Standard Summary Project Fiche – IPA Decentralized National Programmes

1. Basic information

1.1 CRIS Number: TR2009/0324.01

1.2 Title: Strengthening Capacity against Cybercrime

1.3 ELARG Statistical code: 24 -Justice, freedom and security

1.4 Location: Republic of Turkey

Implementing arrangements:

The Central Finance and Contracts Unit (CFCU) will be Implementing Agency and will be responsible for all procedural aspects of the tendering process, contracting matters and financial management, including payment of project activities. The Director of the CFCU will act as Programme Authorizing Officer (PAO) of the project.

The Head of the CFCU will act as Programme Authorizing Officer.

Muhsin ALTUN
PAO, Director
Phone : +90 312 295 49 00
Fax : +90 312 286 70 72
E-mail : muhsin.altun@cfcu.gov.tr
Address : Eskişehir Yolu 4.Km. 2.Street. (Halkbank Kampüsü) No:63 C-Blok
06580 Söğütözü/Ankara TÜRKİYE

1.6 Beneficiary (including details of SPO):

Main Beneficiary:
1) Turkish National Police (Project Implementation: Department of Anti Smuggling and Organised Crime),
2) Gendarmerie General Command

Side Beneficiaries:
2) Ministry of Justice
3) Telecommunication Presidency

Ministry of Interior, Turkish National Police,
Turkish Project Leader will be:
Ahmet PEK
Head of Department of Anti Smuggling and Organised Crime
Phone : +90 312 412 70 12
Fax : +90 312 417 06 21
E-mail : apek@kom.gov.tr
Address : Konur Sok. No: 40 Bakanlıklar-Ankara TÜRKİYE

SPO of the project will be:
Ömer TEKELİ
Deputy Head of Department of Anti Smuggling and Organised Crime, Superintendent Chief at 2nd degree,

Phone : +90 312 412 70 40
Fax : +90 312 417 06 21
E-mail : omertekeli@kom.gov.tr
Address : Konur Sok. No: 40 Bakanlıklar-Ankara TÜRKİYE

Turkish Counterpart RTA of the project will be:
Bilal ŞEN
Department of Anti Smuggling and Organised Crime
Superintendent
Phone : +90 312 412 74 80
Fax: : +90 312 412 74 59
E-mail : bilalsen@kom.gov.tr
Address : Konur Sok. No: 40 Bakanlıklar-Ankara TÜRKİYE

Ministry of Interior, Gendarmerie General Command

The contact persons will be:

Volkan Güner GÜNGÖR
Anti-Smuggling and Organised Crime Department, Head of Cybercrimes Section
Captain
Phone : +90 312 456 33 65
Fax : +90 312 231 29 69
E-mail : vgungor@jandarma.tsk.tr

Ayşe ŞİMŞEK
Foreign Relations and Human Rights Department
EU Project Expert
Phone : +90 312 456 22 71
Fax : +90 312 215 14 17
E-mail : asimsek@jandarma.gov.tr
Address : Jandarma Genel Komutanlığı, Genel Prensipler Başkanlığı Beştepe-Ankara TÜRKİYE

Ministry of Justice

The contact persons will be:

Cengiz TANRIKULU
Ministry of Justice
Judge-rapporteur
Phone : +90 312 204 14 00
Fax : +90 312 296 88 88
E-mail : ctanrikulu@adalet.gov.tr
Address : Adalet Ek Binası, Konya Yolu No: 70 Kat: 6 Ankara TÜRKİYE

Nur ÖZMERİÇ
Ministry of Justice
Judge-rapporteur
Phone : +90 312 414 78 23
Fax : +90 312 425 02 90
E-mail : nozmeric@adalet.gov.tr

Address : Milli Müdafaa Cad. 22 Bakanlıklar 06659 ANKARA

Telecommunication Presidency

The contact person will be:

Ömer TUNÇ
Telecommunication Presidency
Communication Expert
Phone : +90 312 583 36 62
Fax : +90 312 583 36 36
E-mail : omer.tunc@tib.gov.tr
Address : Cevizlidere Cad. No: 11 Balgat Ankara TÜRKİYE

Financing:

1.7 Overall cost (VAT excluded)[1]: 1.400.000 €

1.8 EU contribution: 1.330.000 €

1.9 Final date for contracting: 2 Years after the signature of the Financing Agreement

1.10 Final date for execution of contracts: 2 years after the last date of contracting deadline

1.11 Final date for disbursements: 1 year after the end date for the execution of contracts

2. Overall Objective and Project Purpose

2.1 Overall Objective:

To improve the capacity of law enforcement and criminal justice authorities against cybercrime in line with EU policies and strategies

2.2 Project purpose:

To improve the investigative capacity of law enforcement authorities, adjudication capacity of criminal justice authorities by training and to improve cooperation level between national and international public and private sector bodies against cybercrime including exchange of information, expertise, best practices and to contribute to the implementation of action plan against organised crime.

2.3 Link with AP/NPAA / EP/ SAA

This project proposal addresses the areas defined in the revised Accession Partnership (AP) and the National Program for the Adoption of the Acquis (NPAA) for Turkey's accession to the EU, as follows:

Link with AP:

Short-Term Priorities, Chapter 24 "Justice, freedom and security section" of the Accession Partnership Document (2008) it is stated that:

- Implement the national strategy on organised crime. Strengthen the fight against organised crime, drugs, trafficking in persons, fraud, corruption and money-laundering.

[1] The total cost of the project should be net of VAT and/or other taxes. Should this not be the case, the amount of VAT and the reasons why it should be considered eligible should be clearly indicated (see Section 7.6)

Link with NPAA:
Priority 24.1 – Strengthening and improving the judicial and administrative capacity of the law enforcement forces and continuing to adopt, implement status and function of these bodies to meet EU Standards

Table 24.1.2 Schedule for Necessary Institutional Changes

Ministry of Interior Turkish National Police

14. Strengthening the investigative and preventative capacity against Cybercrime

Priority 24.4 – Implementation of "The National Strategy of Turkey against Organised Crime". Strengthening the fighting capacity against organised crime, drugs, fraud, corruption and money laundering

Table 24.4.2 Schedule for Necessary Institutional Changes

Ministry of Interior16- Strengthening the capacity of law enforcement forces against Cybercrime

Turkey 2008 Progress Report

No progress can be reported on judicial cooperation in criminal matters. Cooperation is ensured by means of international and bilateral agreements and, in the absence there, on the basis of reciprocity and international customary law. Key pending issues are related to effective implementation of relevant Council of Europe conventions, especially on mutual legal assistance and on extradition. Turkey has not signed key international conventions, such as the Second Additional Protocol to the Council of Europe Convention on mutual legal assistance or the Convention on cybercrime. Turkey needs to take the necessary steps to sign a cooperation agreement with Eurojust.

In the area of police cooperation, limited progress has been achieved. A code of ethics for law enforcement agents in line with international standards has been adopted. Turkey has signed a number of bilateral agreements on police cooperation. The lack of legislation on protection of personal data and the absence of an independent supervisory authority is obstructing the conclusion of an operational cooperation agreement with Europol (a strategic cooperation agreement has been in force since 2004). This also creates difficulties when it comes to cooperating at international level. Closer cooperation and communication between law enforcement agencies, and also with the judiciary, is of key importance.

Some progress has been observed in the fight against organised crime. A new Law on witness protection was adopted, with adequate provisions to guarantee the confidentiality of their identity and their security. This is expected to improve the chances of convictions in organised crime cases. The Regulation on the principles and procedures governing controlled delivery was extended to include the coast guard and the customs administration, in addition to the gendarmerie and the police. Following adoption of a Law on cybercrime, an internet department was established under the telecommunications authority to take charge of monitoring, supervision and coordination and some implementing legislation was adopted. Expertise in forensics is good. However, establishment of a national fingerprint and DNA database and adoption of harmonised crime scene investigation practices remain key issues. One important point is that the strategy against organised crime, in line with EU best practice,

needs to be followed up by a specific action plan and implemented accordingly. Special investigative techniques need to be developed and relevant training provided.

2.4 Link with MIPD

In the Multi-annual Indicative Planning Document (MIPD) 2008-2010 for Turkey, it is stated that

Component I – Transition Assistance and Institution Building,
Addressing the Copenhagen political criteria
Justice, Freedom and Security: Migration and asylum policy (including the establishment of reception centres for asylum seekers), border management; visa policy and practice, fight against organised crime, drugs, protection of personal data.

2.5 Link with National Development Plan (where applicable)

Regarding the proposed project, the 9th National Development Plan (2006) included the following statements:

Section: 5.6.6. Making Security Services Efficient

323. Crime related problems are created in an environment where rapid transformation is experienced in social and cultural areas together with economic fluctuations, employment and urban adaptation. They arise due to internal migration, international and organised activities of criminal organizations through the use of information and communication technologies, all of which have led to an upward trend in organised crimes, especially in terrorism. Therefore, the issue of domestic security has maintained its importance also during the 8th Plan period.

324. Even though some progress was accomplished on issues such as fighting terrorism and its financing, illegal migration and refugee movements, human trafficking, organised crime, and drug use and abuse, the programme failed to reach the specified targets.

325. Issues such as lack of coordination among security forces, inability to establish sufficient coordination among relevant institutions in intelligence activities and the failure to strengthen and spread the anti-crime infrastructure means that collecting sufficient evidence to ensure successful convictions remains an important issue

2.6 Link with national/ sectoral investment plans (where applicable)

Strategy Document for the Fight against Organised Crime (October 2006)

Turkish National "Strategy Document for the Fight Against Organised Crime" has been indited including the main principles to deal with all organised crime types in Turkey. There is also an ongoing study for preparing an action plan in line with the strategy document.

Section 3.7:

3.7.8 Fighting Against Information Crimes

a) Work must be conducted, with the contributions of academics and experts, towards activities carried out by organised criminal groups through information systems, and projects must be developed for solving problems encountered in terms of legislation and practice.
b) In-service training activities must be organised with the law enforcement and judicial bodies and relevant institutions to eliminate shortcomings that exist in the fight against information crimes and adversely affect this fight.
c) During the investigation of these crimes, the specialist investigation units must be supported with technical material to examine items stored in the form of digital data.

3. Description of project

3.1 Background and justification:

Cybercrime

Turkish society, like many others around the world, are increasingly relying on information and communication technology (ICT) and are thus increasingly vulnerable to threats such as cybercrime.

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 organised and aimed at generating criminal proceeds. Links between organised crime and cybercrime include that:

- ICT facilitate offences by organised 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 organised and economic crime and other forms of serious crime, including terrorism, therefore need to include measures against cybercrime.

The Convention on Cybercrime

Full implementation of the Convention on Cybercrime of the Council of Europe (the so-called "Budapest Convention" helps countries meet the challenges of cybercrime. The Convention provides for:

- Substantive criminal law measures, that is, conduct that is to be made a criminal offence (illegal access and interception, system and data interference, misuse of devices, child pornography, computer-related fraud and forgery, copy right infringements and others)
- Procedural law, that is, measures for more effective investigations of cybercrimes. It should be underlined that these procedural measures can be used for any criminal offence involving a computer system. For example, they can be used in the case of terrorism, money laundering, trafficking in human beings, corruption or other serious crimes where ICT are involved.
- Efficient international cooperation with general principles of cooperation (that is, general principles on international cooperation, principles related to extradition, principles related to mutual legal assistance, spontaneous information etc.) as well as specific provisions for more effective cooperation. These permit parties to the Convention to apply procedural tools also internationally. This Section also provides for the creation of a network of contact points which are available on a 24/7 basis to facilitate rapid cooperation.

By July 2008, the Convention had been ratified by 23 countries and signed by another 22. It is the only international treaty in this field and increasingly as a global scope. Canada, Japan and South Africa have signed it, the USA has ratified it and Costa Rica, Mexico and the Philippines have been invited to accede.

Obviously, the more countries become a party the more effective the Convention will become. Turkey is one of the few European countries that have not yet signed the Convention.

The Convention on Protecting Personal Data
The Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data.

It is signed ratified by 41 countries in Europe. It is signed by Turkey but it has not adopted or ratified.

With regard to the European Union and the Commission, the Communication on Cybercrime of the European Commission (May 2007) and the Council Conclusions of 8/9 November 2007 expressed strong support to the Convention on Cybercrime in Europe and elsewhere around the world:

2827th Council meeting, Justice and Home Affairs, Brussels, 8-9 November 2007

4) Underlines the confidence placed in the Council of Europe Convention of 23 November 2001 on Cybercrime, supports and encourages implementation of the measures thereof and calls for the widest possible participation by all countries;

5) Attaches the greatest importance to promoting cooperation with non-member countries in preventing and combating cybercrime, more specifically, given the pivotal role of the Council of Europe Convention on Cybercrime by supporting the introduction of that

globally oriented legal framework, in liaison with the Council of Europe, especially in countries where development and technical assistance is being provided;

Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime

1.3. Objectives

The objective is to strengthen the fight against cyber crime at national, European and international level. Further development of a specific EU policy, in particular, has long been recognised as a priority by the Member States and the Commission. The focus of the initiative will be on the law enforcement and criminal law dimensions of this fight and the policy will complement other EU actions to improve security in cyber space in general. The policy will eventually include: improved operational law enforcement cooperation; better political cooperation and coordination between Member States; political and legal cooperation with third countries; awareness raising; training; research; a reinforced dialogue with industry and possible legislative action.

4.1. The fight against cyber crime in general

- Establish a strengthened operational cooperation between Member States' law enforcement and judicial authorities, an action which will begin with the organisation of a dedicated expert meeting in 2007 and which may include the setting up of a central EU cyber crime contact point

- Increase financial support to initiatives for improved training of law enforcement and judicial authorities vis-à-vis the handling of cyber crime cases and take action to coordinate all multinational training efforts in this field by the setting up of an EU training platform

- Promote a stronger commitment from Member States and all public authorities to take effective measures against cyber crime and to allocate sufficient resources to combat such crimes

- Take the initiative for and participate in public-private actions aimed at raising awareness, especially among consumers, of the cost of and dangers posed by cyber crime, while avoiding the undermining of the trust and confidence of consumers and users by focusing only on negative aspects of security

- Actively participate in and promote global international cooperation in the fight against cyber crime

- Initiate, contribute to and support international projects which are in line with the Commission policy in this field, e.g. projects run by the G 8 and consistent with the Country and Regional Strategy Papers (regarding cooperation with third countries)

- Take concrete action to encourage all Member States and relevant third countries to ratify the Council of Europe's Cyber Crime Convention and its additional protocol and consider the possibility for the Community to become a party to the Convention

- Examine, together with the Member States, the phenomenon of co-ordinated and large scale attacks against the information infrastructure of member states in view of preventing and combating these, including co-ordinating responses, and sharing information and best practices

As a result; when EU Policies are compared or matched with Convention on Cybercrime and Convention on Protecting Personal Data, it is seen that, when the Conventions are signed and ratified, they will highly contribute to implement and to adopt other EU policies and decisions. On other words, they will be the base for other policies implementation.

Cybercrime Legislation in Turkey

In recent years, Turkey has taken a number of important measures against cybercrime.

In terms of legislation, these include provisions in the Turkish Penal Code (Law 5237 of 2005) but also the Law on the Regulation of Internet Publications and Combating Crimes Committed via the Publications (Law 5651 of 2007). Many of these provisions are thus rather new and still need to be tested in practice.

Comparing Turkish legislation with the Convention on Cybercrime it seems that a number of provisions are already available, while a few are still missing. These include in particular the misuse of devices (article 6 of the Convention) and the possibility for expedited preservation of computer and traffic data (Articles 17 and 18 and with regard to international cooperation articles 29 and 30).

It has been proposed that Turkey urgently develops legislative amendments to close these gaps. These would allow Turkey to ratify the Convention on Cybercrime. A full review of the effectiveness of Turkish legislation should then be carried out in the near future on the basis of practical experience.

Strategy against Organised Crime

The Strategy Document for the Fight against Organised Crime[2] (October 2006) envisages the need to take measures against cybercrime:

> *3.7.8 Fighting Against Information Crimes*
>
> ***a)*** *Work must be conducted, with the contributions of academics and experts, towards activities carried out by organised criminal groups through information systems, and projects must be developed for solving problems encountered in terms of legislation and practice.*
> ***b)*** *In-service training activities must be organised with the law enforcement and judicial bodies and relevant institutions to eliminate shortcomings that exist in the fight against information crimes and adversely affect this fight.*
> ***c)*** *During the investigation of these crimes, the specialist investigation units must be supported with technical material to examine items stored in the form of digital data.*
> ***d)*** *Since the examination of computers or digital media seized during an investigation requires specialisation and special programs, such examination must be performed by competent personnel who received training in this field.*

[2] 1.1 PURPOSE [of the Strategy Document]
The purpose of this document is to determine the actions to be implemented and the measures to be taken towards strengthening the enforcement and implementation capacities of the judicial bodies, law enforcement bodies and other authorised units in charge of the fight against organised crime, with the aim of actively fulfilling our country's obligations under the National Programme for the Adoption of the EU Acquis and harmonising legislation in order to meet the conditions for accession to the European Union.

Update of the current Strategy Document and a joint action plan preparation according to this Strategy Document is in progress to implement the strategies. The Strategy Document –also as mentioned above- highlighted national and international cooperation and training requirements for law enforcement and criminal justice authorities. It is thought that, Action Plan, which is not published yet, will and should in line with subjects in this Strategy Document. That's why, it is considered that, the project will highly contribute to the implementation of the action plan that will be prepared.

Some of these measures will be followed up through the EC funded project "Strengthening the Investigation Capacity of Turkish National Police and Gendarmerie Against Organised Crime-TR080212".

Institutions involved in measures against cybercrime

These include:

- ***Turkish National Police, Department of Anti-smuggling and Organised Crime/Cybercrime Division***

Turkish National Police Anti-Smuggling and Organised Crimes Department and its 81 provincial divisions are tasked with detecting, preventing and investigating organised criminal activity in urban areas. Cybercrime&IT Division is one of six divisions of the Department and its provincial divisions. The whole staff consists of 5623 personnel in different ranks. 170 of these staff are employed in central and provincial cybercrime divisions where cybercrime matters such "illegal access to any part or whole computer system", "data interference or system interference" and "misuse of devices" investigations are implemented. Training the staff of 81 provincial divisions is also carried out by Central Division

- ***Ministry of Justice:***

In Turkey, public prosecutors are responsible for conducting all investigations. They carry out these investigations through judicial law enforcement units. After cybercrime cases are dispatched to these law enforcement units by public prosecutors, cybercrime divisions of anti smuggling and organised crime departments which operate under them handle these investigations. Ministry of Justice is officially responsible for basic and advanced training of prosecutors and judges

- ***Telecommunication Presidency:***

Telecommunication Presidency has been founded at 2006 within the Information Technologies and Communications Authority undertakes the tasks and responsibilities as follows;
- To carry out required measures in order to prevent the crimes and activities in question in cooperation with the Ministry of Transportation, law enforcement officers, relevant public institutions, content, space and access providers and relevant non- governmental organizations,
- To monitor the content of the publications in the internet and in case of the crimes within the framework of this law, to take required measures in order to block the access of this publications,
- To determine the timing and system of monitoring the content of the publications on the internet,
- To determine the procedures concerning the arrangements and systems which will be used in filtering and blocking,

- To establish monitoring and information warning centers in order to prevent the crimes in question or to have them established, to set up every required technical infrastructure for this purpose,
- To determine the minimum criteria concerning the production of hardware or writing software according to filtering, screening and monitoring procedures,
- To carry out coordination and cooperation with the international organizations operating in the areas of informatics and internet.
- To carry out coordination and cooperation between courts and LEA for LI.

- ***Gendarmerie General Command:***

The Turkish Gendarmerie is a law enforcement agency established in 1839, which carries out law enforcement in the rural areas of Turkey.
Anti-Smuggling and Organised Crime (ASOC) Department at Gendarmerie General Command Headquarters together with 54 ASOC Divisions and 27 ASOC Sections in 81 provinces are tasked with detecting, preventing and investigating organised criminal activity in rural areas. Cybercrime Section is under Organised Crimes Division, one of six divisions of the ASOC Department.
Also "Cybercrime Expert" staff is available under 17 of 54 provincial divisions. In 2010, Cybercrime Section will be a division and sections will be constituted under ASOC divisions of at least five critical Gendarmerie Provincial Commands.
Cybercrime training is carried out by ASOC Department through training at centre and mobile training activities in provinces.

Issues to be addressed by the project

The following issues would need to be addressed by the project:

- Need for effective legislation in line with the EU Acquis. Even if measures are taken to fill the gaps in Turkish legislation in the very near future, a thorough review would need to be carried out to assess the effectiveness of the legislation on the basis of practical experience. In connection with cybercrime it is important to strengthen legislation regarding the protection of personal data (in line with the EU Acquis and Council of Europe Convention ETS 108). This treaty was signed by Turkey in 1981 but has not yet been ratified. Such legislation is relevant with regard to privacy issues but also to enable Turkey to engage in broader law enforcement cooperation with Europol and EU Member States.
- Need for standardized training modules for law enforcement (standard and advanced courses on cybercrime investigations and forensic computing), prosecutors (standard courses on cybercrime investigations, electronic evidence and legal measures) and judges (standard courses on legal measures and electronic evidence). Such courses have been developed or are being developed in European Countries. They need to be adapted to Turkey. A sufficient number of trainers would need to be trained in order to ensure the sustainable delivery of such training.
- Need for efficient international cooperation against cybercrime. This includes the creation of a well-functioning 24/7 point of contact in line with Article 35 of the Convention on Cybercrime according to EU Acquis and measures to establish confidence and working relationships with contact points of other countries. In addition, there is a need to ensure that immediate and urgent measures at the level of police cooperation are followed up by efficient judicial cooperation by the Ministry of Justice and the prosecution service in line with Chapter III of the Convention on Cybercrime.

- As mentioned before the investigations of cybercrime in many cases require the cooperation between law enforcement and Internet service providers. Such cooperation is necessary but can also be problematical considering the different roles of law enforcement (to uphold the law) and ISPs (to provide services to their clients) and the need for both to protect privacy, freedom of expression and other fundamental rights of internet users.

3.2 Assessment of project impact, catalytic effect, sustainability and cross border impact (where applicable)

The project will have major impact on a variety of sectors varying from commerce to public order and to national security. In addition, transnational and cross border security will be considerably improved Another important impact is that fight against cyber crime will be strengthened as Turkey will have up-to-date practices, methods, equipments and well-trained staff similar to that found in EU Member States.

Realization of this project will significantly contribute to Turkey's and EU's capacity of law enforcement and criminal justice authorities against cybercrime in line with EU policies and strategies.

Strengthening the administrative and investigative capacities of the TNP and will make a catalytic effect on the process of investigations, national and international cooperation among law enforcement agencies and process of the judicial services especially against cyber crime.

3.3 Results and measurable indicators:

Results expected from this project are the following (in chart);

Results	Measureable Indicators
1 – Amendment is available in the relevant legislation according to EU policies and also in line with the Convention on Cybercrime and Convention on Protection Personal Data	By month 18, Draft laws for amendment of Turkish Penal Code in line with EU policies and also Convention on Cybercrime are available for submission to Parliament
2 – Training Modules are available and tested for standard and advanced training courses for law enforcement authorities, prosecutors and judges regarding the investigation, prosecution and adjudication of cybercrime	By month 18, training modules (standard for prosecutors/judges and standard/advanced for law enforcement officers) on cybercrime investigations and electronic evidence available and tested for replication A total of 20 trainers trained to deliver onward courses
3 – Procedures for 24/7 point of contact are available and officials responsible for international police and judicial cooperation are able to cooperate internationally according to these procedures which are fully in line with	By month 18, documents on request procedures, responsibilities of point of contact for international cooperation are available

EU Decisions, Convention on Cybercrime and Convention on Protecting Personal Data.	
4 – The dialogue between law enforcement authorities and internet service providers is strengthened; procedures and guidelines are available for requests to cooperate fully in line with Convention on Cybercrime according to EU Acquis.	By month 18, documents on request procedures between law enforcement authorities and ISPs are ready

3.4 Activities:

To achieve all of the results, It will be made under a "Twinning" Contract. The co-financing of the contract has been presented in the indicative budget table.

Result 1 – Amendment is available in the relevant legislation according to EU policies and also in line with the Convention on Cybercrime and Convention on Protection Personal Data

1.1 Review of Turkish legislation against the provision of the Convention on Cybercrime (ETS 185) and Convention on Protecting Personal Data (ETS 108)
1.2 3 workshops on cybercrime legislation in Turkey
1.3 1 regional/international conference on good practices regarding cybercrime legislation
1.4 Drafting the legislation of Cybercrime

Inputs:

- Cost of RTA
- 15 workdays of short-term consultants
- Cost for three workshop including international experts
- Cost for international conference
- 20 workdays of short-term consultants

Result 2 – Training Modules are available and tested for standard and advanced training courses for law enforcement authorities, prosecutors and judges regarding the investigation, prosecution and adjudication of cybercrime

2.1 Review of training materials for law enforcement officers on cybercrime investigations and forensic computing developed by other organizations and projects
2.2 Review of training materials for prosecutors and judges on cybercrime investigations and electronic evidence, developed by other organizations and projects
2.3 2 study visits of staff to Member States to see best practices on training programs and training methods
2.4 Selection of training institution and trainers
2.5 Adaption of training materials to meet Turkish needs for a standard and advanced courses

2.6 Training of trainers for law enforcement officers on cybercrime investigations and forensic computing
2.7 Training of trainers for prosecutors/judges on cybercrime investigations and electronic evidence
2.8 1 Study visit to Member States on training methods and materials for the trained trainers
2.9 5 pilot training courses for law enforcement officers
2.10 3 pilot training courses for prosecutors
2.11 3 pilot training courses for judges
2.12 Finalization of the training materials for law enforcement officers
2.13 Finalization of the training materials for prosecutors/judges

Inputs:

- Cost of RTA
- 35 workdays of national and international short-term consultants
- 25 workdays of national and international short-term consultants
- 15 workdays by project management
- 40 workdays of national and international short-term consultants
- training of trainer workshops (law enforcement)
- training of trainer workshops (judges and prosecutors)
- Cost of 3 study visits
- Cost of 5 training courses (law enforcement)
- Cost of 3 training courses (prosecutors)
- Cost of 3 training courses (judges)
- 20 workdays of national and international short-term consultants
- 20 workdays of national and international short-term consultants

Result 3 – Procedures for 24/7 point of contact are available and officials responsible for international police and judicial cooperation are able to cooperate internationally according to these procedures which are fully in line with EU Decisions, Convention on Cybercrime and Convention on Protecting Personal Data.

3.1 In-service training for the staff of the 24/7 contact point in Turkey, including clarification of responsibilities and procedures
3.2 Internship of 3 24/7 contact point staff in another European contact point. It is proposed that the staff will work for a month in work hours of the contact point. They will observe what should staff do when they receive a request and how the requests are answered.
3.3 In-service training for the Ministry of Justice and the prosecution staff responsible for international cooperation in criminal matters in Turkey
3.4 Preparation of a manual on the subject of cooperation between law enforcement and judicial authorities in cybercrime matters
3.5 Hosting of 2 regional/international events for contact points and authorities responsible for judicial cooperation from other countries
3.6 3 Study visits to Member States to see best practices for international cooperation and to exchange knowledge and experience

Inputs:

- Cost of RTA
- Cost of participation in international meetings of contact points
- 20 workdays of national and international short-term consultants

- Cost of internship (3 x 12 days)
- Cost of study visits
- Cost of participation in international meetings of contact points
- 20 workdays of national and international short-term consultants
- 25 workdays of national and international short-term consultants
- Cost of publication
- Cost of two international events

Result 4 – The dialogue between law enforcement authorities and internet service providers is strengthened, procedures and guidelines are available for requests to cooperate fully in line with Convention on Cybercrime according to EU Acquis.

4.1 1 seminar on law enforcement – service provider cooperation in Turkey
4.2 Workshop for law enforcement authorities to develop written procedures for cooperation with ISPs
4.3 Workshop for ISPs to develop written procedures for cooperation with law enforcement and prepare criminal compliance programmes
4.4 2 Training workshops for ISP and law enforcement staff designated to process requests for cooperation, including training regarding privacy and data protection standards
4.5 1 Seminar on the establishment of formal partnerships between law enforcement and ISPs

Inputs:

- Cost of RTA
- Cost of 1 seminar
- Cost of 2 workshops
- 10 workdays of national and international short-term consultants
- Cost of 3 workshops
- 10 workdays of national and international short-term consultants
- Cost of 2 workshops

3.5 Conditionality and sequencing:

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.

3.6 Linked activities

The project on "Strengthening the Investigation Capacity of Turkish National Police and Gendarmerie Against Organised Crime-TR080212" comprises a component to train and equip organised crime units. This includes equipment for computer forensics and a certain amount of training. It is therefore not necessary to purchase equipment under the current proposed project.

Fighting against cyber crime can be divided into two different subtopic. First is investigation of such crime and the second is computer forensics. Computer forensics involve seizing, searching, examining digital evidences. There are several methods and technical equipments to perform these tasks.

The training in this project-TR080212 comprises training for the technical equipment those supplied from the project and for computer and mobile phone forensic inspection. So by other words it will contribute to the technical capacity of law enforcement bodies. It doesn't comprise training about investigation, prosecution or adjudication of cybercrimes, that's why it is not proposed, there is no over-lap with the EU funded project "Strengthening the Investigation Capacity of Turkish National Police and Gendarmerie Against Organised CrimeTR080212"

The projects, which directly or indirectly have dealt with organised crime and cyber crime, have been achieved. These are:[3]

- Strengthening the Fight against Money Laundering
- Strengthening the Fight against Organised Crime
- Strengthening the struggle against money laundering, financial sources of crime and the financing of terrorism.
- Enhancement of the professionalism of the Turkish Gendarmerie in its law enforcement activities

3.7 Lessons learned

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. Personal relations definitely matter in terms of the success of the project.

[3] http://ec.europa.eu/enlargement/fiche_projet/index.cfm?page=415392&c=TURKEY

4. Indicative Budget (amounts in EUR)

					SOURCES OF FUNDING								
			TOTAL EXP.RE	TOTAL PUBLIC EXP.RE	IPA COMMUNITY CONTRIBUTION		NATIONAL PUBLIC CONTRIBUTION					PRIVATE	
ACTIVITIES	IB (1)	INV (1)	EUR (a)=(b)+(e)	EUR (b)=(c)+(d)	EUR (c)	% (2)	Total EUR (d)=(x)+(y)+(z)	% (2)	Central EUR (x)	Regional/ Local EUR (y)	IFIs EUR (z)	EUR (e)	% (3)
Activity 1													
Twinning contract 1.1	X	–	1,400,000	1,400,000	1,330,000	*95*	70,000	5	*70,000*				
……													
TOTAL IB			1,400,000	1,400,000	1,330,000	*95*	70,000	5	*70,000*				
TOTAL PROJECT			**1,400,000**	**1,400,000**	**1,330,000**	**95**	**70,000**	**5**	**70,000**				

NOTE: DO NOT MIX IB AND INV IN THE SAME ACTIVITY ROW. USE SEPARATE ROW

Amounts net of VAT

(1) In the Activity row use "X" to identify whether IB or INV

(2) Expressed in % of the **Public** Expenditure (column (b))

(3) Expressed in % of the **Total** Expenditure (column (a))

5. Indicative Implementation Schedule (periods broken down per quarter)

Contracts	Start of Tendering	Signature of contract	Project Completion
Twinning Contract 1.1	Q1/2010	Q4/2010	Q3/2012

All projects should in principle be ready for tendering in the 1ST Quarter following the signature of the FA

6. Cross cutting issues (where applicable)

6.1 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.

Turkish National Police 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.

6.2 Environment

It will not have any negative influence on the environment.

6.3 Minorities

According to the Turkish Constitutional System, the word "minorities" encompasses only groups of persons defined and recognized as such on the basis of multilateral or bilateral instruments to which Turkey is a party. This project has no negative impact on minority and vulnerable groups.

6.4 Civil Society

N/A

ANNEX 1: Logical framework matrix in standard format

LOGFRAME PLANNING MATRIX FOR Project Fiche	Programme name and number	Strengthening the Capacity against Cybercrime	
	Contracting period expires 2 years after financing agreement	Disbursement period expires 1 year after the end date for the execution of contracts	
	Total budget : 1.400.000	IPA budget: 1.330.000	

Overall objective	**Objectively verifiable indicators**	**Sources of Verification**	
To improve the capacity of law enforcement and criminal justice authorities against cybercrime in line with EU policies and strategies	10% increase in the number of solved cybercrime cases. 10% increase of the cooperation level between law enforcement authorities and ISPs according to the requests/answers. numbers	EU Commission Turkey Progress Reports in 2011 and onwards Statistical data of Turkish National Police and Ministry of Justice for Cybercrime cases Turkish National Police's statistical data of the requests/answers between TNP and ISPs	
Project purpose	**Objectively verifiable indicators**	**Sources of Verification**	**Assumptions**
To improve the investigative capacity of law enforcement authorities, adjudication capacity of criminal justice authorities by training and to improve cooperation level between national and international public and private sector bodies against cybercrime including exchange of information, expertise, best practices and to	Law enforcement and criminal justice authorities are well trained against cybercrime and are able to cooperate at national and international level with developed procedures according to EU policies and Convention on Cybercrime.	EU Commission Turkey Progress Reports in 2011 and onwards Statistical data of Turkish National Police and Ministry of Justice for Cybercrime cases Statistical data of the 24/7 contact point of Turkey for sent/received requests	The cooperation between the organizations (e.g. TNP, MoJ, Turk Telecom, ISPs) is enough and the contribution level of the organizations like ISPs is high.

contribute to the implementation of action plan against organised crime			Convention on Protection Personal Data is ratified and also Convention on Cybercrime is signed and ratified.
Results	**Objectively verifiable indicators**	**Sources of Verification**	**Assumptions**
1 – Amendment is available in the relevant legislation according to EU policies and also in line with the Convention on Cybercrime and Convention on Protection Personal Data	By month 18, Draft laws for amendment of Turkish Penal Code in line with EU policies and also Convention on Cybercrime are available for submission to Parliament	Draft laws for amendment of Turkish Penal Code Project Reports Steering Committee Reports	Draft laws are processed, submitted to and adopted by Parliament
2 – Training Modules are available and tested for standard and advanced training courses for law enforcement authorities, prosecutors and judges regarding the investigation, prosecution and adjudication of cybercrime	By month 18, training modules (standard for prosecutors/judges and standard/advanced for law enforcement officers) on cybercrime investigations and electronic evidence are available and tested for replication A total of 20 trainers trained to deliver onward courses	Training materials Certificates of "completion of training" Project Reports Steering Committee Reports	
3 –Procedures for 24/7 point of contact are available and officials responsible for international police and judicial cooperation are able to cooperate internationally according to these procedures which are fully in line with EU Decisions, Convention on Cybercrime and Convention on Protecting Personal Data.	By month 18, documents on request procedures, responsibilities of point of contact for international cooperation are available	Documents of "International Request Procedures and Responsibilities" Statistical data of Ministry of Justice for international judicial requests Number/timeliness of international judicial and policial requests sent/received by the Ministry of Justice, law enforcement authorities and the prosecution	Police cooperation is followed by judicial cooperation in a timely manner Fluctuation of staff remains limited

		Project Reports Steering Committee Reports	
4 – The dialogue between law enforcement authorities and internet service providers is strengthened; procedures and guidelines are available for requests to cooperate fully in line with Convention on Cybercrime according to EU Acquis.	By month 18, documents on request procedures between law enforcement authorities and ISPs are ready	Documents of "Request Procedures" Certificates of "participation of workshops" Project Reports Steering Committee Reports	Law enforcement and ISP respect each other's role and privacy of internet users
Activities	**Means**	**Costs**	**Assumptions**
1.1. Review of Turkish legislation against the provision of the Convention on Cybercrime (ETS 185) and Convention on Protecting Personal Data (ETS 108) 1.2 3 workshops on cybercrime legislation in Turkey 1.3 1 regional/ international conference on good practices regarding cybercrime legislation 1.4 Drafting the legislation of Cybercrime	Twinning	€ 230.000	

2.1 Review of training materials for law enforcement officers on cybercrime investigations and forensic computing developed by other organizations and projects 2.2 Review of training materials for prosecutors and judges on cybercrime investigations and electronic evidence, developed by other organizations and projects 2.3 2 study visits of staff to Member States to see best practices on training programs and training methods 2.4 Selection of training institution and trainers 2.5 Adaption of training materials to meet Turkish needs for a standard and advanced courses 2.6 Training of trainers for law enforcement officers on cybercrime investigations and forensic computing 2.7 Training of trainers for prosecutors/judges on cybercrime investigations and electronic evidence 2.8 1 Study visit to Member States on training methods and materials for the trained trainers 2.9 5 pilot training courses for law enforcement officers	Twinning	€ 570.000	

2.10 3 pilot training courses for prosecutors 2.11 3 pilot training courses for judges 2.12 Finalization of the training materials for law enforcement officers 2.13 Finalization of the training materials for prosecutors/judges			

3.1 In-service training for the staff of the 24/7 contact point in Turkey, including clarification of responsibilities and procedures 3.2 Internship of 3 24/7 contact point staff in another European contact point 3.3 In-service training for the Ministry of Justice and the prosecution staff responsible for international cooperation in criminal matters in Turkey 3.4 Preparation of a manual on the subject of cooperation between law enforcement and judicial authorities in cybercrime matters 3.5 Hosting of 2 regional/international events for contact points and authorities responsible for judicial cooperation from other countries 3.6 3 Study visits to Member States to see best practices for international cooperation and to exchange knowledge and experience	Twinning	€ 370.000	

4.1 1 seminar on law enforcement – service provider cooperation in Turkey 4.2 Workshop for law enforcement authorities to develop written procedures for cooperation with ISPs 4.3 Workshop for ISPs to develop written procedures for cooperation with law enforcement and prepare criminal compliance programs 4.4 2 Training workshops for ISP and law enforcement staff designated to process requests for cooperation, including training regarding privacy and data protection standards 4.5 1 Seminar on the establishment of formal partnerships between law enforcement and ISPs	Twinning	€ 230.000	

Pre conditions