ANNEX C1bis: Twinning Light Fiche

Project title: Enhanced prevention and response to cyber crime by the Internal Security Forces in Lebanon

Beneficiary administration: Internal Security Forces (ISF) Cyber Crime Bureau in Judicial Police, the Digital Forensic Lab in Judicial Police, and the Technical Branch in IT Information Department.

Twinning Reference: LB 16 ENI JH 01 23 TWL

Publication notice reference: EuropeAid/177425 /DD/ACT/PS

EU funded project

TWINNING TOOL

1. Basic Information

1.1 Programme:

ENI/2016/039-636 SIPPP -Support to the implementation of the EU-Lebanon Partnership Priorities Programme, direct management

1.2 Twinning Sector: **JH – Justice and Home Affairs, Security sector**

1.3 EU funded budget: ***250.000 EUR***

1.4 Sustainable Development Goals (SDGs): **SDG 16 – Peace, Justice and Strong Institution, particularly 16.3 and 16.4**

2. Objectives

2.1 Overall Objective(s): The overall objective is to reinforce Lebanon's response to cyber terrorism and cybercrimes.

2.2 **Specific objective:** The specific objective is to strengthen the capacities of the Internal Security Forces of Lebanon in mitigating cyber threats and combating cybercrime in line with the national cyber security strategy and International standards

2.3 **The elements targeted in strategic documents**

The proposed Twinning action is in line with the EU-Lebanon policy framework, notably:

[EU-Lebanon Association Agreement, 2006[1]]: The AA entered into force in April 2006, which aims to promote economic growth and stability, through the implementation of the "Single Support Framework" for Lebanon. It frames the financial assistance provided by the EU to Lebanon around three intervention areas: i) growth and job creation, ii) local governance and socio-economic development and iii) rule of law and enhancing security.

[EU-Lebanon Partnership Priorities Plus Compact[2]]: The Partnership Priorities (2016 – 2020) provide a strategic framework for political engagement and for coordinating political, security and cooperation efforts. The Partnership Priorities have been extended until adoption of renewed ones, upon which work is currently taking place, in light of the Joint Communication for the Mediterranean and taking into consideration the new context of multiple crises in Lebanon and urgent need for

[1] https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/lebanon_en
[2] https://www.consilium.europa.eu/en/press/press-releases/2016/11/15/eu-lebanon-partnership/

reforms, relevant Council Conclusions, national strategies, ongoing negotiations with the IMF, and Lebanon´s commitments made at the 3RF.

In terms of the Security Sector, the European Union and Lebanon share several common priorities that will shape their cooperation going forward. These include enhancing the rule of law and strengthening the capacity of the Lebanese security forces, promoting a democratic society, and countering terrorism.

The European Union works on various fronts to promote cyber resilience, safeguarding our communication and data and keeping online society and economy secure. EU adopted in 2020 the EU Cybersecurity Strategy. In November 2022 the EU policy on cyber defence, which aims to boost EU cyber capabilities and strengthening coordination and cooperation between the military and civilian cyber communities.

Multi-Annual Indicative Programme European Union – Lebanon 2021-2027: The MIP has been adopted in 2022. The MIP defines a programming vision for EU bilateral programming and has Rule and law and security as one priority.

3. Description

3.1 Background and justification:

Cybercrime has become a global phenomenon that affects individuals and employees in small and large organizations. It is continuously evolving with new trends emerging all the time.

Today Information and communication technologies (ICTs) have a fundamental impact on our society whereby the internet became a necessity in humans' daily lives, a fact that was exacerbated by the COVID pandemic.

The internet is widely used for various purposes such as work, education, entertainment, research, shopping, banking transactions, and others; most importantly, it brings the world together.

Our increased reliance on technology came hand in hand with the increase in the number of criminal activities committed through the use of the net having diverse consequences ranging from the individual loss of privacy, social and professional victimization, to loss of personal funds, to sustained attacks on a country's infrastructure and informational systems. Cybercrime has breached social media networks, thanks to both increased users[3] and increased use.

Hackers look for opportunities to gain access to people's accounts, and personal or financial information, typically through suspicious links or download.

[3]estimated to be around 4.76 billion social media users (i.e 59.4% of the total global population), Global Social Media Statistics

The Lebanon National Cyber Security Strategy released in June 2019 foresaw the establishment of a national cybersecurity agency, but this has yet to happen. In the absence of a national cyber security agency, the government has institutionalised in 2018 a national inter-ministerial Commission created by resolutions/decisions of the Presidency of the Council of Ministers.

In Lebanon, the ISF is responsible for maintaining internal security and stability, including protecting property and individuals and enforcing laws and regulations.

In 2006, the Cybercrime Bureau of the Judicial Police of the Internal Security Forces was established. It has the dual role of investigating complaints, Cyber Security breaches, and technology related crimes under the supervision of the Judicial Authorities, and of providing basic awareness to public and educational institutions on the latest Cyber Threats and Cyber Attacks.

The ISF investigates based on complaints received by citizens or companies crimes committed via the Internet and other computer networks, dealing particularly with Sextortion, Phishing, Ransomware, Crypto-jacking, Online crimes against children, sexual abuse of minors and children for pornographic purposes on the Internet and others.

ISF also assesses and investigates eventual threats and collects information on cyber-crimes via a wide array of public, private, and open sources.

The departments dealing with the prevention and mitigation of crimes committed through cyberspace are the Cyber Crime Bureau in Judicial Police, the Digital Forensic Lab in Judicial Police, and the Technical Branch in Information Department have around 30 dedicated staff members.

As the efforts of these departments are interlinked and taking into consideration the ISF's limited human resources (due to the compounded socio-political issues of the country), this twinning serves to equip relevant departments with the necessary skills and know-how to provide security for its citizens while maximizing ISF ability to perform their intended tasks by improving internal coordination.

Under the Twinning light ISF requested member state support to institutionalize the training in a view to enhance sustainability, to expand the scope to all ISF departments involved in Cybersecurity as well as to complement the capacity with topics that are not covered by other EU funded projects.

Support may as well be complemented by equipment – As per Twinning Rules, the cost of goods are eligible within a ceiling of 20.000 EUR[4].

3.2 **Ongoing reforms:**

[4] See Annex A7: "*In exceptional and duly justified cases, small items of essential supplies (e.g. small laboratory testing consumables or facilities, etc.) can be eligible for reimbursement, within the global ceiling of EUR 20 000 foreseen for the purchase of goods.*" (section 3.8)

At national Lebanese level, the proposed Twinning light has its basis in ISF Strategic Plan (2018-2022), which is perceived as a roadmap for the ISF to become a more responsive, professional and human rights-observant police service. Lebanon lacks a coherent legal framework and strong institutional capacities to prevent and respond to cybercrimes. To improve the situation, in 2018 the Prime Minister nominated a Coordinator on Cybersecurity and a National Committee on Cybersecurity and Cybercrime was established. This Committee drafted the National Strategy on Cyber Security (2019 – 2022) which is the basis of the proposed intervention. Implementation of both strategies has started but is seriously hampered by the economic and governance crisis in Lebanon faced since 2019. The project is equally in line with the priority under the ISF-digitalization strategy.

The suggested Twinning-light project not only coincides with the priority under the ISF-digitalization strategy but also coincides with on-going projects in modernizing and improving ISF capabilities in responding to modern threats through modern means.

3.3 **Linked activities:**

The proposed Twinning complements the other EU funded projects in the sector:

FIAPP ACT for Lebanon security – Advance Counter Terrorism for Lebanon security 2019/413051 (2019 – 2023): The overall objective of this programme is to reinforce national capacities in Lebanon to react to the threats of terrorism and organized crime while promoting rule of law and human rights in line with International standards. More specifically, strengthening the regulatory framework and national cyber security response against terrorism. Specific trainings have taken place for all stakeholders involved in cybersecurity, including security agencies, to strengthen cooperation and collaboration on investigation and response. Trainings focused on cyber risk assessment, crisis management and incident response and digital forensic investigation.

FIIAPP – Promoting community policing 2020/420605 (2020 – 2024): This project aims at promoting community policing and transparency, including development of new IT solutions for ISF.

CyberSouth – Cooperation on cybercrime in the Southern Neighbourhood Region (Regional Project 2017 – 2023): This regional programme contributed to the prevention and control of cybercrime and other offences involving electronic evidence, in line with international human rights and rule of law standards and good practices.

Project objectives pertained to strengthening legislation and institutional capacities on cybercrime and electronic evidence in the region of the Southern Neighbourhood in line with human rights and rule of law requirements.

CT Inflow and EUROMED Police (Regional Project 2021 – 2027): implemented by CEPOL aim at creating a regional response to CT and organized crime and have

cybersecurity as one topic. This project contributes to enhance the institutional capacity to protect EU neighbours' citizens against transnational serious and organized crime (SOC). It strengthens the operational capacities of the South Partner Countries (SPC) to fight serious and organized crime and reinforces strategic cooperation between national law enforcement authorities in SPC, as well as between SPC and EU.

3.4 **List of applicable *Union acquis*/standards:**

Not applicable

3.5 Components and results per component:

This Twinning Light project aims at providing support to strengthen the institutional and technical capacities of the ISF departments in charge of cyber security and IT security in line with EU best practices. More specifically, the Twinning Light is intended to enhance the institutional capacity of the ISF to detect, prevent, mitigate and recover from cyber-attacks at the (inter)national level.

R1: Institutional capacity of the ISF and its staff improved to fight cybercrimes at international and national level.

R2: ISF capacity and capability strengthened to prevent and respond to cyber incidents

This project will through the exchange of experiences and best practices between Lebanon and an EU member state contribute to the enhanced response of the ISF to cybercrimes. Envisaged is an enhanced cooperation with other cybersecurity stakeholders, judiciary as well as IT departments as well as international cooperation with law enforcement agencies.

Therefore, the projects aims at:

- firstly sharing experiences to understand and compare the system in place at a EU MS and Lebanon – law enforcement component

- initiate a thorough and sustainable cooperation with selected EU MS, starting with a study visit to the peer administration, to get practical understanding of the system and the applied procedures

- a series of workshops to exchange experience with an EU Member State that has developed a well established system of prevention and response to cybercrime - a series of workshops and mentoring sessions to strengthen the capacity of the relevant ISF departments with an EU Member State on selected topics on prevention and response to cybercrimes including the development of a training catalogue for the relevant departments

- organization of a round table for the development of a roadmap to enhance the capacity including concrete recommendations for implementation in the current situation

3.6 Expected activities:

R1: Institutional capacity of the ISF and its staff improved to fight cybercrimes at international and national level.

Activities corresponding to Result 1:

Activity 1.1: Organize study visit for selected ISF-staff to a designated EU Member State, to study the institutional set up of relevant departments including training of a peer police institution in the prevention and response to cybercrimes

Activity 1.2: Convene a series of workshops and roundtables in Lebanon to discuss the status quo of prevention and response to cyber criminality within the ISF and the way forward. This shall include national and international cooperation as well as internal ISF administration such as human resources and technical as well as budgetary and equipment requirements for the proper, transparent and efficient functioning of the ISF.

Activity 1.3: Develop a comprehensive analytical report on the series of workshop and a draft a roadmap with concrete and feasible recommendations in a view to enhance the capacities of ISF

Activity 1.4: Organization of a round table to discuss and endorse the recommendations for improvement of the ISF defence, security measures and capability in handling cyber incidents.

R2: ISF capacity and capability strengthened to prevent and respond to cyber incidents

Activities corresponding to Result 2:

Activity 2.1: Organization of a round table to discuss training requirements in view of the subsequent workshops.

Activity 2.2: Creation of a training plan that would encompasses the essential and needed activities to accomplish the objectives set out of this Twinning Light Project.

Activity 2.3: Organization of a series of workshops in order to enhance the ISF capacity to prevent and address cybercrimes and cyber threats[5]

Topics shall include but not be limited to:

- Methodology of public private cooperation and digital evidence from foreign service providers and international social media platforms (Facebook, Instagram) including the necessary procedural, legal requirements; as well as the means of communication, and forms/templates to be used.
- Online investigations in social media offenses (means to address social engineering attacks), including password theft, website/social media account hacking.
- Open source intelligence tools in online investigations.
- Data recovery;
- Vehicle, video (comparison, manipulation), network forensics (Netflow, packet forensics, flow analysis), mobile forensics, digital and computer forensics;
- Reporting of results and analysis to Judiciary.
- Cyber incident handling and response, as well as threat hunting, and threat intelligence, including analysing security events and logs (Network, Endpoint) to determine Indicator of compromises IOCs through a SIEM (Security incident and event management) solution and/or malware analysis and reverse engineering.

Activity 2.4: Organize specific mentoring sessions after each training session/workshop to provide hands-on training and share professional experience

Activity 2.5: Elaboration of training modules and full documentation of the capacity building activities in view of the development of a training catalogue on prevention and response of cyber-crimes

3.7 Means/input from the EU Member State Partner Administration:

3.7.1 Profile and tasks of the PL:

The Project Leader from the Member State must be a public servant of a Member State administration or equivalent staff, but preferably in a leading position in a law enforcement agency specialized in cybersecurity. The MS Project Leader will manage the implementation of the project with the Project Leader from the Beneficiary Country.

The Project Leader's will ensure his/her ability to mobilise the necessary staff in support of the efficient implementation of the project. In addition, he/she should coordinate, on the Member State side.

The MS Project Leader will continue to work at his/her Member State administration but will devote some of his/her time to conceive, supervise and coordinate the overall thrust of the Twinning Project, and ensure the attainment of the projected outputs. The Project Leader is fully responsible for the fine tuning of the Twinning light and the coordination of the work of the experts.

As a minimum, the project Leader should be able to dedicate to the project at least 3 days per month, with at least 5 on-site visits. He/she will be supported by his/her Member State administration for logistic, accounting and administrative affairs.

Profile:

He/she should have the following:

- University degree: Business or public administration, economics, computer Science or related field ,or equivalent professional experience of (6) years in a member state police/cybercrime department;
- At least 3 years of working experienced in a member state police department with focus on Cyber Security and cybercrime
- Project management experience: managing or assisting in management in at least 1 EU funded projects (preferably twinning) would be considered as an asset;
- Working experience with European Union institutions in cybersecurity including CEPOL desirable
- Excellent working knowledge of written and spoken English.

Tasks:

- Conceive, supervise and coordinate the overall thrust of the project;
- Ensure that projected outputs are reached;
- Co-manage the implementation of the project with the Beneficiary Country Project Leader;
- Co-ordinate MS experts' work and availability;
- Establish and maintain cooperation with all beneficiaries involved in the implementation of the project and other related projects (ensuring the avoidance of overlapping), in close coordination with the Project Leader;
- Ensure the backstopping functions and financial management;
- Organise in coordination with Component Leader study visits for relevant institutions for exchanging knowledge, comparative experience and best practice with the peers in EU Member States;
- Preparation and drafting of interim, and final report in accordance with the Twinning Manual and project reporting;

- Ensuring timely, effective and efficient implementation of the project and achievement of results, through proposed activities.

3.7.2 Profile and tasks of Component Leader*:*

One component leader is foreseen to assist the Project leader in the technical design of the project..

Profile Component Leader

- Business or public administration, Human Ressource development, Computer Science or equivalent professional experience of (5) years in a member state police/cybercrime department;
- At least 3 working experience in working with the member state police in a relevant department for cybersecurity or related department
- At least 3 years working experience with a member state police in a relevant department for training and capacity building - Excellent English skills (oral and written)
- Excellent computer skills.

Tasks of Component Leader

- Communicate with the beneficiary counterparts regarding the reaching of the expected Results.
- Organize the study visit to the member state
- Exchange best practices and institutional development standards to prevent and respond to cybercrimes and develop a series of workshops to exchange best practices on institutional requirements
- Elaborate together with the ISF counterpart recommendations and a roadmap
-Elaborate with the national counterpart a training concept for enhanced capacity of the Irrelevant ISF departments
- Organize and facilitate workshops and trainings on selected topics to enhance the capacity to prevent and respond to cyber threats and cybercrimes

Elaborate a training catalogue for ISF

- Presentation of the elaborated documents in a final event

3.7.3. Profile and tasks of other short-term experts*:*

Other specialist staff can be made available by the Twinning Partner to support the implementation of activities. The proposed pool of short-term experts is expected to cover all relevant areas targeted under this project and should be identified by the Project Leader in the course of defining the operational side letters (OPS).

Short-term experts are officials or assimilated agents of a Member State public administration, or mandated body. The experts made available for the implementation of a Twinning project shall therefore be fully integrated within the Member State institutions involved in the delivery of the required expertise.

The short term experts will work in close cooperation with the PL and the Beneficiary in order to meet the specific objectives as set out above.

Terms of reference for short-term expert(s) will be elaborated by Project Leader and the beneficiary counterpart at the work plan preparation stage.

The short and medium-term experts are expected:

- To have university degree in a relevant subject or (10) years of equivalent professional experience
- A minimum of 3 years of professional experience in the area relevant to the proposed assignment
- Very good communication skills and experience in intercultural exchanges
- Fluency in English (oral and written), French is an asset
- Excellent computer skills.

Tasks of the Short-Term experts:

- Prepare and implement specific tasks based mainly on practical cases and experience in compliance with their mission definition and in accordance with project activities;
- Provide practical advices to relevant staff for execution of different tasks related to the Project;
- Address crosscutting issues;
- Prepare mission reports.

Main areas of expertise required by the team of short-term experts should cover the following fields (the list of fields is not exhaustive):

- Cyber-crime
- Forensic accounting techniques
- Financial crime on internet and crypto-currencies
- Experiences in Asset Recovery Offices
- Capacity building
- Strategic planning
- Legal aspects related to cyber - crime and fight organised crime

4. Budget

Maximum budget available for the Grant: 250.000 EUR

5. Implementation Arrangements

5.1 The Delegation of the European Union to Lebanon will be responsible for tendering, contracting and accounting.

Contact person:

Ingeborg Zorn

Programme Manager Security and Human Rights

European Union Delegation to Lebanon

Ingeborg.Zorn@eeas.europa.eu

5.2 Institutional framework

Lebanon's Internal Security Force (ISF), more specifically with the role of preserving order and security in Lebanon, will be the main beneficiary of the present Twinning Project. The results indicated above will lead to an enhanced capacity of said department in fulfilling its role and sustaining the improvement this Twinning will contribute to enhancing the institutional capacity of the abovementioned beneficiary in fighting cybercrimes and mitigate cyber threats, as well as its capacity to investigate said crimes online.

5.3 Counterparts in the Beneficiary administration:

5.3.1 Contact person:

Colonel Ali Skaine

Head of the IT Department

ali.skaine@hotmail.com

Internal Security Force

Beirut, Sodeco

Republic of Lebanon

5.3.2 PL counterpart

Specify the name, official position and postal address of its institution, (no contact details of the person)

Colonel Ali Skaine

Head of the IT Department

ali.skaine@hotmail.com

Internal Security Force

Beirut, Sodeco

Republic of Lebanon

And;

<u>IT Director – Information Department, Head of Cyber Security Committee</u>

Colonel Khaled Youssef

Internal Security Force

Beirut, Sodeco

Republic of Lebanon

6. **Duration of the project**

8 months.

7. Sustainability

Cyber space and technology is ever changing. Technology and the knowledge on these can easily become obsolete if not properly managed and updated. By supporting the Lebanese Internal Security Force in comprehensively and technically building the capacity to handling, prevent, and/or mitigating cyber threats at the institutional, we are indisputably allowing the abovementioned beneficiary to sustain its effort and minimize the risk of becoming obsolete in the field of cyber security and cybercrime investigations.

Twinning will contribute to enhancing the institutional capacity of the abovementioned beneficiary in fighting cybercrimes and mitigate cyber threats, as well as its capacity to investigate said crimes online. These involves (but not limited to) training on investigating crimes in cyber space and training on how to detect online fraud. Furthermore, it includes training on how to handle a cyber-attack if these should occur, in which damage control will be essential.

The abovementioned activities creates an equilibrium between the theoretical information and the practical knowledge on how to keep Lebanon safe – digitally. In terms of sustainability, we added the necessity for the conducting of an assessment related to human resource and technical needs as well as legislative and institutional capacity of ISF with regards to cybercrimes and draw recommendations for improvement in line with EU best practices. This is crucial as it may allow for the precedence for reforms that would enhance the cooperation between the ISF and the judiciary, which is crucial in order to maximize on the benefits from the lessons learned from the activities of this Twinning

8. Crosscutting issues *(equal opportunity, environment, climate etc…)*

The principles of equal opportunities will be respected and environmental and gender issues will be taken in consideration where necessary. The project will be implemented

in a way to avoid discrimination based on the grounds of the ethnic origin, religion or race.

9. Conditionality and sequencing

There are no special conditions that need to be met in order for the Twinning project to start being implemented.

10. Indicators for performance measurement

The specific, realistic, verifiable indicators for performance measurement are listed in the Logical Framework Matrix included in the annex 1.They are summarized as follows:

For result 1:

- The number of workshops organized on request of of information and digital evidence – minimum 2.
- Number of ISF-staff trained increased by minimum 10%
- Number of staff participating to study visit minimum 5 staff.
- A Guideline on reporting digital forensic analysis results formulated.
- A Assessment carried and needs identified.
- A list of workshops/trainings to be delivered based on priorities prepared.

For result 2:

- Number of staff trained by minimum 20%
- Minimum 2 of Training(s)/workshop(s) on Data recovery, Digital Forensic Lab Management, malware analysis and reverse engineering, vehicle forensics, voice, photo, and video forensics and network forensics. Also, open source intelligence tools delivered, as well as investigation techniques for social media carried.
- An analytical report on the series of workshop and a draft a roadmap with concrete and feasible recommendations in a view to enhance the capacities of ISF.

These measures are solely indicative at this present moment – and can be subjugated to change under the discretion of the appointed experts.

General Objective: to reinforce Lebanon’s response to cyber terrorism and cyber crimes.

Indicators:

1. **Country score in the ITU Global Cyber-security Index**

Specific Objective(s): to strengthen the capacities of the Internal Security Forces of Lebanon in mitigating cyber threats and combating cybercrime in line with the national cyber security strategy and International standards

Indicators:

Reduction in cybercrime incidents

Increase in the number of cybercrime investigations

Number of ISF officers trained in cybercrime prevention and investigation who show increased knowledge in the subject

11. Facilities available

Office accommodation, roundtable and workshop facilities will be provided by the beneficiary.

ANNEXES TO PROJECT FICHE

1. Logical framework matrix Annex C1b