Terms of Reference

Technical Assistance for Implementation of the technical and organizational actions of the National Cyber Security Strategy

(National Center for Cyber Security - NNCS)

A. Context

1. Framework

The Republic of Cabo Verde has requested a $20 million loan from the World Bank to finance the Cabo Verde Digital project (P171099). The project aims to support the Government of Cabo Verde (GoCV) in the implementation of the main priority initiatives of the national ICT and e-governance policy implementation strategies, as well as to continue supporting the strengthening of the national telecommunications sector, and intends to apply part of the resources to contracting Technical Assistance for the implementation of the project, whose objective is to contribute to the transformation of the country into a regional digital hub to accelerate its digital economy through an improved digital infrastructure and reinforced demand for digital services and skills.

To implement the actions defined in the National Cybersecurity Strategy (ENCS), the project, in the *Enabling Legal and Regulatory Environment Component 1,* will support the GoCV in its efforts to implement measures that will make it possible to operationalize the ENCS and improve the global assessment of cybersecurity in the country, ensuring adequate, integrated and systematic protection mechanisms for critical infrastructures and citizens in cyberspace, thereby boosting the National Digital Economy.

1.1. Cabo Verde

Located 500 kilometers off the west coast of Africa, Cabo Verde is an archipelago of 10 islands. The country has an estimated population of 520,500 on nine of the islands. Only 10% of its territory is classified as arable land, and the country has limited mineral resources.

Cabo Verde's economy is driven by tourism based on an attractive year-round climate, beautiful beaches, stable democracy, limited security risks, and proximity to Europe.

Cabo Verde is a low-middle-income country with a GDP per capita of 4.5% in 2018 and a population of 0.5 million. With development indicators such as life expectancy at birth at 73 years (the highest in Sub-Saharan Africa) and an adult literacy rate of 87%, Cabo Verde ranks 121st out of 188 countries on the 2016 UN Human Development Index and it is considered a medium-developed country.

Consolidating its achievements as a middle-income country and further strengthening the conditions for reducing poverty and boosting shared prosperity requires efforts to boost human capital, reduce public debt, improve public sector efficiency, strengthen connectivity and create resilience to natural disasters. With its small open economy, the country is vulnerable to the vagaries of global economic development. Given the fixed exchange rate with the euro, it will be vital for the country to rebuild fiscal buffers to absorb future shocks. Diversification within and outside the tourism sector and more flexible labor markets can help absorb shocks.

1.2. Current State of Cabo Verde's Digital Economy

The vision of Cabo Verde's Digital Strategy (EDCV) is: "A Cabo Verde interconnected, with itself and with the world, developed, inclusive, democratic, open to the world, modern and secure, where full employment and full freedom prevail". It articulated three priority pillars, including the expansion of the connectivity infrastructure, the improvement of capacity and the provision of digital services through a regional market.

Several projects are currently underway to support the vision of the ICT sector, which has resulted in significant growth over the last decade. For example, the EllaLink project, which is a submarine cable connecting Brazil and Portugal via Cabo Verde, would solve the problem of redundancy of Internet connectivity in Cabo Verde given the current dependence on WACS infrastructure, and would also bring an additional 400 Gbps of capacity.

With additional capacity available, the objective will be to significantly reduce Cabo Verde's digital divide by providing universal access to connectivity within the various islands of the archipelago, through public-private partnerships. This will support high-speed connectivity and access to online academic content for higher education institutions and secondary schools, and will enable greater adoption of the WebLab program, which aims to empower the next generation of digital leaders for government and the private sector.

To achieve the connectivity objectives, the Government of Cabo Verde has also promoted Public-Private Partnerships and Private Sector Direct Investments, in order to stabilize, utilize, and preserve: (i) the launch of the "Amílcar Cabral" network consisting of fiber optic cables to sub regional capitals: Nouakchott, Dakar, Banjul, Bissau, Conakry, Freetown and Monrovia (ECOWAS); (ii) the connection to the PEACE fiber optic cable, through South Africa and Mozambique; (iii) the launch of the DILCE fiber optic cable between Cabo Verde and the United States (Boston); (iv) the renewal and implementation of "sub-loops" in the inter-island fiber-optic network; (v) the construction of the Mindelo Data Center (DC3); (vi) and the expansion of the Praia Data Center (DC2).

Cabo Verde has also invested significantly in the creation of a world-class data center at Parque Tecnológico da Praia (The Technology Park of Praia). With seven security levels, it houses and manages data and provides services to the Government of Cabo Verde, companies, banks, and national and foreign entities. It is also designed to offer "cloud computing" services.

In addition to connectivity, the government intends to build a Regional ICT HUB in Cabo Verde through the creation of communication networks that will enable the provision of services such as IP connectivity, cloud services, wholesale international connection to neighboring countries, installation of national and regional IXPs, and Internet peering.

The percentage of people who use the Internet in Cabo Verde has grown significantly over the last two decades, with 57.162% adherence in 2017, compared to 0.241% in 1997. According to the ITU, there were 3.03 percent of fixed (wired) broadband subscriptions per 100 inhabitants, compared to 70.01 percent of active mobile broadband subscriptions per 100 inhabitants in 2017. According to the World Economic Forum's Global Competitiveness Index Report 2017-2018, Cabo Verde ranks 84th in the world in Technology Readiness (including availability of the latest technologies, mobile and fixed broadband subscriptions, and Internet bandwidth), and ranks 136th in the global cybersecurity index (with technical initiatives/measures as the main point to be improved).

1.3. Current status of ENCS implementation

ENCS was created in 2016 for a period of four years, with the following concrete objectives:

- Creation of the National Center for Cyber Security and CSIRT-CV;
- Ensure cybersecurity in critical infrastructures;
- Ensure cybersecurity in National Defense;
- Creation of a cybersecurity culture in society;

Below is the action plan defined in the strategy, as well as the status of each action:

	I. LEGAL MEASURES	

Item	Action Description	Status
I.1	**Proposed General Legislation on Cybersecurity**	
I.1.1	• General Applicable Cybersecurity Standards	Done
I.1.2	• Specific application rules for Critical Infrastructures	
I.1.3	• Legal framework of CNCS and CERT	Done
I.1.4	• Clarification of roles in the response to computer incidents	
I.3	**Identification of critical infrastructure**	
	II. TECHNICAL MEASURES	
Item	**Action Description**	
II.1	**Technical implementation of CERT CV**	
	• Prepare a proposal for the organizational structure of the CERT CV	Done
	• Prepare terms of reference for technological infrastructure	Done
	• Prepare a Recruitment and Training Plan	In progress (OCWAR-C)
	• CERT technical project	In progress (OCWAR-C)
	• CERT installation	In progress (OCWAR-C)
II.2	**Country Cyber Security Risk Analysis**	
	• Prepare terms of reference	Done

	• Current state of cybersecurity assessment	Done (CMM - Oxford)
	• Seek financing (international partnerships)	
	• Hire a consultant to support the process.	
	• Perform risk analysis	
	III. ORGANIZATIONAL MEASURES	
Item	**Action Description**	
III.1	**Proposal to define a definitive Governance structure for Cybersecurity**	
	• Define who is in charge and who is the national focal point for international organizations in order for the country to speak with one voice.	
III.2	**CNCS Organizational Structure Proposal**	
	• Propose an organizational structure	
	• Propose an action plan for the installation	
	IV. TRAINING	
Item	**Action Description**	
IV.1	Technical Staff Training Plan.	
	• For CNCS (including CERT)	In progress (OCWAR-C)
	• For institutions that collaborate with CERT (Banks, CI operators, NOSi, SNIAC, IT-related private parties, Universities, etc.)	In progress (OCWAR-C)

IV.2	Training Plan for personnel from the judicial system and from criminal police bodies and other entities	
	● Training of Magistrates, attorneys, lawyers, etc.	Done
	● Training of judicial police personnel	
	● SIR staff training	
IV.3	Awareness plan for civil servants and company employees as well as the general public	
IV.4	Cyber Defense Training Plan (Armed Forces and Ministry of Defense Staff)	
	V. COOPERATION	
Item	**Action Description**	
V.1	Prepare a cooperation plan in which all cooperation actions are integrated and thus avoid duplication of actions, and yielding better profitability from international support:	
V.1.1	● GLACY Project (Cooperation with the Council of Europe)	Done
V. 1.2	● Process of accession to the Malabo Convention	Done
V.1.3	● Integrate worldwide CERT and CSIRT networks	
V.1.4	● Fostering cooperation at the national level between institutions.	
V. 1.5	● National Defense Cooperation	
V.1.6	● Cooperation at the level of judicial and police bodies	

B. Objective

The main objective of this technical assistance is to support the implementation of technical and organizational measures of the ENCS, which promotes a secure and reliable environment for the use of ICT services and to improve data protection and boost the development of the digital economy in the country. In particular, it will involve the support of the National Center for Cyber Security (NNCS) in defining the necessary technical and organizational actions to promote electronic commerce, protection of personal data and foster a culture of cybersecurity across the country, including combating cybercrime and related reforms.

C. Specific Objective

In order to design the right cybersecurity environment for promoting the economy, the following activities will need to be implemented:

1. Regulation of the legal framework for electronic transactions

Considering that there is legislation in force, which is being updated, it is necessary to adapt the regulations of the ICP-CV to the new legal framework, in order to allow the use of new technologies, and to bring the ICP-CV into line with the best international practices, allowing the signing of future interoperability agreements with public key infrastructures and integration into trusted lists of other countries.

For the purposes of regulating the legal framework, the consultant must provide for the preparation of rules, a Certification Practices Statement, Certification Policies, Security Policies, Accreditation Standards, a definition of criteria for implementing a *National Trust List* compatible with best practices, review the operational procedures of the ECR-CV and the second level Certification Bodies, and define the certificate profiles of the different entities.

2. *WebTrust* for ECR-CV

Recognition of the digital certificate of the Cabo Verde Root Certification Entity (ECR-CV), and the chain of trust of the Cabo Verde Public Keys infrastructure (ICP-CV) in browsers and CCADB repositories (Mozilla, Google and Microsoft) and AATL (ADOBE) is important for the development of electronic transactions, e-commerce and will confidently boost the Digital Economy.

For this purpose, the implementation of an auditing service with *WebTrust* quality is foreseen at ECR-CV, which will then facilitate the process of transmitting trust to the other members of ICP-CV, thus reducing the operating costs of the various Entities of Country Certification.

Consulting services must provide for the necessary steps to be taken to include the ECR-CV certificates in the CCADB (Mozilla, Google and Microsoft) and AATL (ADOBE) repositories. The Auditor must train and transfer practical knowledge to the Accreditation Authority's audit team and undertakes to perform, among others defined by them, the following Audits for the purposes of obtaining *WebTrust* certification:

- Root Key Generation Ceremony Audit (RKGC);
- WebTrust for CA and SSL Point-in Time Audit;
- WebTrust for CA and SS Period-of-Time Audit.

The Auditor must comply with the *WebTrust* specifications to carry out the work and follow good international practices.

3. *Awareness* – Cybersecurity Culture

- Prevalence and design of awareness programs for cyberspace risks and threats, as well as how to face them, both for the general public and for executive management;
- Development and implementation of a national cybersecurity awareness program as part of the implementation of the National Cybersecurity Strategy. Ensure that international examples contribute to these awareness programs;
- Development ethical hacking activities in selected Ministries and Agencies (to be defined with the beneficiary), not only to create awareness of their Cybersecurity gaps, but also to create a roadmap to address them;
- Creation of the national online Cybersecurity Portal and use the Portal and social media to publish appropriate cybersecurity information and disseminate materials to target groups as part of the national cybersecurity awareness program;
- Define metrics to determine the success of all cybersecurity awareness efforts;
- Together with Ministries of Education and/or Universities define and coordinate cybersecurity curricula for schools and universities and, where necessary, develop new curricula based on international best practices;
- Collaborate with stakeholders from higher education and the public and private sectors to identify training needs and develop an industry-based learning program that allows students to gain practical experience in cybersecurity and the use of technology;

D. Methodology

Taking into account the national context, the consulting firm will need to familiarize itself with the existing legal and regulatory environment, institutional capacity, judicial and oversight capacity, and technical and institutional framework relevant to ICT systems, digital platforms, public key infrastructure, electronic transactions and data protection.

E. Deliverables

The project is expected to be completed in 12 months.

The following deliverables will be expected from the various activities to be performed:

Component	***Deliverable***	***Description***	***Type***	***Payment after Approval by the Client***	***Schedule***
Strategy approach	***Inception Report***	*Overview of the job to be done within the scope of work including the* – Roadmap of the implementation consultancy	*Report*	*15%*	*Signing of the contract + 0,5 months*
Regulation of the legal framework for electronic transactions and e-commerce					
	D1- Regulation of standards	• Requirements for Security Auditor Accreditation; • Minimum Physical Security Requirements for Installations of Certifying Entities; • Requirements for Certifying Entities that issue Qualified Certificates; • Rules for the Audit of Certifying Entities that issue Qualified Certificates; • Technical specifications and formats of the trust lists; • Minimum Physical Security Requirements for Registration Unit Facilities;	*Document*	*15%*	*Signing of the contract + 1,5 months*
***WebTrust* for ECR-CV**					

	D2- WebTrust Audit	• Compliance assessment of QSCD and timestamp • Audit for CA Point-in Time (Pre-operational) • Audit for SSL Point-in-Time (Pre-operational) • Audit for CA Period of Time Audit (Optional) • WebTrust for SSL Period of Time Audit (Optional)	*Report, Document,* *Database*	*15%*	*Signing of the contract + ~~(45+10+180 = 235) 235 days~~* *8 months*
	D3 – Final Report	• Remediation • WebTrust for CA Assurance • WebTrust for CA Application		*30%*	*Signing of the contract + ~~270 days~~* *9 months*
***Awareness Raising* – Cybersecurity Culture**					
	D4- Report of public consultation workshops on institutional reforms with stakeholders for capacity building / knowledge transfer	• Cybersecurity/cybercrime awareness program; • Framework for education, definition of curriculum for cybersecurity/cybercrime for Bachelor, Graduate, Masters and/or Doctoral degrees; • Professional training – practical and internationally recognized cybersecurity/cybercrime courses;	*Report*	*10%*	Signing contract + 10 months
	D5- Final report	Institutional reforms, stakeholder capacity building and awareness raising, with clear awareness assessment metrics	*Report*	*15%*	Signing contract + 11 months

Unless otherwise stated in this ToR, all results and reports will be provided in Portuguese and English in Word, Excel and PowerPoint format or equivalent. Preliminary versions of the final results will be submitted electronically and successive versions of the reports will be marked to show changes from the previous draft. Deliveries must be sent to the Special Projects Management Unit (MF-UGPE), with copies of all deliverables provided to NNCS and the World Bank.

F. QUALIFICATOINS OF THE CONSULTANT

The assignment will require a consulting firm with at least 10 years of experience in the areas of Cyber security to guarantee a Digital Economy Strategy, data governance, public key infrastructure (PKI) and emerging technologies in insular countries. They should have experience in working on similar projects and countries.

a) The consultant must have at least ten (10) years of experience in PKI audit and at least five of (5) of them in Web Trust Audit;
b) The consulting firm must have at least three (3) experience in drafting regulations and procedures for PKI;
c) The consultant must have experience in the design and implementation of cybersecurity awareness campaigns.
d) The consultant must have Web Trust Audit implementation experience;
e) The consultant must have experience at least one CA implementation;
f) The consultant must engage Web Trust (CPA) listed audit company and must; submit the agreement document;
g) The experience and knowledge of Cape Verde PKI will also be relevant;

The team should be comprised of the following key experts:

1) Team Leader:

- Bachelors or post graduate degree in computer science or related field;
- At least 7 years in managing large audit engagements;
- Strong experience in information security and pki assessment processes with proven experience (plus certification for that purpose: CISSP, Webtrust Auditor, ISO 27001 Lead Auditor, PMBok, ITIL, COBIT 5);
- Have at least 5 projects assignments related to information security and pki assessment;
- Fluency in one or the other of Portuguese or English and proficiency in the other; and
- Experience in these areas in Africa will be a plus.

2) Legal Specialist:

- At least 10 years of relevant experience of practicing law;
- Relevant experience in advising and drafting laws which are the subject matter of these ToRs, global and regional legal standards and best practices, including emerging legal issues, in the Domains and related fields;
- A demonstrably successful track record in one or more similar assignments;
- Experience in these areas in Africa will be a plus.

The Local Legal Specialist shall have:

- Local qualification/accreditation to practice law in Cabo Verde:
- Good understanding of the Cabo Verde legal context with at least 8 years of relevant experience of practicing law, including in Cabo Verde, with an emphasis on advising and/or drafting of laws and/or regulations in Cabo Verde; and
- Fluency in Portuguese and proficiency in English.

3) Engineering Expert- Web Trust Auditor:

- Bachelors or post graduate degree in computer science or related field;
- Have more than ten (7) years of experience as a senior auditor in PKI Systems;
- Possess a Web Trust audit license;
- Have COBIT, ITIL, ISO 27000 family certification
- Have performed at least 3 (three) *WebTrust* audits and 5 (five) years' experience in process related to web trust;
- The Consultant must have at least three (3) experience in drafting regulations and procedures for PKI;
- Experience in Capacity Building as referred to in these ToRs;
- Must have experience in the design and implementation of cybersecurity awareness campaigns;

4) Technical Expert:

- Bachelors or post graduate degree in computer science, Cybersecurity, or related field.
- At least 5 years of professional experience in cybersecurity.
- Relevant experience in similar assignments focusing on cybersecurity policies.
- Specific knowledge of the cybersecurity models and best practices.
- Fluency in one or the other of Portuguese or English and proficiency in the other.
- Experience in Capacity Building as referred to in these ToRs;

G. A Lump-Sum form of Contract shall be signed with the Consulting Firm, and the inherent payments are linked to approval of deliverables specified on item E. above (Time Schedule for Deliverables) and the payment of reimbursable expenses are made upon presentation of the receipt of the incurred expenses at the actual cost.

Annex 1

Existing Legal Instruments

Legal Document	Date of underwritten/approval	Description
Cybercrime		
Law No. 8 IX 2017 - Cybercrime Law		Cybercrime
Law No. 9/2021 - Cybersecurity Law		Cybersecurity
E-commerce/E-transactions		
Decree-Law No. 33/2007,	September 24th	Regulates the use of electronic signatures, recognition of their legal efficiency, certification activity, as well as electronic contracting
Regulatory Decree No. 18/2007	December 24th	Decree Law 33/2007, of September 24, which regulates the use of the electronic signature, the recognition of its legal efficiency, the certification activity, as well as electronic contracting
Decree-Law No. 44/2009	November 9th	Creates the Public Key Infrastructure of Cabo Verde, called ICP-CV, aimed at establishing an electronic confidence structure
Ordinance No. 4/2008	February 18th	Indicates the amount of fees due for accreditation and registration of certifying entities for digital signatures
Ordinance of the Ministry of Infrastructure, Transport and the Sea No. 2/2008	January 28th	Sets the registration terms of certifying entities that issue qualification certificates.
Data Protection		
Data Protection Law (Law 133/V/2001 (as amended by Law 41/VIII/2013) and Law 132/V/2001, of 22 January 2001.		
Intellectual Property Rights		
[Others]		
Consumer Protection		

Decree-Law No. 46/2007 (in Portuguese)		
[International Treaty Obligations related to Digital Economy Law Domains]		
Berne Convention for the Protection of Literary and Artistic Works (Berne Convention)		Copyright
Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)		
World Intellectual Property Organization Copyright Treaty (WCT)		
Budapest Convention for Cybercrime and Digital evidence		
Malabo Convention for Cybersecurity, cybercrime and data protection		