Twinning Project Fiche

Strengthening the capacity of the public administrations to combat cybercrime in the Hashemite Kingdom of Jordan.

TABLE OF CONTENT

LIST OF USEFUL ABBREVIATIONS	
AA	Association Agreement
AP	Action Plan
BC	Beneficiary Country
CID	Criminal Investigation Department of the Jordan Police
DG	Directorate General
EC	European Commission
ENPI	European Neighbourhood Policy Instrument
EUD	European Union Delegation to Jordan
EU MS	European Union Member State
FLD	Forensic Laboratories Department
GoJ	Government of Jordan
IT	Information Technology
MoJ	Ministry of Justice
NCP	National Contact Point
OVI	Objectively Verifiable Indicator
PAO	Programme Administration Office
PM	Prime Minister
PSD	Public Security Department
RTA	Resident Twinning Advisor
STE	Short Term Expert
SWOT	Strengths & Weaknesses, Opportunities & Threats (analysis)
TNA	Training Needs Assessment
ToT	Training of Trainers
USAID	USA bi-lateral aid program
UN	United Nations
UNDP	United Nations Development Program
VET	Vocation and Educational Training
WB	World Bank

STANDARD TWINNING PROJECT FICHE

1. BASIC INFORMATION

1.1 Programme: Support to the Implementation of the Action Plan Program (SAPP II)
Cris Nr: 2009/020-478

1.2 Twinning Number: JO/13/ENP/JH/22

1.3 Title: Strengthening the capacity of the public administrations to combat cybercrime in the Hashemite Kingdom of Jordan.

1.4 Sector: Justice and Home Affairs

1.5 Beneficiary Country: The Hashemite Kingdom of Jordan

2. OBJECTIVES

2.1. Overall Objective

To improve the capacity to fight internet crime in Jordan, according to the Jordan Law and in line with the relevant EU standards and international best practices.

2.2. Project Purpose

To improve the ability of the Public Security Department -Criminal Investigation Department of the Jordan Police (PSD-CID) in implementing investigations on cybercrime cases and, in so doing, to improve the level of cooperation with its partners institutions at both National and International levels in order to combat cybercrime through the exchange of information, best practices and experience.

2.3. Contribution to National Development Plan/ Cooperation Agreement/ Association Agreement/ Action Plan

In 2002 the EU and Jordan signed the first Support to the **Association Agreement** Programme (SAAP). The agreement aimed at upgrading the Jordanian administration's institutional capacities so it could deal with all aspects of the Association Agreement. A second support programme to the Association Agreement was concluded in 2005. The newer central element of the ENP is the bilateral **ENP Action Plans** agreed between the EU and each partner. The EU-Jordan ENP Action Plan **(AP)** was adopted in 2005, and has been implemented over a 5 year period. The AP defined a set of priorities covering a number of key areas for specific action, the implementation of which would facilitate the fulfilment of the provisions of EU-Jordan Association Agreement and consequently the Barcelona Process. The 6 priorities of the AP are: enhancing political dialogue and reform; economic and social reform and development; trade related issues, market and regulatory reform; **cooperation in justice and home affairs**; transport, energy, information society and environments, and people to people contacts, including education.

In November 2008, Jordan requested for advancing relations with the EU, with the aim of bringing Jordan closer to the EU by reinforcing the current Partnership and creating new avenues of cooperation in areas of mutual interest. The request was officially submitted to the Seventh Association Committee meeting held in Brussels in June 2009, which included the Government's views on how to enhance

bilateral relations in the political, economic, trade, and social spheres, as well as deepen cooperation in key sectors such as energy, water, transport, agriculture, and science and **technology**. The EU approved Jordan's advanced status Action Plan in November 2010.
Under chapter 17 of the EU-Jordan Action Plan (AP), Jordan and the European Union agreed to *Fight Against Organised Crime*. For this purpose both parties will engage in a dialogue with a view to accede to the Council of Europe Convention on Cyber-Crime and its Additional Protocol. Moreover, they will exchange of information and best practices in the fight against cybercrime.

3. DESCRIPTION

3.1. Background and Justification

The Jordanian society, like many others around the world, are increasingly relying on Information and Communication Technology (ICT) and are thus increasingly vulnerable to threats using information and communication technologies for criminal practices or in the other words cybercrime practices. Threats include attacks against the confidentiality, integrity and availability of computer data and systems, including different types of malware (viruses, trojans and worms), botnets and denial of service attacks, phishing and other types of identity theft, computer-related forgery and fraud, child pornography, hate speech and infringements of copyright and related rights. Cybercrime is probably the most transnational of all forms of crime thus requiring extensive and efficient international cooperation. Cybercrime is increasingly organized and aimed at generating criminal proceeds. Links between organized crime and cybercrime include:

- ICT facilitate offences by organized criminal groups and networks, in particular; economic crime;
- ICT create vulnerabilities at all levels of society and the economy that are exploited by criminal groups;
- ICT facilitate logistics, anonymity and reduce risks of criminal groups;
- ICT are used for money laundering;
- ICT facilitate global outreach of criminal groups;
- ICT shape criminal groups that increasingly take the shape of networks.

Another risk is the terrorist use of the internet and threats against ICT. This may take the form of denial of service attacks against critical infrastructure, recruitment, training or propaganda for terrorism, financing of terrorism or the use of ICT by terrorist groups for logistical purposes. Measures against organized and economic crime and other forms of serious crime, including terrorism, therefore need to include measures against cybercrime.

The protection and safety of people and their property are the most important duties of the Public Security Directorate, resulting in law enforcement activities in cases where the safety of people or their properties has been infringed. Electronic services are very common in Jordan and growing both in size and quality and are used nowadays by a majority of citizens in Jordan. Crime is, depending on the community reality, in all countries as well as in Jordan continuously evolving and as a result crime will also hit digital information services. The number of cyber-crimes in Jordan is increasing and therefore Jordan intensified its efforts to fight cyber-crimes and approved the first cybercrime law in 2009.

In response to the increasing of cybercrime offenses in Jordan, the Public Security Directorate established the Anti-cybercrimes unit within the Criminal Investigation Department in 2008 to enforce national legislation on cyber-crimes and by conducting technical investigations on cyber-crimes. The

unit is supported by communications, digital evidence and laboratory sub-divisions to extract and analyze the digital evidence. The unit currently employs (31) officers and investigated (589) cyber-crime cases in 2011, including identity, email, electronic data and website thefts, electronic threats, phishing, electronic fraud and ATM skimming. A detailed statistical table is shown below.

Cybercrime type	**2008**	**2009**	**2010**	**2011**	**2012**
Impersonate	7	43	35	150	49
Electronic Defamation and extortion	14	77	176	114	125
Electronic financial fraud	9	37	24	20	17
mail Theft	0	28	25	40	18
Theft of electronic data (master servers, images ...)	3	14	15	3	5
Penetration sites	1	2	21	11	31
Abuse of children	0	1	1	2	3
Communication issues (threat, discomfort)	112	348	185	251	185
Total	**146**	**550**	**482**	**589**	**433**

In 2010, the government passed a provisional Information Systems Cybercrimes Law to address important issues of electronic crimes like hacking or illegally obtaining information for financial transactions, however, the law included also a number provisions that perceived as a hinder to expression. Ultimately, the law was not passed and the Anti-cybercrimes division is authorized to practice its authorities based on technical measures in penal law.

In 2011 the Criminal Investigation Department (CID) established a new forensic lab with (35) technicians handling digital forensic analysis. The Forensic Laboratories Department (FLD), established on 1 January 1965, general duties include training courses in the fields of forensic labs and physical and digital evidence, using small forensic digital labs practicing cyber-crime analysis, and other labs not related to cyber-crime. FLD has (9) qualified technicians to manage cyber-crime projects.

Due to the global nature of information networks, there is an ever-growing vulnerability to cyber-crime. To tackle this threat, traditional mutual assistance and operational law enforcement cooperation proves often ineffective and inadequate. The objective of this twinning project is to implement applied European best practices in this field in different Member States and perspectives for an effective Europe-wide campaign against cyber-crime.

3.2. Linked Activities

- **Twinning Project Fiche - Strengthening the Public Security Directorate in the Fight against Terrorism and Organized Crime.**
  In 2007 Jordan has implemented the project “Strengthening the Public Security Directorate in the Fight against Terrorism and Organized Crime” in order to strengthen the capacity of the PSD - namely the Forensic Laboratories Department FLD and the explosives section in the Preventive Security Department- to fight terrorism and organized crimes in line with EU and international standards and best practices.

- **Twinning Project Fiche - Institutional Strengthening for the Telecommunications Regulatory Commission in Jordan**

The aim of this ongoing twinning contract is to support the Telecommunications Regulatory Commission (TRC) in developing its regulatory framework, and operational capacities to be in line with the international standards and EU best practices.

– **TAIEX Expert Mission on Combating Cybercrimes - Amman, Jordan 21 to 23 march 2011**
The assistance aimed at providing the Cybercrime Unit within the Crime Investigation Department with expertise in the techniques of cybercrime detection and investigation. It focused on the necessary tools and equipment to perform effective investigations on Cybercrimes.

3.3. Results

Three mandatory results will be achieved by the Twinning Partners. In order to achieve these three results a series of activities have to been implemented. They are grouped in three components. Each component is dedicated to the achievement of one result.

Result 1. The capacity of the CID officers in charge of managing investigations on cybercrime cases is strengthened through better knowledge of the new technologies, the adequate use of the instruments and tools of cyber investigation and to prepare accurate reports in particular in the fields of credit card fraud, intrusion attacks and child sexual abuse online.

Result 2. Improved level of co-operation between CID- division of cybercrimes - and other relevant institutions at both the national level (Ministry of Justice, Laboratories and Crime Evidence Department, Family Protection Department within the PSD) and the international level in implementing co-ordinated actions in the fight against cybercrime.

Result 3. Raised public awareness on the methods and dangers of cyber crime, in particular amongst the young population, families, banks and private companies, and educational sector, including the main measures to combat and prevent them.

3.4. Activities

The Twinning Project will undertake the following activities[1]:

Activity 0.1 Kick-off meeting

The implementation of the project will start with the arrival of the Resident Twinning Adviser (RTA) in Jordan. The RTA will have to be placed in his/her office. S/he will be introduced to the BC stakeholders of the project and to his/her counterparts and staff. S/he will finalise the hiring of the project assistant.

A one-day kick-off meeting will be organized in the first month of the project, aiming at launching and presenting the project to the stakeholders, the media and the public at large. In order to guarantee large public information and visibility about the start of the project, the meeting will be concluded with a press conference and a press release.
Benchmarks: Stakeholders, media and public informed about the start and content of the project by start of month 2.

Activity 0.2 Steering Committee meetings

[1] Note: The listed activities and the proposed means for achieving the results are indicative and can be revised in the framework of the preparation of the contract between twinned institutions.

On a quarterly basis, regular Steering Committee meetings will be held to promote the effective management and monitoring of project activities. Progress in the areas of the project's interventions will be discussed with the beneficiaries and Steering Committee members.

Activity 0.3 Closing conference

A closing conference (wrap-up meeting) will be held during the last months of the project at which the results and impact of the project will be presented to the beneficiary, the Jordanian Government, the civil society and other donors. The conference will present recommendations for possible follow-up and lessons learned for and from similar projects.

Benchmarks: Closing conference organized. Recommendations and lessons learned formulated and discussed. Stakeholders, media and public informed about the results of the project at its end.

3.4.1 Component I[2]:

Activities connected to result 1: The capacity of the CID officers in charge of managing investigations on cybercrime cases is strengthened through better knowledge of the new technologies, the adequate use of the instruments and tools of cyber investigation and to prepare accurate reports in particular in the fields of credit card fraud, intrusion attacks and child sexual abuse online.

.

Activity 1.1: Assessing the capacities and training needs of CID staff/divisions in charge of cybercrime cases investigation

Tasks:

1.1.1 Development of a detailed capacity building and training needs assessment focused on CID staff/division in charge to be prepared commonly by the MS and BC experts (the relevant target divisions of the assessment are: Intellectual property division, cybercrime division, Investigation division).

1.1.2 Support to set up of training plan (including specific curricula) targeted to each of the CID staff/divisions' needs. In particular the areas of credit card fraud, intrusion attacks and child sexual abuse online, should be tackled.

1.1.3 Conducting an analyses on the needs of hardware and software to improve the capacities of the CID to combat cybercrime providing recommendations on the best software to be adopted (this action should be done in close cooperation with Ministry of Planning and international cooperation).

1.1.4 Support to set up of a first draft of the Needs and Training assessment report.

1.1.5 Organization and Implementation of at least two seminars involving senior officials/directors in order to agree with them the results of the needs assessment and in sharing with them the introduced MS best practices and know-how on ITC tools' management, management of cyber investigations, reporting.

1.1.6 Development of the final draft of Assessment report containing the comments and the indications collected during the seminars as for task 1.1.4.

Benchmark: A detailed capacity building and training needs assessment report developed and shared within CID

[2] All required printing needs will have to be paid for by either the EUMS or the beneficiary country as agreed during the negotiation of the contract.

Activity 1.2: Study visit to MS country/ies involving PSD decision makers

Tasks:

1.2.1 Organisation and implementation of a familiarization trip to MS Twinning country involving the senior officials/directors of the target divisions within the PSD (three persons having the role of decision makers for relevant issues concerning cybercrime) in order to share with them the methods of work adopted by the MS twinning institution(s) in the field of fighting cybercrime, presenting the EU Acquis, the MS best practices and the used instruments and tools, and to discuss any possible future initiative of cooperation with European networks of related institutions.

Benchmarks: Three PSD decision makers for relevant issues concerning cybercrime implementing the trip to MS twinning country/ies and receiving detailed information on the methods of work adopted by the MS twinning institution(s) in the field of fighting cybercrime, presenting the EU Acquis, the MS best practices and the used instruments and tools.

Activity 1.3: Training of CID officers in charge of methods and instruments for fighting cybercrime

Tasks:

1.3.1 Identification and selection of the persons within CID staff to be trained within the relevant divisions (Intellectual property division, cybercrime division, Investigation division).

1.3.2 Execution of the training courses for CID staff, to be indicatively implemented in three levels (according to needs): beginners, intermediate, advanced (indicative number of persons to be trained: 60 persons).

1.3.3 Support to set up of a practical manual containing the training material.

Benchmarks: At least 60 BC policemen working within the CID- cybercrimes division trained on how (at least) to manage ITC tools' to fight cybercrime, how to implement actions of cyber investigations, how to prepare adequate reports.

Activity 1.4: Setting up and implementation of a training of trainers- program ensuring the sustainability of the introduced best practices within the PSD

Tasks:

1.4.1 Assisting to set up a ToT plan and detailed curricula according to the different targets of training within the PSD.

1.4.2 Identification of trainers within the three relevant divisions of CID (Intellectual property division, cybercrime division, Investigation division) on the base of the group of trainees attending the advanced level course as for 1.3.2 (indicative number of selected trainers: 15 persons).

1.4.3 Implementation of the ToT program according to the identified plan and targets within PSD.

Benchmarks: At least 15 CID policemen trained according to the developed ToT plan for PSD; a practical manual for ToT developed; at least two pilot training coursed implemented and evaluated by project MS experts.

Activity 1.5: Study visit for CID policemen in MS country/ies focused on technical methods and sharing best practices management issues as adopted in the EU MS

Tasks:

1.5.1 Organisation and implementation of a plan of 4 study visits involving 5 participants from Criminal Investigation Department workers staying 6 nights each in the MS country/ies sharing best practices on actions against cybercrime.

Benchmarks: Study visit implemented, 20 CID experts trained and best practice shared with them.

3.4.2 Component II[3]:

Activities connected to result 2: Improved level of cooperation between CID- division of cybercrimes and other relevant institutions at both the national level (Ministry of Justice, Laboratories and Crime Evidence Department, Family Protection Department within the PSD) and international level in implementing coordinated actions of fight against cybercrime.

Activity 2.1: Improve the cooperation between the CID and the MoJ

Tasks:

2.1.1 Organisation and implementation of a two-days Forum of discussion involving MoJ (senior officials and Judges) and PSD/CID senior officials in order to assess the needs of the Judges in terms of better understanding the ITC instruments and tools used by cybercrime and identification for initiatives to enhance the level of cooperation between the PSD and MoJ in cybercrime issues.

2.1.2 Implementation of at least three seminars of three days each involving MoJ judges with PSD policemen from CID, Laboratories and Family protection divisions, in order to enhance the level of know-how on cybercrime cases, in terms of technology used and understanding of the mechanisms.

2.1.3 Implementation of two (one-day) discussion meetings with Judges and PSD-CID in order to facilitate discussions on possible changes in methods of cybercrime investigation and to examine possibilities for future initiatives of cooperation including the identification of pilot actions to apply and to evaluate the new methods.

2.1.4 Support to set up a document containing recommendations for new methods and best practices for enhancing the cooperation between MoJ and PSD-CID in cybercrime actions as identified in the meetings and workshops.

Benchmarks: Meetings implemented, document containing recommendations on new methods identified and a plan for future pilot actions of cooperation between MoJ and PSD-CID agreed among the partners.

Activity 2.2: promoting the cooperation with ITC telecommunication companies on cybercrime

Tasks:

[3] All required printing needs will have to be paid for by either the EUMS or the beneficiary country as agreed during the negotiation of the contract.

2.2.1 Implementation of technical meetings involving ITC and telecommunication companies' representatives with PSD-CID to share and collect technical information and to enhance the mechanisms of cooperation among them in order to better implement the task of cybercrime investigations.

2.2.2 Identification of concrete methods and instruments for better cooperation between telecommunication stakeholders with PSD-CID and ITC divisions in order to increase the capacity of these departments to deal with cybercrime issues.

2.2.3 Identification and implementation of at least one pilot action (to be defined during the meetings of coordination) in which the level of enhanced cooperation between PSD and the relevant companies will be monitored and evaluated.

Benchmark: At least one pilot action (to be defined during the meetings of coordination) of joint cooperation between ITC and telecommunication companies with PSD-CID.

Activity 2.3: Enhancing the capacity of PSD-CID to cooperate at the international level in actions to prevent and to combat cybercrime

Tasks:

2.3.1 Implementation of technical workshops with MS experts focused on informing the CID staff on the main networks established at international level aimed to promote coordinated actions to prevent and combat cybercrime and to show the experience of the related MS with counterparts in Europe.

2.3.2 Implementation of a conference to promote cooperation to fight against cybercrime, involving all relevant government institutions in Jordan and representatives of the international networks (INTERPOL, EUROPOL etc.)[4]; the purpose of this conference is to enhance the process of criminal investigation on fight against cybercrime by facilitating the discussions on possible changes, to exchange required information, to show the experience and structures of other countries and of coordinated actions at international level.

2.3.3 Support to prepare a preliminary assessment of the possibility of Jordan ratifying the Budapest Convention

Benchmark: Increased know how and skills of CID staff to accede international networks of institutions combating cybercrime and to manage coordinated actions such as investigations and exchange of information on international cases.

3.4.3 Component III[5]:

Activities connected to result 3: Raised public awareness on the methods and dangers of cyper crime, in particular amongst the young population, families, banks and private companies, and educational sector, including the main measures to combat and prevent them.

Activity 3.1: Capacity building to PSD/CID to identify and implement actions of raising the Awareness on cybercrime focused on relevant stakeholders

[4] Representatives of international networks cannot receive fees and produce Project Management cost.

[5] All required printing needs will have to be paid for by either the EUMS or the beneficiary country as agreed during the negotiation of the contract.

Tasks:

3.1.1 Implementation of a program of training sessions targeted to CID staff, aimed to enhance their capacities to promote and to implement actions of awareness and coordination focused to general public and relevant stakeholders in the field of cybercrime prevention (the topics of the seminars should contain at least: communication and awareness, media and public relations, techniques and methods of coordination with stakeholders and enhancing public participation).

3.1.2 Support the development of a practical manual targeted to PSD-CID containing the material developed for the training sessions, the introduced methods of communications, relations and stakeholders' coordination, best practices and practical case studies from MS counterpart(s).

3.1.3 Implementation of workshops with PSD-CID and IT staff with civil society organisations (NGOs, private universities, Jordan branches of international organisations for family and children protection, and so on) to increase their level of awareness on cybercrime, to inform about practical cases of actions against cybercrime and to promote initiatives of coordination and cooperation in this field; meetings will be attended by MS experts in order to provide follow up and technical support in implementing the method of coordination.

3.1.4 Implementation of workshops with PSD-CID with other relevant governmental institutions (Ministry of Education, public universities, Ministry of communications) to raise their level of awareness on cybercrime and to promote actions of coordination and cooperation in this field; meetings will be attended by MS experts in order to provide follow up and technical support in implementing the method of coordination.

Benchmarks:

- A practical manual targeting the PSD-CID and containing the material developed for the training sessions, the introduced methods of communications, relations and stakeholders coordination, best practices and practical case studies from MS counterpart(s)
- At the end of the activity, at least 10 persons of CID staff have enhanced their capacities in communication and awareness, media and public relations, techniques and methods of coordination with stakeholders and promoting public participation

Activity 3.2: Implementing an awareness campaign to inform the general population on cybercrime dangers, according to specific targets

Tasks:

3.2.1 Common work with MS and PSD-CID experts for the setting up of an awareness campaign plan focused on different target groups (young population, customers of banks and financial companies, families, students and teachers).

3.2.2 Development of awareness materials focused on users of Facebook and other social networks; ().

3.2.3 Development of awareness materials focused on customers of private banks and companies:

3.2.4 Development of awareness materials focused on families: (

3.2.5 Development of awareness materials focused on students and teachers of secondary school: (d).

Benchmarks: Awareness campaign identified and developed,

3.5. Means

The means of the present Twinning Project is basically the public expertise made available by the MS administration over a 15 month duration. The MS key staff will consist of:

- The PL will coordinate the project from the home base of the MS Twinning administration. The PL will pay at least one mission every three months to Jordan. ,.
- The RTA will reside in the BC during the full duration of the Twinning Project activities. He is in charge of the day to day implementation of the project. The RTA Assistant and the translator, who will both support the RTA in implementing the daily tasks.
- The Key Short Term Experts in a number of selected fields.

3.5.1 Profile and tasks of the Project Leader (PL)

The Project Leader should be a high ranking civil servant with broad knowledge of all processes in the area of development and implementation of risk analysis, institutional and operational aspects that the project component is dealing with. The PL will continue to work at his/her Member State (MS) public administration but devote, some of his/her time to conceive, supervise and co-ordinate the overall thrust of the Twinning project. The PL will allocate a minimum of 3 days per month including one visit every 3 months to Jordan as long the project lasts.

Qualifications and skills

- University degree in Public Administration, Political Science, IT Engineering, computer science or another degree and equivalent to deal with cybercrimes analysis, discover and detection
- Current working experience as senior officer in a MS public administration or in a MS police institution with direct involvement of implementing the policies to combat cybercrimes
- Very good organizational, coordination, planning reporting and communication skills.
- Computer literacy (MS Office applications, Excel, E-mail, and internet)
- Experience assessment of the training and work group.
- Experienced knowledge of main cybercrime issues.
- Previous work experience with similar project would be an asset.

Tasks

- Overall project co-ordination;
- Co-chairing, with the Jordan PL, the regular project implementation steering committee meetings;
- Mobilizing short- and medium term experts;
- Executing administrative issues (i.e. signing reports, administrative order etc.)

3.5.2 Profile and tasks of the Resident Twinning Advisor (RTA)

Qualifications and skills

- University degree in Public Administration, Political Science, IT Engineering, computer science or another degree and equivalent to deal with cybercrimes analysis, discovery and detection
- Current working experience as senior officer in a MS public administration or in a MS police institution with direct involvement in the field of analysis, discovery and detection in cybercrimes.
- Good analytical and planning skills.
- Computer literacy (MS Office applications, Excel, E-mail, and internet)
- Very good organizational, coordination, reporting and communication skills.

- Fluency in oral and written English;
- Good leadership skills.
- Previous experience in management of EU funded projects and implementing similar missions in other ENPI countries would be an asset. .

Tasks
The RTA will be in charge of the day to day implementation of the project. RTA will carry out his responsibility according to the Twinning Manual.

In the implementation of his/her daily tasks, the RTA will be supported by two assistants, of Jordanian nationality, who will be hired by the Twinning project for the entire period of project implementation (15 months). One assistant will be primarily responsible for general project duties and secondly translation and interpretation duties while the other one will be more focused on linguistic (interpretation and translation) issues.

3.5.3 Profiles and Tasks of the Short- Term Experts
The RTA will be assisted by a number of STEs identified according to the activities mentioned above. The role, profile and duration of these experts will be defined in the work plan in accordance with the activities to be undertaken by both the RTA and the MS Project Leader. The following qualifications are indicative:

Qualifications and skills
- Minimum of 5 years professional experience in a Public administration or in a police institution department in the respective fields concerning combat against cybercrime
- University degree in Public Administration, Political Science, IT Engineering, computer science or another degree and equivalent to deal with cybercrimes analysis, discover and detection
- Proven ability the crime evidences.
- Experience assessment of the training and work group.
- Experience knowledge of main cybercrime issues.
- Good knowledge of the EU Acquis and International conventions against cybercrime
- Good written and oral command of English

Tasks
- Development of a Gap Analysis model for PSD-CID;
- Support to the beneficiary staff for the development of an action plan for establishing an integrated system in Jordan for combating and preventing cybercrime in line with EU best practices;
- Provision of training and ToT
- Support to the development of practical manuals
- Follow up to Beneficiary staff in implementing actions of coordination with relevant stakeholders in both preventing and identifying initiatives to combat cybercrimes.

4. INSTITUTIONAL FRAMEWORK
The main beneficiary Institution of this project will be the PSD-CID as this institution plays a key role in coordinating the actions of investigation on cybercrime in Jordan. As Beneficiary Administration, the PSD-CID will be committed to assign relevant staff to cooperate and work closely with their MS counterparts. They will work together in achieving the results of this project.

According to needs, other bodies of the Jordan state administration, which are relevant in the process of raising the awareness in the general public, or to share with PSD-CID know-how and the initiatives to prevent and combating cybercrime at National and International levels, may also get involved in some of the project activities or share some of the attained results. In particular, for the implementation of the project's activities and in accordance to the different tasks as established by the Jordan institutional and legislative framework, the PSD-CID is supposed to be supported by some partners which are the Family Protection Department, the ITC and the Laboratory Departments within the PSD, and the Ministry of Justice for the involvement of the judges in component 2.
PSD-CID is committed to make available the necessary office space and equipment for the MS partners to carry the project's activities. This includes access to the Internet as well as computer/s and necessary equipment (printer, photocopier, telephone, fax etc.). It also includes the provision of suitable venues/material/equipment for training and meetings in the BC. During the implementation period, the RTA will be accommodated with an appropriate office space and communication tools.

Most of the twinning activities will be undertaken within the PSD-CID, apart from study visits which will be implemented by Jordan experts in the Twinning MS Country. PSD-CID main offices are located in Amman, but the project may also have to engage in activities in selected governorates/districts outside the capital.

Since the civil servants of the PSD are generally not able to perform activities in a high level of English, an assistant will be hired specifically for translation and interpretation. Ideally this person should have adequate skills in the specific fields of IT and cybercrime investigations.

5. BUDGET

The total estimated budget of the project is EUR 900,000

6. IMPLEMENTATION ARRANGEMENTS

6.1 Implementing Agency responsible for tendering, contracting and accounting

The Programme Administration Office (PAO) is in charge of the coordination of all the activities and the administrative management of the Support to the Association Agreement Programme. The PAO will be the responsible institution for the management of this twinning project. It manages the tenders, contracts and payments and this, in accordance with the procedures of ex-ante control defined in the Practical Guide to contract procedures financed from the General Budget of the EC in the context of external actions.

Contact details of PAO responsible of the contract:
Ministry of Planning and International Cooperation
Mr. Marwan Al-Refai
Programme Administration Office
Support to the implementation of the EU-Jordan Association Agreement
P.O. Box 555 Amman, 11118 Jordan
Fax: 00 962 6 464 9024
Marwan.r@mop.gov.jo

6.2 Main counterpart in the Beneficiary Country

BC Project Leader

LtCol. Khlif Al-Amro Head of Training division/ CID
Phone Number: 00962779915159
E-mail: khlif.amro @yahoo.com
Address: Amman – Abdali

The Jordan Project Leader (PL) is a senior civil servant at decision-making level. He will act as the counterpart of the Member State PL. He will ensure the overall steering and coordination of the project from the Jordan side, including proper policy dialogue and political support. The PL's seniority will ensure his ability to mobilise the necessary staff in support of the efficient implementation of the project. He will lead/coordinate Project Steering Committee (PSC) from the Jordan side.

RTA counterpart
Captain Mustafa Al sukar, Assistant of head of anti-cybercrime division/CID.
Phone Number: 00962772273803
E-mail: cyber.crimes@psd.gov.jo
Address: Amman-Abdali

The RTA Counterpart is a senior civil servant who will work with the RTA on a daily basis to ensure proper coordination and implementation of all activities of the project and achieve an efficient transfer of knowledge and information. He may be involved in one or more of the components of the twinning fiche and be responsible, together with the RTA, for the drafting of the reports to be submitted to the PLs which will be discussed and approved by the Project's Steering Committee.

6.3 Contracts
There will be one twinning contract with a selected Member State or consortium of Member States.

7. INDICATIVE IMPLEMENTATION SCHEDULE

7.1 Launching of the call for proposals: January, 2013

7.2 Start of project activities: July, 2013

7.3 Project completion: September, 2014

7.4 Duration of the execution period: (15+3) months

8. SUSTAINABILITY
The project shall continue its effects and benefits in the long term after the end of the envisaged activities. This can be achieved by ensuring the transfer of know-how with the institutions involved (at both Public and private levels). In this sense, all training materials elaborated under the Twinning Project will continue to be used by the PSD-CID and by the other involved partners and stakeholders after the project's completion. All materials - Action Plans, Training Material and Manuals - elaborated within the project shall be submitted in English, so as to ensure smooth dissemination of the project results and sustainability of results. The full time translator financed under the twinning project will support the translation of the documents into Arabic during the joint working process.

The institutional sustainability of the project results will also be guaranteed by the direct involvement of the PSD-CID as main beneficiary institution of the Twinning project. Accordingly, this institution will ensure the synergies and the connections of all relevant stakeholders at both public and private levels, as well as with the other relevant actors in the fight against cybercrime (specifically, the general public through target groups as defined by the project, and the educational sector).

The financial sustainability of the outputs attained by the project will be ensured by the Jordan Government through the provision of relevant funding to PSD, in order to implement its daily tasks.

9. CROSS-CUTTING ISSUES

9.1 Equal Opportunity

Participation in this project will be open to both males and females involved in the sector. Records of professionals' participation in all project related activities will reflect this and will be kept with the project documentation. All the staff of the pilot enforcement offices will involve the activities of the project equally. Jordan PSD and also the other side beneficiaries are equal opportunity employers. Selection of staff and other personnel to work on the projects will be based on objective assessments of qualification and experience, without regard to gender.

9.2 Environment

The project will not have any negative influence on the environment.

9.3 Minorities

This project has no negative impact on minority and vulnerable groups.

9.4 Civil Society

The project aims to provide a considerable input in enhancing the level of the cooperation between the relevant Governmental institutions and the civil society organisations in the actions to prevent and combat cybercrime. In the specific, the component 3 is focused on implementing actions to increase the level of awareness to the general public, according to identified targets (young population, families, banks and private companies, educational sector) on the dangers and methods of cybercrime and the main measures to combat and to prevent them. Moreover, the project is foreseen to develop actions in which a forum of discussion between PSD staff with civil society organisations (NGOs, private universities, Jordan branches of international organisations for family and children protection, and so on) will be organised and implemented. This activity is aimed to inform and share with civil society organisations about the dangers of cybercrime in Jordan, on practical cases of actions against cybercrime and to promote initiatives of coordination and cooperation in this field.

10. CONDITIONALITY AND SEQUENCING

10.1 Conditionality

Projects to be implemented through twinning require the full commitment and participation of the senior management of the beneficiary institution. In addition to providing the twinning partner with adequate staff and other resources to operate efficiently, the senior management must be involved in the development and implementation of policies and changes required to deliver the project results.

The EU funded projects completed in previous years have shown us that the training courses should continue after the end of the project and have a continuous aspect. So, it is essential to pay attention to the training of trainers and prepare appropriate education and training materials.

Functional personnel give greater support to the project than hierarchical superiors. The involvement of aforementioned kind of personnel, increase the contribution of the beneficiary.

Full contribution of beneficiary country personnel in the project must be provided, and the workshops and other activities must be held out of the facilities where they are in charge. This would prevent the lack of concentration stemming from the unexpected interruptions of their daily occupations.
Since the project will be run through a twinning contract, the project team shall have a very good cooperative approach. Particularly, the resident twinning advisor and his counterpart should work in close collaboration and mutual understanding.

10.2 Sequencing

A number of various activities may run in parallel. However, some activities are dependent upon the completion of other activities in the same component or in another component. Further details about scheduled activities shall be arranged among the BC and the selected MS PL and RTA during the phase of project preparation.

ANNEXES

I. Logical framework planning matrix

ANNEX I: logical framework matrix

Name and Project Number: **Strengthen the capacity of the public administrations to combat cybercrime in The Hashemite Kingdom of Jordan.**		Cris Nr: 2009/020-478 Support to the Implementation of the Action Plan Program (SAPP II) **TOTAL BUDGET: € 900,000**	
Overall Objective	**Objectively verifiable Indicators**	**Sources of Verification**	
To improve the capacity to fight cyper crime in Jordan, according to the Jordan Law and in line with the relevant EU standards and international best practices.	Increase in the number of solved cybercrime cases. increase of the cooperation level between relevant authorities (specifically the PSD-CID) and stakeholders according to the requests/answers numbers	EU Commission Jordan Progress Reports in 2013 Statistical data of Jordan National Police and Annual report of MoJ for Cybercrime cases Jordan National Police's statistical data of the requests/answers between CID and other public stakeholders	
Project Purpose	**Objectively verifiable Indicators**	**Sources of Verification**	**Assumptions**
To improve the ability of the Criminal Investigation Department of the Jordan Police (PSD-CID) in implementing investigations on cybercrime cases and, in so doing, to improve the level of cooperation with its partners institutions at both National and International levels in order to combat cybercrime through the exchange of information, best practices and experience.	PSD-CID are well trained against cybercrime and are able to cooperate at national and international level with developed procedures according to the Jordan law, and in line with the EU policies and Convention on Cybercrime.	EU Commission Jordan Progress Reports in 2011 Statistical data of Jordan National Police and Annual report of MoJ for Cybercrime cases Statistical data of the CID for sent/received requests on cybercrime cases	The cooperation between the organizations (PSD-CID, laboratories, Family protection Dept. MoJ, IT and telecommunication companies, civil society organisations, banks, in-line Ministries) is enough and their contribution level to the establishment of an integrated system in Jordan against cybercrime is high. Police cooperation is followed by judicial cooperation in a timely manner Fluctuation of staff remains limited Continued commitment from

			the Jordan Government to support the enforced system against cybercrime
Results	**Objectively verifiable Indicators**	**Sources of Verification**	**Assumptions**
1. The capacity of the CID officers in charge of managing investigations on cybercrime cases is strengthened through better knowledge of the new technologies, the adequate use of the instruments and tools of cyber investigation and to prepare accurate reports in particular in the fields of credit card fraud, intrusion attacks and child sexual abuse online	-. A detailed capacity building and training needs assessment report developed, shared and approved within CID -. Three PSD decision makers for relevant issues concerning cybercrime implementing the trip to MS twinning country/ies and receiving detailed information on the methods of work adopted by the MS twinning institution(s) in the field of fighting cybercrime, presenting the EU acquis, the MS best practices and the used instruments and tools. -. At least 60 BC policemen working within the CID- cybercrimes division trained on how (at least) to manage ITC tools' to fight cybercrime, how to implement actions of cyber investigations, how to prepare adequate reports -. At least 15 CID policemen trained according to the developed TOT plan for PSD; a practical manual (in English and Arabic languages) for ToT developed; at least two pilot training coursed implemented and evaluated by project MS experts -. A plan of Study visits implemented, 20 CID experts trained and EU best practice shared with them	• Project Progress Reports • Project Needs Assessment report • Training action plan and training material (including training and ToT manuals) • List of participants forums and workshops • Leaflets and brochures printed • PSD-CID website, • Minutes of the Meetings and Mission Reports, including study visits	• PSD-CID and other involved Departments within Jordan Police are functioning and operative when project's activities start • Appropriate expertise and necessary documentations available • Strong involvement of the PSD at all levels • Beneficiary institutions ensure staff and trainees available
2. Improved level of cooperation between CID- division of cybercrimes and other relevant	-. Meetings between MoJ and PSD-CID implemented, a document developed, containing recommendations on new methods	• Project Progress Reports • Developed materials (organisational set up, training	• Continuous cooperation between PSD-CID with the relevant stakeholders

institutions at both the national level (Ministry of Justice, Laboratories and Crime Evidence Department, Family Protection Department within the PSD) and international level in implementing coordinated actions in the fight against cybercrime.	identified and a plan for future pilot actions of cooperation among the partners -. At least one pilot action (to be defined during the meetings of coordination) of joint cooperation between ITC and telecommunication companies with PSD-CID. -. Increased know how and skills of CID staff to accede international networks of institutions combating cybercrime and to manage coordinated actions such as investigations and exchange of information on international cases - a preliminary assessment of the possibility of Jordan ratifying the Budapest Convention finalised	plan, training curricula, standard operation procedures, plan of actions of joint cooperation between PSD-CID and telecommunication companies) • List of participants of workshops and seminars • INTERPOL and EUROPOL guidelines • Minutes of the Meetings and Mission Reports	• Strong involvement of the PSD at all levels • Stakeholders are willing to initiate project's actions
3. Raised public awareness on the methods and dangers of cyper crime, in particular amongst the young population, families, banks and private companies, and educational sector, including the main measures to combat and prevent them.	-. A practical manual (in both English and Arabic) targeted the PSD-CID containing the material developed for the training sessions, the introduced methods of communications, relations and stakeholders coordination, best practices and practical case studies from MS counterpart(s) -. At the end of the project, at least 10 persons of CID staff have enhanced their capacities in communication and awareness, media and public relations, techniques and methods of coordination with stakeholders and promoting public participation -. Awareness campaign identified sample of brochures designed: focused on users of social networks, focused on customers of private bankers, focused on families, focused on students and teachers of secondary school.	• Project Progress Reports • Training action plan and training material (including training manual on media relations and communications) • List of participants forums and workshops • Leaflets and brochures of awareness campaign printed • PSD-CID website, • Minutes of the Meetings and Mission Reports	• Continuous cooperation between PSD-CID with the relevant stakeholders • Strong involvement of the PSD at all levels • Stakeholders are willing to initiate project's actions

Components and Activities	**Assumptions**
Component 1:.	
1.1 Assessing the capacities and training needs of CID staff/divisions in charge of cybercrime cases investigation **1.2** Familiarisation trip to MS country/ies involving PSD decision makers **1.3** Training to CID-in charge officers on methods and instruments for fight against cybercrime **1.4** Setting up and implementation of a training of trainers- program ensuring the sustainability of the introduced best practices within the PSD **1.5** Study visit for CID policemen in MS country/ies focused on technical methods and sharing best practices management issues as adopted in the EU MS	• Legislation, information and data are available • The recommendations and the operational guidelines will be accepted by PSD-CID and supported by the Jordan Government • PSD-CID involved staff will maintain high commitment in attending project actions focused to them
Component 2:.	
2.1 Improving the cooperation of CID with the MoJ **2.2** promoting the cooperation with ITC telecommunication companies on cybercrime **2.3** Enhancing the capacity of PSD-CID to cooperate at international level in actions to prevent and to combat cybercrime	• MoJ will mantain high commitment in the designing of instruments and tools for fostering the system against cybercrime • PSD-CID ensure staff participation • Cooperation among all involved stakeholders is high
Component 3:.	
3.1 Capacity building to PSD/CID to identify and implement actions of raising the Awareness on cybercrime focused on relevant stakeholders **3.2** Implementing an awareness campaign to inform the general population on cybercrime dangers, according to specific targets	• PSD-CID ensure staff participation • Cooperation among all involved stakeholders is high