IPA 2011 CROATIA PROJECT FICHE

1. Basic information

1.1. CRIS Number: IPA/2011/ 022-954/4

1.2. Title: Strengthening capacities of the Ministry of the Interior to combat computer crime

1.3. ELARG Statistical code: 03.24

1.4. Location: Republic of Croatia, Ministry of Interior

Implementing arrangements:

1.5. Implementing Agency:

Central Finance and Contracting Agency

The Programme Authorising Officer (PAO) for the project is:

Ms Marija Tufekčić, Director
Ulica grada Vukovara 284
10000 Zagreb, Croatia
Telephone: +385 (0)1 4591 245
Fax: +385 (0)1 4591 075
E-mail: marija.tufekcic@safu.hr

1.6. Beneficiaries (including details of SPO):

Ministry of Interior

The Senior Programme Officer:

Mr Filip Dragović, Director
Directorate for European Integration and International Relations
Ministry of Interior
Ilica 335
10 000 Zagreb, Croatia

Financing:

1.7. Overall cost (VAT excluded)1: EUR 700 000

1.8. EU contribution: EUR 665 000

1.9. Final date for contracting: 3 years following the date of conclusion of the Financing Agreement

1.10. Final date for execution of contracts: 3 years following the end date for contracting

1.11. Final date for disbursements: 4 years following the end date for contracting

2. Overall Objective and Project Purpose

2.1. Overall Objective:

To enhance capacities of the Ministry of Interior to combat cybercrime within the EU and international environment, in line with the related European policies and strategies.

2.2. Project purpose:

Component I – Forensic Science Centre

To develop the capacities of the Forensic Science Centre (FSC) to provide support to investigating cybercrime, as well as the expertise and evidence for processing and prosecuting of such criminal offences, following the best practices of the EU Member States.

Component II – Criminal Police Directorate

To enhance the capacities of the Criminal Police to investigate cybercrime, including the ability to exchange information and cooperate with the relevant law enforcement agencies of other countries and to operate in line with the EU anti-cybercrime initiatives.

2.3. Link with AP/NPAA / EP/ SAA

Croatia 2010 Progress Report:

4.7. Chapter 7: Intellectual property law: „The Ministry of the Interior, the Ministry of Science, Education and Sports and the Croatian Academic and Research Network concluded a cooperation agreement on prevention and settlement of computer incidents and other forms of computer crime.

[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)

However, violations of intellectual property are a growing concern for the health and safety of consumers. Public awareness of those topics remains low. Involvement of organised crime groups in IPR violations is increasing. Measures are therefore required to strengthen the capacity of the police and prosecutors."

Communication from the Commission to the Council and the European Parliament "Enlargement Strategy and Main Challenges 2010-2011": „However, efforts must continue and further intensify in particular in the field of judicial and administrative reform, the fight against corruption and organised crime, …"

2.4. Link with MIPD

The project is in line with **MIPD 2009 – 2011 under component I:**

Executive Summary: "Under IPA Component I which core activity is Institution Building, the priorities as regards the *political area* (first area of intervention under this MIPD) which were envisaged in the previous MIPD 2008-2010 will be maintained, i.e. with some possible support in the fields of judiciary including fight against organised crime, …"

"Concerning the ***ability to assume the obligations of membership*** (third area of intervention), IPA assistance will continue to support the institutional capacity building for *acquis* transposition and implementation according to the priorities identified in the Accession Partnership, the screening reports and subsequent negotiations in the different chapters of the *acquis*."

1. OBJECTIVES AND CHOICES FOR ASSISTANCE, **1st area of intervention -Political criteria:** „To assist in the systematic, efficient and coordinated fight against corruption and organised crime;"

The **MIPD 2011-2013**, adopted in June 2011, provides for support under the sector justice and home affairs and fundamental rights. Main objectives of this sector include support Croatia's efforts to fight organised crime and corruption. Indicators to assess the impact of EU support may include the number of successful prosecutions and final convictions for cases of organised crime and strengthened capacity of law enforcement institutions, including improved inter-agency and international cooperation.

2.5. Link with National Development Plan (where applicable):

Not applicable

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

Not applicable

3. Description of project

3.1. Background and justification:

One of the most important tasks of Croatian institutions has been fulfilling of all the requirements for accession to the European Union and preparing for cooperation and operation within the EU legal and institutional framework.

The importance of coordinating the efforts to combat "the rapidly growing threat from cyber crime"[2] has been recognized within the EU, as "multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate. Cyber tools pose a direct threat to security but are also increasingly important facilitators for most forms of organised crime and terrorism".

Cybercrime is understood as "criminal acts committed using electronic communications networks and information systems or against such networks and systems". The term cyber crime is applied to three categories of criminal activities. The first covers traditional forms of crime such as fraud or forgery, though in a cybercrime context relates specifically to crimes committed over electronic communication networks and information systems. The second concerns the publication of illegal content over electronic media. The third includes crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking. Common to each category of crime is that they may be committed on a mass-scale and with a great geographical distance between the criminal act and its effects. Consequently the technical aspects of applied investigative methods are often the same (Communication from the Commission "Towards a general policy on the fight against cyber crime" of 22 May 2007, COM(2007) 267 final).

The Communication from the Commission "Towards a general policy on the fight against cyber crime" of 22 May 2007 and the Justice and Home Affairs Council Conclusions of 8-9 November 2007 expressed strong support to the Council of Europe Convention on Cybercrime in Europe and elsewhere around the world. Furthermore, the Council conclusions of 27 November 2008 on a concerted work strategy and practical measures against cybercrime state that that it is important to combat the various elements of cybercrime and invite the Member States and the European Commission to determine a joint working strategy, taking into account the content of the Council of Europe Convention on Cybercrime.

The Convention[3] is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. The Convention on Cybercrime is the predominant European and international instrument in this field.

The issue of prevention and tackling the cybercrime at the European level was further pursued by the Communication from the Commission of 30 March 2009 COM(2009) 149 final on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

The Internal Security Strategy, adopted by the European Council in February 2010, as well considers cybercrime as one of the main challenges for the internal security of the EU.

[2] The State of Internal Security in the EU, A Joint Report by EUROPOL, EUROJUST, and FRONTEX

[3] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

In 2010 Europol established the European Union Cybercrime Task Force, in order to pursue operational and strategic issues on cybercrime investigations, prosecutions and cross–border cooperation in the fight against cybercrime.

The Communication from the Commission "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" 22 November 2010, COM(2010) 673 final, recognizes cybercrime as a growing threat and, as one of the five strategic objectives includes the task to "Raise levels of security for citizens and businesses in cyberspace". The Action 1: Build capacity in law enforcement and the judiciary, envisages that: "By 2013, the EU will establish, within existing structures, **a cybercrime centre**, through which Member States and EU institutions will be able to build operational and analytical capacity for investigations and cooperation with international partners.". As well: "At national level, Member States should ensure common standards among police, judges, prosecutors and forensic investigators in investigating and prosecuting cybercrime offences.".

Cybercrime Legislation in Croatia

Republic of Croatia has ratified the Council of Europe Convention on Cybercrime adopted by the on 17th October 2002 and it came into power on the 1st July 2004. In accordance with the commitments, amendments related to cybercrime were introduced into the Criminal Code in 2004.

On 26th March 2003 the Republic of Croatia signed the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of racist and xenophobic nature committed through computer systems. Although the Additional Protocol entered into force on 21st June 2008, amendments to the Criminal Code in year 2004 already introduced provisions regarding the offence of racial and other discrimination (art. 174), where the paragraph 4 criminalize denial, significantly diminishing, approval or justification of the criminal acts of genocide or crimes against humanity committed through computer systems.

The new Law on Criminal Procedure, adopted on 15 December 2008, will come into force on the 1st September 2011, but in relation to crimes within the jurisdiction of Office for Suppression of Corruption and Organized Crime it entered into force on the 1st July 2009. Amendments to the Law on Criminal Procedure and provisions which will come into force in September 2011 will greatly contribute to the successful implementation of criminal investigation related to the crimes within the domain of cyber crime, as it'll be possible to use specific evidence gathering measures, including:

1) surveillance and interception of telephone conversations and other means of remote technical communication;
2) interception, gathering and recording of electronic data;
3) entry on the premises for the purpose of conducting surveillance and technical recording at the premises;
4) covert following and technical recording of individuals and objects;
5) use of undercover investigators and informants;
6) simulated sales and purchase of certain objects, simulated bribe-giving and simulated bribe-taking;
7) offering simulated business services or closing simulated legal business;
8) controlled transport and delivery of objects from criminal offences.

As well, it needs to be pointed out that the reform of the entire criminal legislation in Croatia reform of the entire criminal legislation in Croatia is ongoing. Therefore, the Criminal Code shall be further amended to comply with international obligations and modernization on the basis of good practices in other European penal systems, as well with the provisions of the Convention on Cybercrime. Thus, the draft proposes legislative and other solutions related to the ability to prosecute the perpetrators of crimes against the confidentiality, integrity and availability of computer data and systems, criminal acts in connection with computers, in conjunction with the content and in connection with violations of copyrights and related rights, resolving of procedural issues related to search and obtaining of evidences, the powers of police authorities, the Court's jurisdiction, extradition of offenders, mutual cooperation and obligations of Internet services providers.

Also, taking into account the additional protocol to the Convention, along with the existing provisions of Article 106 and 174 of Criminal Code, a new criminal offense under Article 151, along with other incriminating behaviour, now provides the prohibition of using computer system with purpose to expand the material that advocates, promotes or incites racial hatred or discrimination against any individual or group based on differences in race, skin colour, gender, sexual orientation, national or ethnic origin or on the basis on faith differences.

Criminal Police

Republic of Croatia currently does not have a specialized organizational unit to deal with cyber crime.

At the national level cyber crime issues are covering two police officers in the Department of Economic Crime and Corruption, which is a part of the strategic wing of the National Police Office for Suppression of Corruption and Organized Crime. One of these officers is the contact point person for G 24//7 Network, which provides contacts for investigations which involve electronic evidence that require urgent assistance from foreign law enforcement agencies.

The scope of work of National Police Office for Suppression of Corruption and Organized Crime, as a separate organizational unit within the Criminal Police, is suppression of the most complex crimes, particularly crimes of corruption and organized crime. Within this Office are also four regional operating divisions in Zagreb, Split, Rijeka and Osijek, whose task is to conduct police investigations in cases of national-level crime.

At the local level, the Republic of Croatia is divided into 20 Police Administrations which are, depending on the size and population, classified into 4 categories. Depending on the category, in every Police Administration there is a department, division or group for economic crime, where 1-4 police officers are responsible for the issues of computer crime and intellectual property rights protection.

Responsibility for the offences in the area of cyber crime is divided as follows:

- Racial and other discrimination (Art.174 st.4) - Department of Terrorism in cooperation with the Department of Economic Crime

- Child pornography on a computer system or network (Art.197a) - Department of General Crime in cooperation with the Department of Economic Crime

- Breach of confidentiality, integrity and availability of computer data, programs or systems (Art. 223) - Department of Economic Crime

- Computer forgery (Art.223a) - Department of Economic Crime

- Computer Fraud (Art.224a) - Organized Crime Department and the Department of Economic Crime

By systematic monitoring of the problem of computer crime it was found that the most common offence is computer fraud, with growth of 176% in 2010 compared to same period in 2009.

CYBERCRIME CRIMINAL OFFENCES	REPORTED			SOLVED		
	Number of offences		+ -%	Number of offences		+ -%
	2009	2010		2009	2010	
Child pornography on computer systems or networks	30	63	+ 110,0	29	53	+82,8
Breach of confidentiality, integrity and availability of computer data, programs or systems	8	8	0,0	7	8	+ 14,3
Computer forgery	15	27	+80,0	16	27	+68,8
Computer fraud	296	818	+ 176,4	269	800	+ 197,4

In addition to this, the increase of cases of so-called "phishing", theft of identity through the Internet (especially on social networks), unauthorized access to computer systems (hacking), fraud attempts through unsolicited e-mail addresses in the form of so-called Nigerian letters, notices of lottery winnings was also observed.

The continuing growth and development as well as the availability of information and communication technology are enabling the development of these forms of criminal activities, especially in the area of organized crime or activities of organized criminal groups, money laundering and terrorism and it is certainly a growing threat to the Republic of Croatia. Therefore, measures to fight these most serious crimes are also including measures against cyber crime.

Technical equipment

The acquisitions of equipment are regularly planned by annual procurement plans, within the available budget, so in this respect so far the Police National Office for Suppression of Corruption and Organized Crime received equipment for different activities:

Equipment for video surveillance at the Department for Criminal Investigations - Kt&C, Lawmate, Lec, Sim, Ovation Systems, Vtq, Bwa, Ffs, Ceotronics, Samsung, Sony, Canon, Jvc, Nokia, Sony-Ericsson.

Equipment for audio monitoring at the Department for Criminal Investigations - Spectronic, Bea, Ovation Systems, Olympus, Archos, Bwa, Ffs.

Equipment to control of movement and positioning at the Department for Criminal Investigations - Cte International - Microline, Pg Control-Spyfox, Net Hawk.

Special communication equipment - Motorola Tetra radio system

Forensic equipment: programs to recover deleted data from computer - EASEUS Data Recovery Wizard (at all Police Administrations), 4 sets of forensic equipment Portabello Forensic Workhouse (Zagreb, Rijeka, Split and Osijek Police Administrations), laptops with forensic tool EnCase and associated equipment ((Zagreb, Rijeka, Split and Osijek Police Administrations), 3 units for mobile phone forensics Uffed Pysical PRO Ruggedized System (regional PNUSKOK departments except Zagreb).

Objectives

Since the existing capacities of the criminal police are not sufficient to tackle the cybercrime in the adequate way, especially having in mind the trend of the sharp rise of criminal offences in this field, the target of this project is to strengthen administrative capacities of Ministry of Interior to successfully fight against all forms of cybercrime.

The activities and results of the project shall be applied both at the national and the regional level, where the majority of participants of the training activities will be police officers from the regional level.

Forensic Science Centre

Information and communication technology crime (Cybercrime) forensics

It is extremely important that forensic experts and law enforcement officers deal with digital evidence with extreme care, to conduct analysis and expertise and present evidence in a thorough and transparent way. In the process of forensic investigation many computer tools and devices are used to help investigators in the preservation, retrieval and analysis of digital evidence.

Computer forensics is an important field of forensic science, not only because of cybercrime, but as well for processing other criminal cases. Computer security incidents have become daily life and became inevitable. In addition to resolving cases in which criminals take advantage of the weaknesses of computers, computer programs and networks, computer forensic experts use their knowledge in monitoring and detection of other various crimes and their perpetrators. It already became evident that the future of solving criminal cases shall more and more involve the computer forensics and related methods to disclose information about crime.

Furthermore, cybercrime is probably the most transnational of all forms of crime, thus requiring extensive and efficient international cooperation. Offenders are often associated with offenders outside the Republic of Croatia, and it is needed to strengthen the fight against cyber crime at national, European and international level.

Forensic Science Centre

Forensic Science Centre "Ivan Vučetić" (FSC) is a part of the General Police Directorate of the MoI. It provides forensic expertise in the following areas: documents, DNA, drugs, fibres, finger prints, firearms, fire and explosion, handwriting, marks, paint, road accident analysis and when needed crime scene investigations. It is the only institution in the Republic of Croatia that deals with this matter and it provides forensic services also to the Ministry of Justice, the Ministry of Defence, and the Customs.

FSC "Ivan Vučetić" has implemented a quality management system (QMS) according to international ISO 17025 standard for testing and measuring laboratories and since April 2010, has been accredited. The scope of accreditation includes various methods in several groups of forensic science: firearms & toolmarks examinations, gunshot residue analysis, fingerprint development, drugs, DNA, arson and explosives. In 2010 FSC "Ivan Vučetić" FSC prepared and applied additional 30 methods for accreditation.

At this point Forensic Science Centre "Ivan Vučetić" has no established positions for expertise of information and communication technology crime, which represents a serious problem because the number of requests for computer crime expertise, that FSC is receiving, continuously increases and FSC is not able to conduct such expertises.

In order to become able to provide the requested services related to cybercrime, in February 2011 within the FSC were opened 2 additional work places for forensic experts for computer crime[4].

Objectives

The nature of electronic evidence is such that it poses special challenges for its admissibility in court. To meet these challenges, it is an obligation to follow proper forensic procedures. These procedures include, but are not limited to, four phases: collection, examination, analysis, and reporting.

Forensic Science Centre expects from the project substantial assistance in providing training and establishing the operation procedures for cybercrime forensic service in the FSC, in order to prepare to conduct the following:

Computer & Network systems forensics

Methods

[4] Decree on the amendments of the Decree on the internal organization of the Ministry of Interior, Official Gazette 26/11

- The recovery of information (clones, images, etc), undeletion and recovery of deleted and hidden files and parts of files; searching recovered information for keywords, documents, evidence of ownership etc.

- Sequencing the events that have occurred within a computer to determine if a particular act occurred before another.

- Examination of other common everyday items containing digital data (e.g. air-bag systems, fax machines. Copying devices, etc.)

- Reading and deciphering magnetic stripes on plastic cards and analysis of smart cards

- intrusion detection and unauthorized access to networks (LAN, wireless, etc.) including searching for various Internet activity

Applicable on

- various computer hard disks, USB drives, smart media, flash memory, floppy discs and other storage media such as Zip, Jaz or Optical disks, Tapes and CD-ROMs including a variety of different computer operating systems

- computer peripheral devices (such as tape streamers, removable hard disks etc.) and other devices with digital storage capability (e.g. cameras, various consumer goods)

- line telephone, fax-machines, air-bag systems, copying devices,

- magnetic cards, smart cards, etc.

- Server logs data, IPS (Internet service providers) logs data

Mobile devices forensics

Methods

- Recovery of information, undeletion and recovery of deleted and hidden files and parts of files from mobile devices, smartphones, PDAs, GPS devices and other portable (embedded systems) or office technology.

- Identification and analysis of mutual communication in space and time using data from telecommunication network systems

- Establish the functionality of a piece of software or a machine e.g. could a system be used for phone cloning

Applicable on

- mobile devices, smartphones, PDAs, GPS devices and other portable (embedded systems) or office technology

- other unknown electronic devices

Video & Audio Forensics

Methods

- Enhancement and de-multiplexing of digital videotape to produce footage which can be used for identification or presentation purposes
- Applying image processing techniques to enable the removal of interfering background from items, such as bank notes, bearing fingermarks
- Applying digital processing techniques to enhance audio

Applicable on

- Various media for digital video storage (CDs, DVDs, etc)
- All kind of digital images
- Various media for digital video storage (CD, DVD, audio recorders, mobile devices)

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

Project impact:

The project will have major impact on enhancing and strengthening the combat against cybercrime with up-to-date practices, methods and well-trained police officers in line with EU policies and strategies.

Thus, the project will have a positive effect on fulfilling requirements for Croatia's accession to the EU and subsequent operation within the EU Justice, Freedom and Security framework.

Catalytic effect:

The project will enhance the administrative and investigative capacities of Croatian Ministry of Interior and will make a positive effect on the process of investigations, national and international cooperation among law enforcement agencies and process of the judicial services especially against cyber crime

Sustainability:

The Ministry of Interior will provide for the effective implementation of the project and will guarantee the sustainability of efforts.

Cross border impact:

In January 2011 Europol issued an iOCTA (Internet facilitated Organised Crime Threat Assessment) which states:

„Cybercrime is borderless by nature. For measures to combat cybercrime to be effective, adequate cross-border provisions are needed and the international cooperation and mutual assistance in law enforcement within Europe and between the EU and third countries needs to be substantially enhanced.„

Enhancing of its capacities to combat cybercrime shall as well enable Croatian Ministry of Interior to give higher contribution to the international cooperation in this field.

3.3. Results and measurable indicators:

Component I – Forensic Science Centre

Results	Measureable Indicators
1. Forensic Science Centre experts for computer crime enabled to provide cybercrime forensic services	• 2 employees of FSC trained
2. Training programme for experts including issues of collection, examination, analysis and reporting of electronic evidence	• Training modules delivered
3. Standard Operation Procedures for collection, examination, analysis, and reporting of electronic evidence	• Standard Operation Procedures delivered

Component II – Criminal Police Directorate

Results	Measureable Indicators
1. Enhanced administrative capacities of the criminal police to fight cybercrime at the national, regional, European and international level	• At least 30 police officers trained[5] • Project recommendations applied
2. Established training modules and manuals for Police Academy for further continuous education of police officers in the field of cybercrime	• Training modules and manuals delivered

3.4. Activities:

Component I – Forensic Science Centre

Contract: 1 – Twinning

[5] Beside police officers from PNUSKOK headquarters there will be trained at least 20 police officers from PNUSKOK regional departments and police administrations

1.1 Capacity building for forensic science officers on collection, examination, analysis and reporting of electronic evidence according to recommended procedures of ENFSI (European Network of Forensic Science Institute)

1.1.1 Assessment of training needs

1.1.2 Designing a training programme and producing/compiling training materials

1.1.3 Drafting the operation plan for training of forensic science experts

1.1.4 Traineeship for 2 forensic science experts in the MS forensic science services (duration 10 weeks)

1.1.5 Practical implementation of learned techniques in BC under supervision of MS expert/s

1.1.6 Guidelines for cybercrime forensic science operating procedures

1.1.7 Final report and recommendations

Input – twinning contract

Component II – Criminal Police Directorate

Contract: 1 – Twinning

1.2 Designing the organisational model for improvement of Criminal Police administrative capacities to combat cybercrime

1.2.1 Analysis of the existing administrative capacities

1.2.2 Study visit to MS cybercrime investigation services (3 persons)

1.2.3 Drafting the organisational model

1.2.4 Presentation of the proposed organisational model to the General Police Directorate management

1.2.5 Final report and recommendations

1.3 Capacity building for criminal police officers on investigating cybercrime

1.3.1 Assessment of training needs

1.3.2 Designing a training programme and producing/compiling training materials

1.3.3 Drafting of the operation plan for implementation of the training

1.3.4 Implementation of the training programme (workshops, internships)

1.3.5 Guidelines for cybercrime investigation

1.3.6 Final report and recommendations

1.4 Developing capacities of the Police Academy to provide training on combating cybercrime

1.4.1 Assessment of the existing training capacities regarding cybercrime

1.4.2 Designing a training programme and producing/compiling training materials

Input – twinning contract

3.5 Conditionality and sequencing:

Implementation of the project requires full commitment and involvement on behalf of the beneficiary institution. Therefore, the Ministry of Interior commits itself to provide adequate staff for all necessary activities for the successful implementation of the project.

The Ministry of Interior already has in place all the structures for preparation and implementation of the project, including the staff with experience from previous CARDS, Phare and IPA projects.

3.6 Linked activities

- The IPA 2009 HR2009-01-36-01 national programme, entitled "Capacity Building in the Field of Fight against Sexual Exploitation and Sexual Abuse of Children, and on Police Assistance to Vulnerable Crime Victims" has a significant "cyber crime" dimension, related to child pornography.
- Republic of Croatia is a participant of IPA Regional Programme 2010 Strengthening capacities in the fight against cybercrime, which comprises a component to train cybercrime units.

The project has started in November 2010 and its main objective is to enhance the ability of countries of Western Balkan and Turkey to prevent and control cybercrime as well as strengthen the capacities to cooperate effectively against cybercrime.

Regional training meetings, workshops, conferences, training the trainer courses and all other aspects of training provided within this project will be also used as a benefit in strengthening capacities in fight against cybercrime.

3.7 Lessons learned

Results of the previous EU financed projects were very helpful for the Ministry of Interior providing significant assistance in the process of reaching the EU standards in the area of justice and home affairs. Results of these projects have been facilitating Croatia’s efforts regarding fulfilling all the requirements for the EU membership and building readiness for operating and cooperating within the EU Justice, Freedom and Security framework.

4. Indicative Budget (amounts in EUR)

					SOURCES OF FUNDING								
			TOTAL EXP.RE	TOTAL PUBLIC EXP.RE	IPA COMMUNITY CONTRIBUTION		NATIONAL PUBLIC CONTRIBUTION					PRIVATE CONTRIBUTION	
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	X	–	700 000		665 000	95	35 000	5	35 000	-	-	-	–
TOTAL IB			700 000		665 000	95	35 000	5	35 000				
TOTAL PROJECT			**700 000**		665 000	**95**	35 000	**5**	35 000				

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	3 Q 2012	1 Q 2013	2 Q 2014

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

Based on the fundamental principles of promoting equality and combating discrimination, as provided in Croatia's legislation and practice, participation in the project will be guaranteed on the basis of equal access regardless of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.

6.2. Environment

Not applicable

6.3. Minorities

Not applicable

ANNEXES

1- Log frame in Standard Format

2- Amounts contracted and Disbursed per Quarter over the full duration of Programme

3- Description of Institutional Framework

4 - Reference to laws, regulations and strategic documents:

Reference list of relevant laws and regulations

Reference to AP /NPAA / EP / SAA

Reference to MIPD

Reference to National Development Plan

- Not applicable

Reference to national / sector investment plans

5- Details per EU funded contract (*) where applicable:

For *twinning covenants*: account of tasks expected from the team leader, resident twinning advisor and short term experts

ANNEX I: Logical framework matrix in standard format

Strengthening capacities of the Ministry of the Interior to combat computer crime	Programme name and number IPA 2011	
Ministry Of Interior	Contracting period expires: 3 years following the date of conclusion of the Financing Agreement	Disbursement period expires: 4 years following the end date for contracting
	Total budget: EUR 700 000	**IPA budget: EUR 665 000**

Overall objective	**Objectively verifiable indicators**	**Sources of Verification**	
To enhance capacities of the Ministry of Interior to combat cybercrime within the EU and international environment, in line with the related European policies and strategies	• successful solving of cybercrime cases	• Regular EC and Croatian reports	
Project purpose	**Objectively verifiable indicators**	**Sources of Verification**	**Assumptions**

Component I – Forensic Science Centre • To develop the capacities of the Forensic Science Centre (FSC) to provide support to investigating cybercrime, as well as the expertise and evidence for processing and prosecuting of such criminal offences, following the best practices of the EU Member States Component II – Criminal Police Directorate • To enhance the capacities of the Criminal Police to investigate cybercrime, including the ability to exchange information and cooperate with the relevant law enforcement agencies of other countries and to operate in line with the EU anti-cybercrime initiatives.	• MoI applying procedures in line with the European policy and the best practices of the EU Member States	• MoI reports • EC reports	• Full commitment of the MoI to fight cybercrime • Efficient cooperation and co-ordination of the principal actors • Recommendations of the project applied

Results	Objectively verifiable indicators	Sources of Verification	Assumptions
Component I – Forensic Science Centre		• Project reports	• All necessary preconditions for implementation met
1. Forensic Science Centre experts for computer crime enabled to provide cybercrime forensic services	• 2 employees of FSC trained		
2. Training programme for experts including issues of collection, examination, analysis and reporting of electronic evidence	• Training modules delivered	• Project reports	
3. Standard Operation Procedures for collection, examination, analysis, and reporting of electronic evidence	• Standard Operation Procedures delivered		
		• Project reports	
Component II – Criminal Police Directorate			
1. Enhanced administrative capacities of the criminal police to fight cybercrime at the national, regional, European and international level	• At least 30 police officers trained • Project	• Project reports • EC and Croatian reports	

2. Established training modules and manuals for Police Academy for further continuous education of police officers in the field of cybercrime	recommendations applied • Training modules and manuals delivered	• Project reports • EC and Croatian reports	

Activities	**Means**	**Costs**	**Assumptions**
1.1 Capacity building for forensic science officers on collection, examination, analysis and reporting of electronic evidence according to recommended procedures of ENFSI	Twinning	Twinning: EUR 700 000 Total: EUR 700 000	• Full commitment of the MoI • Organisational, technical and infrastructure capacities necessary for implementation of the project in place • Human resources for the implementation of the project in place
1.1.1 Design a training needs	Twinning		
1.1.2 Designing a training programme and producing/compiling training materials	Twinning		
1.1.3 Drafting of the operation plan for implementation of the training	Twinning		
1.1.4 Traineeship for 2 forensic science			

experts in the MS forensic science services (duration 10 weeks)	Twinning		
1.1.5 Practical implementation of learned techniques in BC under supervision of MS expert/s	Twinning		
1.1.6 Guidelines for cybercrime forensic science operating procedures	Twinning		
1.1.7 Final report and recommendations	Twinning		
1.2 Designing the organisational model for improvement of Criminal Police administrative capacities to combat cybercrime	Twinning		
1.2.1 Analysis of the existing administrative capacities	Twinning		
1.2.2 Study visit to MS cybercrime investigation	Twinning		

services (3 persons) 1.2.3 Drafting the organisational model 1.2.4 Presentation of the proposed organisational model to the General Police Directorate management 1.2.5 Final report and recommendations 1.3 Capacity building for criminal police officers on investigating cybercrime 1.3.1 Assessment of training needs 1.3.2 Designing a training programme and producing/compiling training materials 1.3.3 Drafting the operation plan for implementation of the training 1.3.4 Implementation of the training programme (workshops, internships) 1.3.5 Guidelines for	Twinning Twinning Twinning Twinning Twinning Twinning Twinning Twinning		

cybercrime investigations 1.3.6 Final report and recommendations 1.4 Developing capacities of the Police Academy to provide training on combating cybercrime 1.4.1 Assessment of the existing training capacities regarding cybercrime 1.4.2 Designing a training programme and producing/compiling training materials	Twinning Twinning Twinning Twinning		

Pre conditions:

ANNEX II: amounts (in €) Contracted and disbursed by quarter for the project

Contracted	**4Q/2012**	**1Q/2013**	**2Q/2013**	**3Q/2013**	**4Q/2013**	**1Q2014**	**2Q2014**				
Twinning		700 000									
Cumulated		700 000									
Disbursed											
Twinning							700 000				
Cumulated							700 000				

**

ANNEX III: Description of Institutional Framework

Ministry of Interior

At the national level in the Department of Economic Crime and Corruption, which is part of the strategic wing of the National Police Office for Suppression of Corruption and Organized Crime, is covering cyber crime issues.

At the local level, the Republic of Croatia is divided into 20 Police Administrations, which are depending on the size and population divided into 4 categories. Depending on the category, in every Police Administration there is Department, Division or Group for economic crime, consisting of 1-4 police officers responsible for the problems of computer crime and intellectual property rights protection.

Forensic Science Centre "Ivan Vučetić" (FSC) is a part of the General Police Directorate of the MoI. It provides forensic expertise in the following areas: documents, DNA, drugs, fibres, finger prints, firearms, fire and explosion, handwriting, marks, paint, road accident analysis and when needed crime scene investigations. It is the only institution in the Republic of Croatia that deals with this matter and it provides forensic services also to the Ministry of Justice, the Ministry of Defence, and the Customs.

In order to become able to provide the services related to cybercrime, in February 2011 within the FSC were opened 2 work places for forensic experts for computer crime.

ANNEX IV:

Reference list of EU and international documents:

- Convention on Cybercrime, CETS No.: 185, Council of Europe
- Additional Protocol to the Convention on cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems
- UN General Assembly Resolution 58/199 Creation of a global culture of cybersecurity and the protection of critical information infrastructures
- Communication from the Commission "Towards a general policy on the fight against cyber crime" of 22 May 2007, COM(2007) 267 final
- Conclusions of the Justice and Home Affairs Council Meeting of 8-9 November 2007
- Conclusions of the Justice and Home Affairs Council Meeting of 27-28 November 2008

- Communication from the Commission on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" of 30 March 2009 COM(2009) 149 final
- Internal Security Strategy for the European Union "Towards a European Security Model", Council Document, 5842/2/2010
- Communication from the Commission "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" 22 November 2010, COM(2010) 673 final

Reference list of relevant Croatian law and regulations:

- Criminal Code, Official Gazette 110/97, 27/98, 129/00, 51/01, 11/03, 105/04, 84/05, 71/06,110/07, 152/08, 76/09
- Law on Criminal Procedure, Official Gazette 152/08, 76/09
- Decree on the amendments of the Decree on the internal organization of the Ministry of Interior, Official Gazette 26/11

Reference to AP/NPAA/EP/SAA:

- Croatia 2010 Progress Report, http://ec.europa.eu/enlargement/pdf/key_documents/2010/package/hr_rapport_2010_en.pdf
- Communication from the Commission to the Council and the European Parliament "Enlargement Strategy and Main Challenges 2010-2011", http://ec.europa.eu/enlargement/pdf/key_documents/2010/package/strategy_paper_2010_en.pdf

Reference to MIPD 2009 – 2011 under component I

- Instrument for Pre-Accession Assistance (IPA) Multi-annual Indicative Planning Document (MIPD) 2009-2011 for Republic of Croatia, http://ec.europa.eu/enlargement/pdf/mipd_croatia_2009_2011_en.pdf

ANNEX V:

The project includes one twinning contract amounting to EUR 700 000.

Profile of the Project Leader

Requirements:

- University degree
- Minimum 10 years experience in law enforcement
- Experience in suppression of cybercrime
- Fluency in written and spoken English language
- Proven contractual relation to public administration or mandated body, as defined under Twinning manual 5.3.2.
- Experience in project management

Additional assets are:

- Experience in implementation of EU standards in Candidate Countries;
- Experience with EU twinning projects;

Tasks of the Project Leader:

- Participation in Steering Committee meetings
- Project reporting
- Ensuring backstopping and financial management of the project in the MS
- Supervising and coordinating implementation of the project
- Participation in coordination of deployment of short-term experts
- Overall responsibility, coordination and direction of the MS TW partner inputs

Profile of the Resident Twining Adviser

Requirements:

- University degree
- Minimum 10 years experience in law enforcement;
- Experience in suppression of cybercrime
- Experience in project management;
- Working level of English language
- Proven contractual relation to public administration or mandated body, as defined under Twinning manual 5.3.2.

Assets:

- Experience in advanced investigation methods
- Experience in organizing and conducting training programmes.

Tasks of the Resident Twining Adviser

- Day to day management of the project in the Beneficiary institution
- Advising on related EU policies and best practices, legislation and regulations;
- Monitoring project implementation and, if needed, proposing corrective management actions;
- Support and coordination of all activities in the BC;
- Organization of visibility events (kick-off and final event);
- Networking with stakeholders of the project in Croatia and in MS.

Profile of the Short-term experts

Requirements:

University degree

- Minimum 5 years experience in the police force
- Experience in cybercrime investigations
- Fluency in written and spoken English language
- Proven contractual relation to public administration or mandated body, as defined under Twinning manual 5.3.2.

Assets:

- Experience in implementation of EU standards in Candidate Countries;
- Experience with EU twinning projects;

Tasks of the Short-term experts:

- Drafting analyses;
- Drafting the documents as required by the project fiche;
- Conducting the trainings