REQUEST FOR EXPRESSIONS OF INTEREST
(CONSULTING SERVICES – INDIVIDUAL CONSULTANT SELECTION)

Country: Lebanon
Project Name: GFPP for Lebanon Digital Acceleration Project (LDAP)
GFPP Grant No.: **TF0C8895**
Project No.: P181954

Assignment Title: Cybersecurity Legal, Regulatory, and Institutional Framework Assessment and Law Drafting
Reference No.: **LB-OMSAR-537759-CS-INDV**

The Republic of Lebanon represented by the Office of the Minister of State for Administrative Reform (OMSAR) has received a Grant (# TF0C8895**)** from the World Bank's Grant Facility for Project Preparation (GFPP), and intends to apply part of the proceeds of this grant for consulting services.

The consulting services ("the Services") include conducting a comprehensive assessment of Lebanon's cybersecurity legal, regulatory, and institutional landscape to identify gaps, overlaps, and inconsistencies in the current framework, and benchmarking international good practices and adaptable models. The assignment is expected to be completed in approximately **20 weeks** from contract signature.

The detailed Terms of Reference (TOR) for the assignment are attached to this request for expressions of interest – Annex I.

The **Office of the Minister of State for Administrative Reform (OMSAR)** now invites eligible individual consultants ("Consultants") to indicate their interest in providing the Services. Interested Consultants should provide:

1. A curriculum vitae (CV) demonstrating the required qualifications and relevant experience, and
2. A brief Methodology and Work Plan (not exceeding 5 pages) outlining the proposed technical approach and logical sequencing of activities to fulfil the 5-phase scope of work.

Minimum Qualifications and Experience
The Consultant must meet the following minimum requirements:

Education

Advanced degree in Law, Cybersecurity, Public Policy, or related field.

Experience

- Minimum 10-12 years in cybersecurity law, policy, or regulation;
- Proven experience drafting national-level legislation;

- Experience in institutional assessments in public sector contexts; and
- Experience in fragile or developing country environments preferred.

Technical Expertise

- Strong knowledge of:
    - International Organization for Standardization (ISO 27001/27002)
    - National Institute of Standards and Technology (NIST Cybersecurity Framework)
    - Organization for Economic Co-operation and Development (OECD cybersecurity principles)
    - EU cybersecurity directives (e.g., NIS/NIS2)

Language

Fluency in Arabic and English required.

The attention of interested Consultants is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers" (September 2025) ("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest.

An Individual Consultant will be selected in accordance with the **Selection of Individual Consultants** method set out in the Procurement Regulations.

Further information can be obtained at the address below during office hours (09:00 AM to 04:00 PM Beirut Time).

Expressions of interest (including CV and a methodology/work plan not exceeding 5 pages) must be delivered in a written form to the address below (in person, or by mail, or by e-mail) by **COB June 22, 2026**.

Office of the Minister of State for Administrative Reform (OMSAR)
Technical Unit – Preparation Grant for Lebanon Digital Acceleration Project
Attn: Ms. Mirvat Hammoud – Procurement Specialist
Omar Daouk Street, Mina El Hosn Sector,
STARCO Building, Bloc A, 5th Floor, Room 505a
Beirut, Lebanon
Tel: +961 (1) 371 505; ext. 160
E-mail: *mhammoud@omsar.gov.lb*

Annex I

Terms of Reference
PREPARATION GRANT FOR LEBANON DIGITAL ACCELERATION PROJECT (P181954)

Cybersecurity Legal, Regulatory, and Institutional Framework Assessment and Law Drafting

1. BACKGROUND

Lebanon is facing a protracted, multidimensional crisis that has impaired state institutions and public service delivery. Fragmented digital systems, reliance on paper-based processes, and limited trust in electronic transactions continue to hinder efficiency, transparency, and accountability across the public and private sectors. These challenges are compounded by gaps in digital governance, incomplete regulatory activation, and limited institutional capacity to operationalize key digital enablers.

To address these issues, a strategic investment to modernize Lebanon's public sector through digital transformation, stimulate private sector growth, and accelerate the development of a robust digital economy is under preparation with World Bank support. The Lebanon Digital Acceleration Project (the "Project") will establish secure, scalable, and resilient digital infrastructure including cloud services, data platforms, and cybersecurity systems that are essential for attracting investment and fostering innovation. By strengthening digital ID, e-signature capabilities, and the legal framework for digital transactions, the Project will improve the ease of doing business and enable trusted, efficient engagement between the public and private sectors. In parallel, the Project will advance key regulatory reforms in telecom, data protection, cybersecurity, e-signature, artificial intelligence (AI) and other areas, while investing in Lebanon's digital talent pool. Together, these measures will lay the foundation for a more competitive, dynamic, and inclusive economy.

The World Bank's Grant Facility for Project Preparation (GFPP) has been extended to OMSAR to support Project preparation. The GFPP grant will be implemented by a Technical Unit (TU) housed within OMSAR.

An important enabler of secure digital transformation is the establishment of a comprehensive national cybersecurity governance and institutional framework to protect government systems, critical information infrastructure, digital services, and public data against cyber threats and risks. In Lebanon, there are ongoing efforts to establish a coherent national cybersecurity framework, including the development and strengthening of the necessary institutions and institutional arrangements, governance structures, and legal and operational mandates various laws, regulations, institutional mandates and the 2019 National Cybersecurity Strategy partially address aspects of cybersecurity.

In this context, a draft cybersecurity law and framework and accompanying texts and secondary instruments are being developed and circulated among stakeholders; consequently, a coherent consolidation and review to ensure the development of a modern, fit-for-purpose legal and institutional framework aligned with international good practices

and adapted to Lebanon's institutional and operational realities are needed, and hence this proposed assignment.
This assignment should be undertaken in a manner consistent with the applicable national cyber security governance framework and institutional mandates.

2. Assignment and Objectives

This assignment aims to:

- Conduct a comprehensive assessment of Lebanon's cybersecurity legal, regulatory, and institutional landscape;
- Identify gaps, overlaps, and inconsistencies in the current framework;
- Benchmark international good practices and adaptable models;
- Reconstruct and refine the conceptual foundations of a national cybersecurity legal framework, taking into account the current draft law; and
- Develop a comprehensive national Cybersecurity legal and institutional framework, and supporting implementation instruments, for submission to CoM.

3. Core Objectives

- Assess the current cybersecurity legal and regulatory environment;
- Evaluate institutional roles, existing institutional mandates and coordination mechanisms at national level;
- Benchmark international best practices (e.g., EU, NIST, OECD, GCC models);
- Conduct high-level consultations with key stakeholders;
- Review and update as needed the previously circulated draft cybersecurity legal and institutional framework
- Draft a national Cybersecurity Framework as part as the broader legal and institutional review, along with supporting implementing instruments (per description below).
- The above shall be build upon existing national legal and institutional work in the field of cybersecurity.

4. Detailed Scope of Work and Deliverables

Phase 1: Inception and Methodological Alignment

- Confirm understanding of objectives, scope, and constraints;
- Define methodology for legal, regulatory, and institutional assessment;

- Define approach for reviewing, refining and validating elements of the previously circulated draft law and accompanying texts;
- Identify key stakeholders and consultation strategy;
- Develop detailed work plan and timeline.

Deliverable D1: *Inception Report.*

Phase 2: Legal, Regulatory, and Institutional Assessment

- Review all relevant laws, decrees, regulations, and policies (e.g., cybercrime, data protection, telecom, critical infrastructure, defense, digital services) drawing on the previous analyses already undertaken in this area and expanding them where needed (as such the consultant will not duplicate already existing work);
- Map institutional mandates, roles, and overlaps across ministries and agencies, with a focus on existing institutional mandates and coordination mechanisms at the national level;
- Assess existing governance mechanisms for cybersecurity coordination;
- Conduct targeted consultations with key public sector stakeholders;
- Identify institutional strengths, gaps, inconsistencies, and risks;
- Benchmark leading cybersecurity legal and institutional models (e.g., EU NIS2 Directive, US NIST framework, UK NCSC model, UAE/Saudi frameworks);
- Identify adaptable elements for Lebanon (such as governance models, legal provisions, etc.); and
- Define guiding principles for the cybersecurity framework, including:
    - Risk-based approach
    - Proportionality
    - National security considerations
    - Protection of critical infrastructure
    - Public-private collaboration
    - Privacy and human rights alignment
    - Clear institutional roles and accountability

Deliverable D2: *Cybersecurity Baseline Assessment Report and Benchmarking and Design Principles Report.*

Phase 3: Cybersecurity Legal Framework

- Review/refine key elements of the previously circulated draft law based on consultations and available references;
- Define the structure and scope of the cybersecurity legal framework, ensuring coherence with national digital governance frameworks and avoiding duplication or conflict with existing or proposed institutional mandates;
- Draft the Cybersecurity Framework and core implementing texts, including but not limited to:
    - Definitions and scope
    - Institutional roles and mandates, ensuring clear articulation of roles in line with existing governmental competencies.
    - National cybersecurity governance model
    - Critical infrastructure protection
    - Incident reporting and response obligations
    - Risk management requirements
    - Compliance and enforcement mechanisms
    - Public-private cooperation provisions
    - Data protection and privacy considerations
    - International cooperation
- Ensure alignment with Lebanese legal system and constitutional framework; and
- Ensure consistency with existing laws (e.g., Law 81/2018).

Deliverable D3: *Draft National Cybersecurity Framework and core implementing texts.*

Phase 4: Institutional and Implementation Framework

- Define institutional architecture for cybersecurity governance, in alignment with existing national digital governance structures and competencies;
- Clarify roles and responsibilities across entities including accountability, coordination, and reporting lines, while preserving the strategic policy role of relevant national authorities in digital transformation;
- Propose coordination mechanisms (e.g., National Cybersecurity and Information Security Agency (NCISA) and relevant entities), in a manner consistent with existing

and/or proposed legislative frameworks and without creating duplicative or parallel institutional structures;

- Develop high-level implementation roadmap;
- Identify capacity-building and resource requirements to support implementation; and
- Propose secondary regulations and implementation instruments.

Deliverable D4: Draft Institutional and Implementation Framework

Phase 5: Consultation and Finalization

- Conduct validation workshops for draft law and implementation framework with key stakeholders and incorporate feedback; and
- Prepare the final submission package for the Council of Ministers.

Deliverables D5:

- *Final Framework Report*

5. QUALIFICATIONS

Education

Advanced degree in Law, Cybersecurity, Public Policy, or related field.

Experience

- Minimum 10-12 years in cybersecurity law, policy, or regulation;
- Proven experience drafting national-level legislation;
- Experience in institutional assessments in public sector contexts; and
- Experience in fragile or developing country environments preferred.

Technical Expertise

- Strong knowledge of:
    - International Organization for Standardization (ISO 27001/27002)
    - National Institute of Standards and Technology (NIST Cybersecurity Framework)
    - Organization for Economic Co-operation and Development (OECD cybersecurity principles)
    - EU cybersecurity directives (e.g., NIS/NIS2)

Language

Fluency in Arabic and English required.

6. COMPLIANCE REQUIREMENTS

The selected Consultant must adhere to all applicable World Bank regulations and guidelines, including but not limited to the *World Bank's Guidelines on Preventing and Combating Fraud and Corruption in Projects Financed by IBRD Loans and IDA Credits and Grants*, and must disclose any actual or potential Conflict of Interest (COI).
In addition, the Consultant must comply with the following Environmental and Social (E&S) requirements aligned with the World Bank Environmental and Social Framework (ESF) and the Lebanon Digital Acceleration Project (LDAP) commitments:

1- Code of Conduct (CoC)

The Consultant must sign and follow a CoC covering data confidentiality, respectful conduct, non-discrimination, and zero tolerance for SEA/SH.

2- Labor and Working Conditions

The Consultant shall perform the assignment in accordance with applicable labor and working condition requirements under the World Bank Environmental and Social Framework (ESS2), including maintaining safe and healthy working practices, professional conduct, and respect for applicable occupational health and safety standards.
The Consultant shall have access to the Project's Grievance Mechanism for raising any work-related concerns or complaints arising during the assignment.

3- Data Security, Privacy, and Cybersecurity

All data handled under this assignment must be securely stored, accessed only by authorized staff, and managed using privacy-by-design and cybersecurity best practices. Any data breach must be immediately reported.
All data shall comply with applicable Lebanese data protection laws and regulations.

4- Stakeholder Engagement and Grievance Redress

Any targeted technical consultations conducted as part of policy development shall inform participants about the Project's Grievance Mechanism and how complaints can be submitted.

5- SEA/SH Prevention

The Consultant shall comply with zero-tolerance requirements for SEA/SH and adhere to appropriate professional conduct and reporting procedures when engaging with stakeholders, in line with the Project's CoC and World Bank requirements.

6- Environmental Considerations for ICT (ESS3)

Any ICT equipment or data storage devices used must be managed responsibly, including secure data wiping and environmentally sound disposal.

7. DELIVERABLES AND PAYMENT SCHEDULE

The engagement will be completed in approximately twenty weeks (20 weeks) from contract signature date, with key phases and deliverables structured as follows:

Phase	Deliverable	Week of Delivery (from contract signature)	Payment (% of Total)
1	D1 Inception Report	4	10%
2	D2 Cybersecurity Baseline Assessment Report and Benchmarking and Design Principles Report	8	30%
3	D3 Draft Cybersecurity Law and core implementing texts	12	20%
4	D4 Draft Institutional and Implementation Framework	16	20%
5	D5 Final Framework Report	20	20%

8. REPORTING AND GOVERNANCE

Project Oversight and Management Structure

A Technical Committee (TC) will be established to provide strategic direction, oversight, and effective management of the engagement. Chaired by the Grant Coordinator, without prejudice to the roles and prerogatives of participating entities, the TC shall be composed of members from OMSAR, OMSTAI, and other involved ministries and/or relevant public entities, as applicable. The TC will serve as a coordination and oversight mechanism responsible for reviewing the Consultant's progress and facilitating alignment among participating entities, in accordance with the mandates, roles, and decision-making authority for each entity.

Reporting Obligations

The Consultant will report to the Grant Coordinator and provide regular updates to the TC, including all participating entities. In addition to the contractual deliverables, the Consultant, shall participate in progress meetings with the TC team to ensure methodological alignment.

Deliverable Acceptance and Payment Clearance

- Deliverable Review: All deliverables listed in the TOR are subject to review by the World Bank (WB) and the Technical Committee (TC) to ensure methodological alignment and quality, with input from all participating entities.

- Formal Acceptance: A deliverable is considered formally accepted upon written notice (via email or formal letter) from the Grant Coordinator, following review by the WB and the TC.
- Administrative Requirements for Payment: To initiate payment processing, the Consultant shall submit an Invoice Package to the Grant Coordinator, including:
    - The Official Invoice for the specific milestone.
    - A copy of the written acceptance notices from the Grant Coordinator, reflecting TC's validation.
    - Evidence of deliverable submission.

    Nothing in this TOR shall be construed as establishing, modifying, or pre-empting any superseding the legal mandates, roles or decision-making authority of any participating public entity under applicable laws and regulations.

Currency of Payment
Payments will be processed in U.S. Dollars.

9. INTELLECTUAL PROPERTY & CONFIDENTIALITY

Intellectual Property Rights
All documents, data, analyses, policy drafts, tools, and materials produced under this assignment shall become the exclusive property of Government of Lebanon. The Consultant shall not publish, use, or share any materials without prior written approval from the Government of Lebanon.

Confidentiality Obligation
The Consultant shall maintain strict confidentiality of all information accessed during the assignment and shall ensure that no information is shared, disclosed, or used outside the scope of this contract, in accordance with applicable Lebanese laws and regulation.