement. The DMS project has been certified by the ICRC for preparation and procurement as a PPP project, through a competitive bidding process via the Solicited PPP Procurement route. The project is in line with Nigerian Communications Act (NCA), 2003 and the ICRC Act 2005.

3. Device Management System in Nigeria

3.1. In NCC's role as the independent regulator of the telecommunications sector, the organization is responsible for creating an enabling environment for competition among operators, as well as ensuring the provision of qualitative and efficient services.

The NCC is required to ensure that all devices that are shipped into Nigeria, sold in Nigeria and/or deployed on the network are authorized in line with its Type Approval guidelines.

3.2. NCC's proposed DMS solution is based on the International Mobile Equipment Identifier (IMEI). Cloned or duplicated IMEI numbers are two of the more prevalent methods of introducing illegal devices unto the telecommunication network. A DMS solution based on the IMEI portends to address the single biggest source of illegal devices. An IMEI-based DMS solution can achieve:

- Curtail the counterfeit mobile phone market by permitting only registered IMEI number on the network.
- Discourage mobile phone theft, by making inoperable devices that appear on the network with a flagged IMEI number
- Enhance national security by eliminating illegal devices.
- Facilitate blocking or tracing of stolen mobile phones and other smart devices.
- Increase revenue generation for the government.
- Mitigate the use of stolen phones for crime.
- Protect consumer interest.
- Reduce the rate of kidnapping.
- Serve as a repository for keeping records of all registered mobile phones' IMEI and owners of such devices.
- The system will contribute to fair trade and competition in the market.

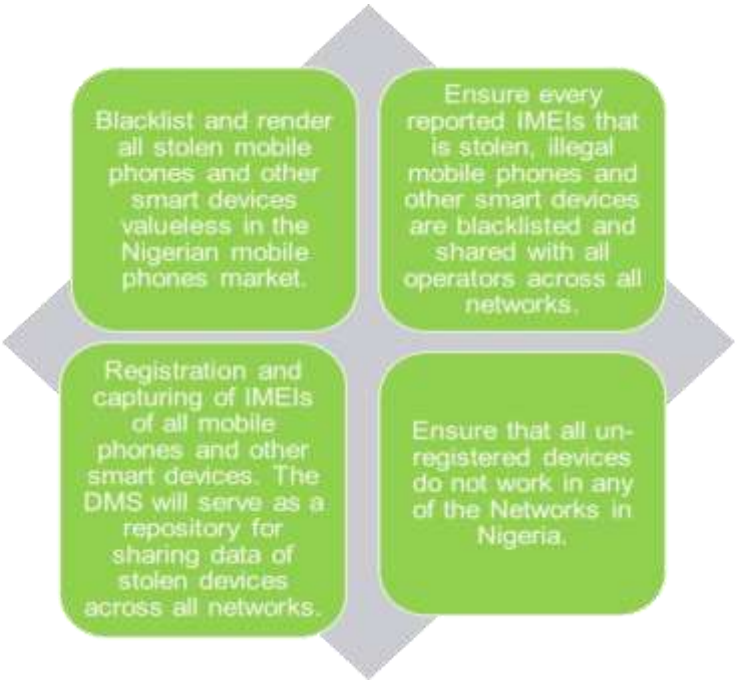

Figure 1: DMS Enablement

4. Device Market Assessment in Nigeria

4.1. With more than 200 million active lines on the Nigerian telecommunication network (as of December2021), there is great potential for the development of a DMS in the Nigerian market. It is estimated that there were approximately 132 million unique devices on the telecommunication network in 2020. Data from Original Equipment Manufacturers (OEMs) suggests that approximately 63 million devices are sold each year in Nigeria.

Estimates suggest that the average device owner changes devices every 6 –18 months. The size and turnover of the mobile device market offer vast opportunities for the implementation of a DMS.

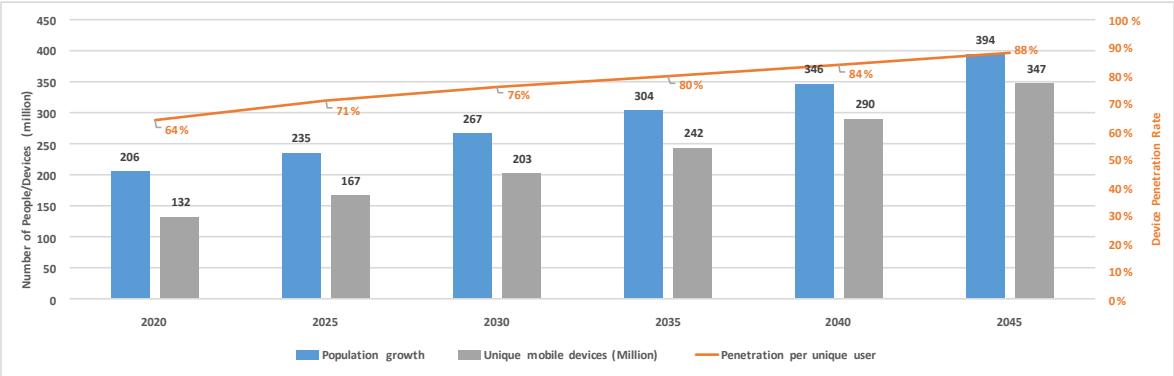

Figure 2: Unique device management penetration by population

4.2. The Nigerian Communications Commission (NCC) keeps detailed records of telecom network subscribers and active lines. The table below presents records for the period up to December 2021 and depicts a telecom density over 100 percent in the last quarter of 2021.

Table 3-1: Subscriber Data from NCC

	Operator	Dec'21	Nov'21	Oct'21	Sep'21
Active Lines	Mobile (GSM)	195,128,265	192,854,406	191,618,839	190,520,914
	Mobile (CDMA)	-	-	-	-
	Fixed Wired/Wireless	106,385	106,430	106,520	106,401
	VoIP	229,248	225,489	226,410	226,754
	Total	195,463,898	193,186,325	191,951,769	190,854,069
Connected Lines	Mobile (GSM)	304,048,720	299,970,153	229,582,206	229,467,077
	Mobile (CDMA)	-	-	-	-
	Fixed Wired/Wireless	218,354	218,223	217,862	217,789
	VoIP	1,114,366	1,107,875	1,101,333	1,094,094
	Total	305,381,440	301,296,251	300,901,401	300,778,960
	Tele density	102.40	101.20	100.56	99.98

4.3. The digital economy is equivalent to 15.5% of global GDP, growing two and a half times faster than global GDP over the past 15 years. According to NCC industry data, the telecom sector is estimated to contribute between 11 – 14 percent per quarter to GDP. This figure has been rising in the last few years consistent with increasing competition, decreasing telecom sector tariffs, and increasing tele-density. Innovations in the market such as 5G, nternet-of-Things (IoT) will only further the rate of penetration of telecom devices in Nigeria which makes the DMS project a welcome development.

5. Legal and Regulatory Environment

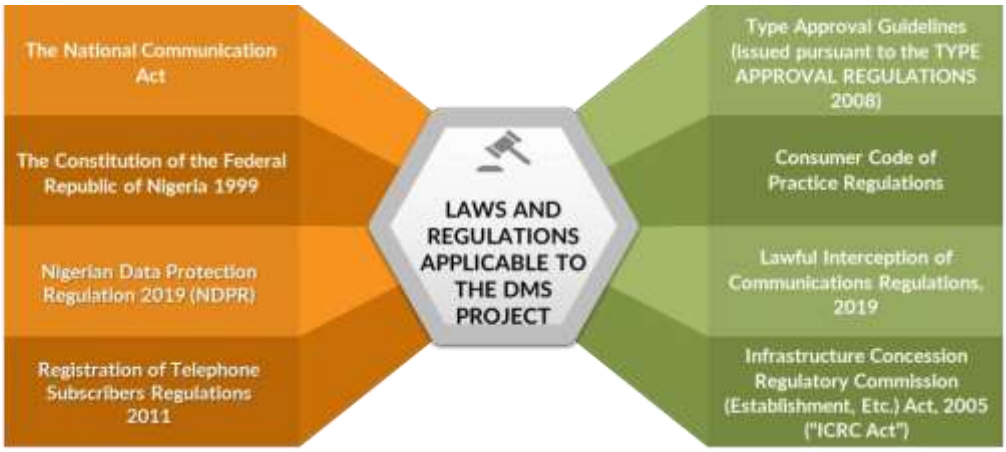

Figure 3: Laws and regulations applicable to the DMS project

5.1. Since the DMS project is to be implemented under a PPP model, there are specific laws and regulations applicable to PPPs which are:

a. The Infrastructure Concession Regulatory Commission Act 2005 ("ICRC Act")
b. National Policy on Public Private Partnership and its Supplementary Notes
c. ICRC Public Private Partnership Regulations 2014

5.2. The implementation of the DMS project will require licenses, permits and approvals as follows:

a. **Federal Executive Council** - The ICRC Act provides that all projects shall be submitted to the Federal Executive Council for approval on the recommendation of the relevant sector, ministry, or agency prior to entering any contract. In addition to the above all necessary approvals such as OBC and FBC approvals for the project will be gotten from FEC but sought through the ICRC.

b. **The NCC Directive**: The Nigerian Communication Commission in exercise of its statutory powers under section 148 of the NCA will have to issue an order to Network service providers, authorizing them to generate and provide IMEI of all subscribers on their respective networks.

6. Institutional Framework

Figure 4: Institutional framework for the implementation of the DMS

6.1. Figure 4 above highlights the institutions that will work together to ensure the success of the DMS in Nigeria.

a. Ministry of Communications and Digital Economy

The Minister formulates policy for the telecommunication sector. The Nigeria Revised National Identity Policy for SIM Card registration 2021 which set the tone for the commencement of the DMS project was released by the Ministry. The policy released in May 2021, has one of its focus areas- the development and deployment of a Device Management System (DMS) to fight against phone theft, kidnapping and other vices as well as the continued sale of substandard phones in the Country. The DMS is designed to be a repository for keeping records of all registered mobile phones' International Mobile Equipment Identity (IMEI) and owners of such devices.

b. Infrastructure Concession Regulatory Commission (ICRC)

The ICRC is the regulatory agency for PPP transactions in Nigeria. The ICRC provides technical/advisory support to line ministries and monitors the implementation of PPP projects. ICRC is part of NCC's Project Delivery Team for the procurement of the DMS project and, as per the ICRC Act, will take custody of the DMS PPP Agreement when effected and monitor the performance of obligations by both parties.

c. National Information Technology Development Agency (NITDA)

NITDA is statutorily mandated by the NITDA Act of 2007 amongst other functions to develop regulations for electronic governance and monitor the use and protection of electronic data interchange and other forms of electronic communication transactions. The NITDA issued the Nigerian Data Protection Regulation in 2019, in recognition of the protection accorded to private persons as it relates to their personal data which includes but is not limited to names, identification numbers, IMEI numbers, SIM and other personal identifiable information. By this regulation, the DMS controller is under an obligation to work with the NITDA to provide personal data of data subjects where required, and without consent of such data subjects where it is in furtherance of national security.

d. Nigerian Customs Service (NCS)

The two core functions of the Nigerian Custom Service are collection of revenue (import and excise duties) and prevention of smuggling. Another function of the NCS which is relevant to the DMS project is combating trade in illicit goods and import of fake and substandard goods. The NCS also works in collaboration with other government agencies at all approved ports and border station.

e. Standard Organization of Nigeria (SON)

The Standard Organization of Nigeria also regulates the standard of telecommunication devices such as mobile phones and other related products in Nigeria. SON requires that all telecommunication devices that are arriving in Nigeria port must be accompanied by SONCAP certificate. SONCAP is a pre-shipment verification of conformity to Standards process used to verify that products to be imported into Nigeria are in conformity with the applicable standards or approved equivalents, and technical regulations before shipment.

One of the objectives of the DMS project which is to increase capacity to detect clones, counterfeit or sub-standard devices aligns with the mandate of SON as an organization.

7. Technical Solution

7.1. The technical approach is based on the implementation of a DMS system in India. India was selected as the benchmark case because its telecom sector has several factors that are comparable to Nigeria. For instance, there are multiple large operators in the Indian telecom market. The telecom network is spread over a wide geographic area and there is a significant underserved population.

The Indian DMS system was setup by the Center for Development of Telematics (C-DOT), a technology center of excellent for the Government of India. Prospective bidders will be expected to propose architecture that addresses the unique requirements of the Nigerian market.

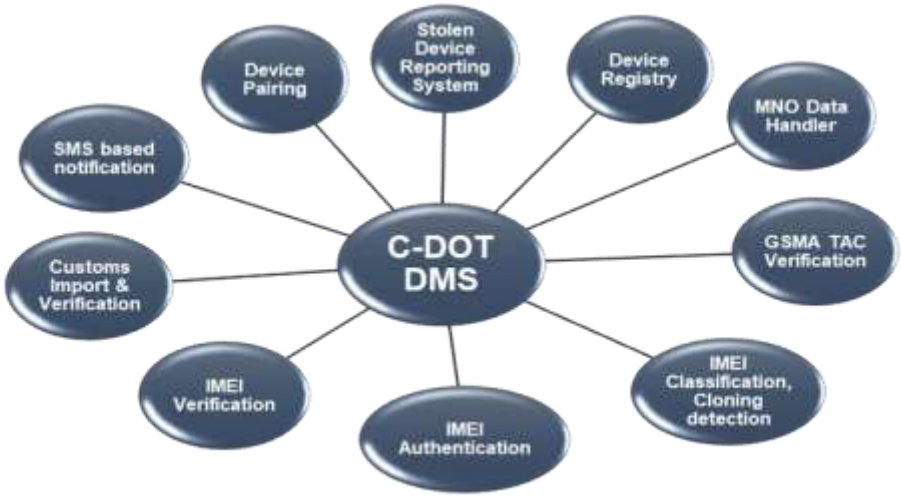

Figure 5: CDOT DMS Modules

7.2. The C-DOT DMS provides a single, unified access point for authentication of mobile devices in the network. It is a fully standards compliant, 100% software-based product and supports 2G/ 3G, 4G/ LTE, 5G and IT interfaces. It also offers an extensive feature set for implementing service logic, active triggering, reporting, alarming and more.

C-DOT DMS is a web-based system which hosts nationwide database containing the IMEIs of all the mobile devices used in the mobile network and the reported blacklisted mobile devices in a country. It acts as a central system for all MNOs to share the black-listed IMEIs nationwide. All MNOs need to provision their EIR blacklist from DMS blacklist. In this way an IMEI which was blocked by one Telecom Circle-MNO will not work in all the other Telecom Circle-MNO. If the stolen mobile is tried to be used - corresponding traceability details will be presented to the local state police for recovery. It also maintains Device Registry of all mobile devices available in the country. The system also provides other features like mobile device verification, authentication, device pairing etc.

8. Transaction Structure and Project Risks

8.1. The table below highlights the DMS project risks and allocation between NCC and the private party.

Table 7-1: Risk Sharing Between Public and Private Partners

Nature of Risks	Risks better allocated to Private Sector	Risks better allocated to Public Sector	Shared
PROJECT RISKS			
1. Regulatory Risks			
1.1 Modifications to national data privacy legislation		Yes	
1.2 Regulatory and policy makers' indecisiveness and trend towards protectionism		Yes	
1.3 Lack of consistent rules and legislation at global, regional, country, and local levels		Yes	
2. Technology Design Risks			
2.1 Design not fit for purpose	Yes		
2.2 Delays in design completion	Yes		
2.3 Revisions to global data management best practices	Yes		
2.4 Challenge to identify genuine device once duplicate IMEIs are detected	Yes		
3. Technology Acquisition & Deployment Risks			
3.1 Difficulty in achieving required standards and specifications	Yes		
3.2 Project management	Yes		
3.3 Labour dispute risks	Yes		
3.4 Subcontractor dispute or insolvency	Yes		
3.5 Staff health risks	Yes		
3.6 Time overruns	Yes		
3.7 Delays in acquiring regulatory approval		Yes	
3.8 Change in the landscape of mobile operators			Yes
3.9 Enhanced tactics of malicious actors using illegal mobile devices	Yes		
4. Operations and Maintenance Risks			
4.1 Failure to achieve service standards/performance standards	Yes		
4.2 Technology downtime / blackouts	Yes		
4.3 Interface risks between technology and mobile operators			Yes
4.4 Increased level of digitization has exacerbated the risk of cybercrime			Yes

Nature of Risks	Risks better allocated to Private Sector	Risks better allocated to Public Sector	Shared
5. Resource or Input Risks			
5.1 Increased cost or limited availability of input materials	Yes		
5.2 Scarcity of technical staff to administer and maintain technology solution	Yes		
6. Revenue Risks			
6.1 Revenue shortfalls compared with forecasted figures	Yes		
6.2 Revenue risk due minimal uptake of technology	Yes		
7. Other Project Risks			
7.1 Early termination			Yes
7.2 Change of concessionaire ownership			Yes
7.3 Default by external funding sources	Yes		
COUNTRY RISKS			
8. Political Risks			
8.1 Changes in technical requirements by government		Yes	
8.2 Delays in regulatory approval by government		Yes	
8.3 Public opposition		Yes	
8.4 Changes in laws and regulations		Yes	
8.5 Risk of government intervention, discrimination, seizure, and expropriation of the project			Yes
8.6 Risk of selective internet blackout by the government		Yes	
8.7 Limited cooperation and misaligned interests with national security services and customs officials		Yes	
9. Financial Risks			
9.1 Rise in interest rates	Yes		
9.2 Foreign Currency fluctuation	Yes		
9.3 Inflation rates	Yes		
9.4 Changes in tax rates	Yes		
10. Other			
10.1 Weather events and natural disasters			Yes
10.2 Political Instability/Security related risks			Yes
10.3 Collusion between malicious actors dealing in illegal mobile devices and relevant authorities			Yes