



**Digital Transformation for Africa / Western Africa Regional Digital
Integration Program (DTfA/WARDIP SOP1)**

REQUEST FOR EXPRESSION OF INTEREST

**CONSULTANCY FOR INSTITUTIONAL FRAMEWORK DEVELOPMENT FOR THE
NATIONAL DIGITAL FORENSICS LABORATORY**

Country: The Republic of The Gambia

Project Name: Digital Transformation for Africa / Western Africa Regional Digital Integration Program (DTfA/WARDIP SOP1)

Project ID: P176932

Reference: WARDIP/C3.4.1/2025/CS/QCBS001

Assignment Title: Institutional Framework Development for the National Digital Forensics Laboratory

Duration of the assignment: Six (6) months

Deadline of submission : 8th August, 2025, 16:00 GMT

Deadline of submission : 27th August, 2025, 16:00 GMT

Selection Method: Quality and Cost Based Selection

Background

The growing scale and sophistication of cyber threats demand robust national capabilities for digital evidence handling, forensic investigation, and the prosecution of cybercrime. Recognizing this, the Government of The Gambia, through its National Cybersecurity Strategy (2022–2026), has committed to enhancing the operationalization of the Digital Forensics Lab (DFL) a critical entity to support national cybercrime response efforts.

While the DFL is envisaged as a modern facility for processing and storing and investigating digital evidence, its effectiveness relies not only on physical infrastructure and technical tools, but on a functional institutional framework that enables its full operationalisation. As outlined in The National Cybersecurity Policy 2022-2026 under Action Point 7.6.3.1.1.5 (Page 26), one of the key strategic actions is to “*establish the requisite framework to operationalize a digital forensics laboratory.*”

This entails developing clear institutional mandates, governance structures, inter-agency coordination mechanisms, standard operating procedures, and legal and regulatory alignment to ensure that the DFL can function efficiently and with credibility. Furthermore, it must ensure role clarity among stakeholders such as law enforcement, intelligence agencies, the judiciary, regulatory bodies, etc.

This consultancy is therefore initiated to design a comprehensive institutional framework that will underpin the full operationalization of the DFL. The framework will define the roles, responsibilities, policies, protocols, and coordination mechanisms required for the lab to operate effectively and sustainably in support of national cybersecurity and digital justice efforts.

Objectives of the assignment:

OBJECTIVES OF THE ASSIGNMENT

The main objective of this consultancy is to design, develop and deliver a clear, practical institutional framework to operationalize the National Computer Forensics Laboratory (NCFL) in The Gambia.

Specific objectives include:

- Assess current institutional arrangements, governance gaps, and stakeholder needs related to digital forensics and other documents, such as MoUs, SOPs, etc.
- Define a governance and management structure for the DFL, including leadership bodies, reporting lines and decision-making authorities.
- Clarify roles and responsibilities of all stakeholders (law enforcement, judiciary, intelligence services, regulators and DFL staff) in the digital forensics process.
- Develop a draft standard operating procedures (SOPs) for evidence collection, analysis, storage, chain of custody, disposal, etc.
- Review existing legal and regulatory frameworks; recommend amendments or new provisions to enable NCFL operations.
- Design inter-agency coordination mechanisms, including communication channels, referral protocols and joint working groups.

Activities, Deliverables and tentative Timeline:

TIMEFRAME:

Deliverables	Timeframe	Responsibility
PHASE I		
Stage 1.1: Situational and Capacity Assessment:	Week 1-2	Consultant
Stage 1.2: Institutional Framework:	Week 2-3	Consultant
Stage 1.3: Legal and Regulatory Alignment:	Week 3-4	Consultant
Stage 1.4: Infrastructure and Human Resource Assessment and Planning:	Week 4-5	Consultant
Stage 1.5: Sustainability and Resource Mobilization Strategy:	Week 5-6	Consultant
PHASE II		
Stage 2.1: Procurement of Equipment, Application, Licenses, etc.	Week 6-8	Consultant
Stage 2.2: Installation, configuration, and	Week 8-9	Consultant

commissioning of all components of the Digital Forensics Laboratory (DFL) as required in this TOR		
PHASE III		
Stage 3.1: Draft Training Curriculum Stage 3.2: Training Materials Package	Week 9-10	Consultant
Stage 3.3: Two (2) Days Validation Workshop of all Deliverables	Week 10 - 11	Consultant
Stage 3.4: Submission of All Deliverables after Validation Workshop	Week 11- 12	Consultant
Deliverables	Timeframe	Responsibility
PHASE I		
Stage 1.1: Situational and Capacity Assessment:	Week 1-2	Consultant

III. QUALIFICATIONS:

Firm's Experience:

The Consulting Firm must demonstrate extensive experience in cybersecurity, digital forensics, or institutional framework development. The Firm should have:

- A minimum 10 years of operational experience delivering consultancy services in cybersecurity and digital forensics
- Proven track record in successfully executing at least three(3) similar institutional frameworks or digital forensics projects, preferably for law enforcement, government, or international organizations.
- Must have a strong background in Project Management with at least 3 years of managing similar projects.
- Experience working in the African region or in developing country contexts will be an added advantage.
- Availability of a multidisciplinary team with expertise in cybersecurity, digital forensics, legal and regulatory affairs, and project management.
- Experience in Digital Forensics Tools like Cellebrite UFED, Cellebrite Physical Analyzer, XRY Software, BlockBox Lab XL (RF Forensic box), X-Ways Forensic etc. would be an added advantage.

Consultant (s') Experience: Project Coordinator

The Consultant(s) is required to have the following qualifications:

- A Master's Degree in Cybersecurity, Computer Science, Cybercrime, Law or related fields OR a Bachelor's Degree in the above stated qualifications with over 5 years of experience.
- At least 10 years of professional experience, including digital forensics or cybersecurity strategy.
- Experience working with law enforcement or government cybersecurity programs.
- Proven experience developing institutional or governance frameworks.
- Strong report writing and facilitation skills.
- Experience in Digital Forensics Tools like Cellebrite UFED, Cellebrite Physical Analyser, XRY Software, Block Box Lab XL (RF Forensic box), X-Ways Forensic, etc., would be an added advantage.
- Certificates in Project Management (PMP, PRINCE2, etc.) will be an added advantage

Consultant's Experience: Legal Personnel

The Consultant(s) is required to have the following qualifications:

- A Master's Degree in Law, Cyber Law, International Law, or related legal disciplines **OR** a Bachelor's Degree in the above fields with over 5 years of relevant experience.
- At least 10 years of professional legal experience, preferably with a focus on technology, cybercrime, digital rights, or cybersecurity regulations.
- Demonstrated experience in developing or advising on legal and regulatory frameworks related to cybersecurity, data protection, or digital forensics.
- Experience working with law enforcement, government bodies, or international organizations on cyber-related legal matters.
- Familiarity with legal implications of digital evidence handling, chain of custody, and admissibility in court.
- Strong legal research, analysis, and policy drafting skills.
- Experience in multi-stakeholder legal consultations and facilitation is desirable.

CONTACT:

Further information and the **full TOR** can be obtained from the email addresses below during office hours from **08:00 to 16:00 GMT on Mondays to Thursdays and from 0800 to 12:30 GMT on Friday**. Expressions of interest together with relevant documents must be delivered via email addresses below not later than **16:00 27th August 2025**. Submissions should be in softcopy marked as **Expression of Interest for Institutional Framework Development for the National Digital Forensics Laboratory**.

All interested firms are urged to send their expression of interest letters with attached documents to the following email addresses:

- Sent to the Project Coordinator: slowe@wardip.gm
- Attention to the Project Procurement Specialist: adanso@wardip.gm cc: sdrammeh@mocde.gov.gm / Sanusi_drammeh@yahoo.com

Physical Address of the Project:

Digital Transformation for Africa –

Western Africa Regional Digital Integration Program
C/O Ministry of Communications and Digital Economy
Bertil Harding Highway, Stadium Junction, Bakau, The Gambia, West Africa.
Digital Address (Google Maps): F889+WWH