ANNEX C1: Twinning Fiche

Project title: Strengthened capacities (human and legal) of Criminal Police Department and Special Prosecution Office for Combating High-Tech Crime and public awareness

Beneficiary administration: Ministry of Interior of the Republic of Serbia

Twinning Reference: SR 17 IPA JH 01 21

Publication notice reference: EuropeAid/172578/ID/ACT/RS

EU funded project

TWINNING TOOL

LIST OF ABBREVIATIONS

AFCOS – Anti-Fraud Coordination Service

AML - Anti-Money Laundering

AML/CFT - Anti-Money Laundering/Countering the Financing of Terrorism

APML- Administration for the Prevention of Money Laundering

ARO - Asset Recovery Office

CA - Contracting Authority

CAS - Crime Analysis Service

CEPOL – The European Union Agency for Law Enforcement Training

CFCU - Department for Contracting and Financing of EU Funded Programmes

CFT - Countering the Financing of Terrorism,

CSO – Civil Society Organisation

EC – European Commission

EU- European Union

FATF - Financial Action Task Force

FIU - Financial Intelligence Unit

HJC –HighJudicial Council.

IPA – Instrument for Pre-Accession Assistance

IT- Information Technology

MoI - Ministry of Interior

MS – Member State

NPAA - National Plan for the Adoption of the*Acquis*

NPO – Non Profit Organisations

PSC - Project Steering Committee

SAA- Stabilisation and Association Agreement

SIENA- Secure Information Exchange Network Application

SCOC - Service for Combating Organized Crime

SOCTA - National Serious and Organised Crime Threat Assessment

TNA – Training Need Analysis

ToT – Training of trainers

1. Basic Information

1.1. Programme: EU Integration Facility IPA 2017, (indirect management, with ex-ante control).

Please be aware that following the entry into force of the AU-UK Withdrawal Agreement[1] on 1 February 2020 and in particular Articles 127(6), 17 and 138, the references to natural or legal persons residing or established in a Member State of the European Union and to goods originating from an eligible country, as defined under Regulation (EU) No 236/2014[2] and Annex IV of the ACP-EU Partnership Agreement[3], are to be understood as including natural or legal persons residing or established in, and to goods originating from, the United Kingdom[4]. Those persons and goods are therefore eligible under this call.

1.2 Twinning Sector: Justice and Home Affairs (JH)

1.3 EU funded budget: 1.000.000 EUR

1.4 Sustainable Development Goals (SDGs): SDG 16 Peace, Justice and Strong Institutions: Inclusive societies, strong institutions and equal access to justice

2. Objectives

2.1 Overall Objective

To contribute to meeting the EU accession requirements under Chapter 24 of the *Acquis* – Justice, freedom and security and to contribute to strengthening legislative framework and institutional capacities, for fulfilling the requirements of EU membership.

2.2 Specific objective

To strengthen capacities of Criminal Police Directorate, Service for combating organized crime, Department for Combating High-Tech Crime and Special Prosecution Office for High-Tech Crime

2.3 The elements targeted in strategic documents i.e. National Development Plan/Cooperation agreement/Association Agreement/Sector reform strategy and related Action Plans

Links to EU Strategic documents

- Stabilisation and Association Agreement (SAA). The Stabilization and Association Agreement (Article 84), states: 1. "The Parties shall cooperate in order to prevent the use of their financial systems and relevant non-financial sectors for laundering of proceeds from criminal activities in general and drug offences in particular, as well as for the purpose of financing terrorism; 2. Cooperation in this area may include administrative and technical assistance with the purpose of developing the implementation of regulations and efficient functioning of the suitable standards and mechanisms to combat money laundering and financing of terrorism equivalent to those adopted by the Community and international fora in this field, in particular the Financial Action Task Force (FATF)".

[1] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community.
[2] Regulation (EU) No 236/2014 of the European Parliament and of the Council of 11 March 2014 laying down common rules and procedures for the implementation of the Union's instruments for financing external action.
[3] Anexx IV to the ACP-EU Partnership Agreement, as revised by Decision 1/2014 of the ACP-EU Council of Ministries (OJ L196/40, 3.7.2014.)
[4] Including the Overseas Countries and Territories having special relations with the United Kingdom, as laid down in Part Four and Annex II of the TFEU.

- EC Progress report 2020 stated that on cybercrime, convictions were rendered against 49 individuals (first instance). The operational capacity within the police to effectively address cybercrime was strengthened, including through the establishment of special investigative units which deal with abuse of credit cards, e-commerce and e-banking and suppress illegal and harmful content on the internet. Staff in the cybercrime department increased (from 15 to 22). The EC Progress report noted also that Serbia's cybercrime strategy, adopted in late 2018, is being implemented.
- Moneyval Report. In light of Serbia's progress in strengthening its framework to tackle money laundering and terrorist financing since its mutual evaluation report in April 2016, Moneyval has re-rated in February 2019 the jurisdiction on ten Recommendations, nine of which were originally rated "partially compliant" or "non-compliant". The Financial Action Task Force (FATF) decided at its plenary meeting held from 16 to 21 June 2019 that Serbia will no longer be subject to the FATF's monitoring under its ongoing global anti-money laundering and counter-terrorist financing (AML/CFT) compliance process (the so called "grey list").
- **The Revised Indicative Strategy Paper for Serbia (2014-2020)** indicates "as concerns money laundering, there is lack of analytical capacities to systematically identify suspicious cases, and a need for an effective system for monitoring and analysing cash transactions".In the area of organised crime, support will be provided for strengthening strategic framework, inter-agency cooperation and capacities to implement an integrated approach."
- **EU – Western Balkan flagship initiative to reinforce engagement on security.** Through six flagship initiatives, the Western Balkans Strategy sets out the EU's unprecedented support to the transformation process in the Western Balkans, targeting specific areas of interest for both the EU and the Western Balkans countries. Concerning "engagement on security", this initiative will focus on "Reinforced cooperation on fighting organised crime, countering terrorism and violent extremism and on border security."
- **The New EU Cybersecurity Strategy in Digital Decade** was adopted on 16 December 2020. The new Cybersecurity Strategy allows the EU to step up leadership on international norms and standards in cyberspace, and to strengthen cooperation with partners around the world to promote a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values. The new Cybersecurity Strategy aims to safeguard a global and open Internet, while at the same time offering safeguards, not only to ensure security but also to protect European values and the fundamental rights of everyone. Building upon the achievements of the past months and years, it contains concrete proposals for regulatory, investment and policy initiatives, in three areas of EU action:1- Resilience, technological sovereignty and leadership, 2-Building operational capacity to prevent, deter and respond, 3-Advancing a global and open cyberspace through increased cooperation.
- **The EU Security Union Strategy for the period from 2020 to 2025.** On 24 July 2020, the European Commission set out a new EU Security Union Strategy for the period from 2020 to 2025. It maps out the main actions, tools and measures to ensure European security, both in the physical and digital world, and across all parts of society. The COVID-19 pandemic has opened new avenues for cyber criminals and has rendered people more susceptible to violent extremist discourses online. It has further showed the need to protect, both in the physical and digital environments.EU countries cannot address these threats effectively acting on their own. This is why, at EU level we need to build the tools, infrastructure and environment in which national authorities can and do work together effectively to tackle shared challenges.The new way forward on internal security as part of the Security Union Strategy replaces the previous security strategy set out in the European Agenda on Security (2015-

2020)**.** Building on the previous work of the Commission, the Council and the Parliament, the Security Union Strategy puts citizens at the centre of the approach and focuses on three priority areas: 1-Fighting organised crime and human trafficking, 2-Countering terrorism and radicalisation, 3- Fighting cybercrime

- **The first EU Cyber Defence Policy Framework dates back to 2014. The latest update was released in 2018**. **The EU Cyber Defence Policy Framework** from 2014 is one of the main documents that specifically address these issues. It serves as groundwork for countering threats arising from cyberspace. The 2018 update to the Cyber Defence Policy Framework identifies several priorities: the development of cyber defence capabilities, the protection of the EU CSDP communication and information networks; training and exercises; research and technology; civil-military cooperation and international cooperation.
- **SoutheastEurope Strategy 2020** indicates that the need to counter corruption is essential to the broad goal of promoting growth, since corruption is a major deterrent to investment.
- **The European Strategy for a Better Internet for Children** (2016) aims to establish a safe online environment to give children the digital skills and tools they need to fully and safely benefit from being online
- Regulation (EC) no. 460/2004 repealed by Regulation (EU) no. 526/2013 established the **European Network and Information Security Agency (ENISA),** the core organisation on the EU level in the area of implementing measures in CS/IS, cooperation among the countries and reacting on concrete issues in this field.
- **Strategy for incident response and cyber crisis cooperation, published in August 2016** - a high-level summary of the basics of incident response, focusing on the work of Computer Security Incident Response Teams (CSIRTs).
- Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, **the European Programme for Critical Infrastructure Protection (EPCIP).**
- **Directive 2013/40/EU of the European Parliament and of the Council** on attacks against information systems

Links with other international documents

- **Council of Europe Convention on Cybercrime (CETS 185)** with additional Protocol on Xenophobia and Racism (ETS 189)
- **The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)** (also called the Lanzarote Convention) represents the most advanced and comprehensive standard in this field. The Lanzarote Convention has been signed and ratified by 40 states including all Western Balkans countries.
- **The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS no.108)** is signed by 47 states, including Western Balkan countries. The objective of this convention is to strengthen data protection and the legal protection of individuals with regard to the automatic processing of personal information relating to them.
- **UN Resolution 2462 (2019)** adopted by the Security Council at its 8496 meeting on 28 March 2019.
- **Consolidated FATF Strategy on Combating Terrorist Financing, FATF**

Links with national strategic documents and national legislation National Strategies

- **The Action Plan for Chapter 24.** The ongoing reform processes in Home affairs sector are translated into the steps to be taken and envisaged in the detailed Action plan for Chapter 24. This contract is in line with activities of the revised Action Plan

for Chapter 24 related to strengthen capacities for fight against organized crime, financial investigation and fight terrorism financing.

- **The Action Plan for Chapter 23.** This project will contribute to the revised Action Plan Chapter 23, namely to activities related to fight against corruption. The project will all also contribute to strengthen capacities of judiciary, prosecutors and High Judicial Council (HJC).
- **The National Plan for the Adoption of the*Acquis* (NPAA)** - http://www.mei.gov.rs/npaa_eng__2014_2018.pdf
- **Strategy for development of Information security 2017-2020** adopted 25 May 2017 – This Strategy includes the State's readiness to face the global challenge of data protection, information systems, as well as achieving greater citizen security in the digital environment.
- **National Priorities for International Assistance 2014-17with projections to 2020**. This project is in line with defined following priority within the Home affairs sector: Priority 1: Improving the overall security and fight against crime. Measure 1.2: Strengthening the capacities of state authorities to efficiently process cases of organised crime, corruption, money laundering, terrorism financing, terrorism, war crimes and other criminal acts. This project is also in line with priorities related to the Justice Sector: Improving judicial system, legal certainty and fight against corruption. Measure 1.2: Further supporting the reform of the judicial system in line with the EU accession requirementsand Measure 1.3.: Improving anticorruption policy in line with enhancing prevention, prosecution and processing of corruption cases.
- **Strategy for combating terrorism (2017-2021),** adopted in October 2017(„Official Gazette of the Republic of Serbia“, n°.55/05, 71/05 –101/07, 65/08, 16/11, 68/12 – US, 72/12, 7/14 – US and 44/14).
- **Strategy for development of Informationsecurity 2017-2020** adopted 25 May 2017 – ThisStrategyincludes the State's readiness to face the global challenge of data protection, information systems, as well as achieving greater citizen security in the digital environment.(http://www.srbija.gov.rs/vesti/dokumenti_sekcija.php?id=45678)
- **Cybercrime strategy for 2019-2023.-** („Official Gazette of the Republic of Serbia”, 05 Num: 23-8630/2018) - http://arhiva.mup.gov.rs/cms_cir/decaipolicija.nsf/Strategija%20za%20borbu%20protiv%20visokotehnolo%C5%A1kog%20kriminala%20(2019%20-%202023)
- **Strategy for combating terrorism (2017-2021),** adopted in October 2017 - http://www.srbija.gov.rs/vesti/dokumenti_sekcija.php?id=45678
- **The Strategic Police plan 2018-2021** The Strategic Police plan covers also the area of fight against organized crime. Both documents are in synergy.
- **National Serious and Organised Crime Threat Assessment (SOCTA)** has been developed and is a basis for the selection of priorities and the adoption of strategic and operational decisions.
- **National Strategy against Money Laundering and the financing of terrorism, 2014-2019-** Pursuant to Article 45(1) of the Law on Government (Official Gazette of RS, No 55/05, 71/05 – corr., 101/07, 65/08, 16/2011, 68/2012 – CC decision, 72/2012, 7/2014 – CC decision and 44/2014 - https://www.legislationline.org/download/id/6049/file/Serbia_national-aml-cft-strategy-2014_en.pdf
- **Negotiation position of the Republic of Serbia for the Intergovernmental Conference on the Accession of Serbia to the European Union Chapter 32** „Financial control“, July 2014.
- **Law on ratification of Convention on Cybercrim**e (Official Gazette RS, No. 19 dated March 19th 2009)

3. Description

3.1. Background and justification:

a) Key relevant legislation

A set of legal acts were adoptedin order to achieve provisional harmonization with the EU standards:

- Law on ratification of Convention on Cybercrime (Official Gazette RS, No. 19/2009)
- Law on the Organization and Competences of State Authorities for Combating High-Tech Crime (Official Gazette of the Republic of Serbia No 61/2005 and 104/2009)
- Criminal Procedure Code ("Official Gazette of the Republic of Serbia", No. 72/11, 101/11, 121/12, 32/13, 45/13 and 55/14).
- The Law on Police, adopted by the National Assembly of the Republic of Serbia in 2016
- The Law on Seizure and Confiscation of Proceeds of Crime (Official Gazette of the Republic of Serbia 2009)
- The Convention on Laundering, Search, Seizure and Confiscation of Proceeds of Crime and on the Financing of Terrorism ("Official Gazette of theRepublic of Serbia ", No. 19/
- The Law on records and data processing (Official Gazette of the Republic of Serbia 24/2018 – art 24)
- The Law on Government ("Official Gazette of the RS", No. 55/05, 71/05 – correction, 101/07, 65/08, 16/11, 68/12 – CC, 72/12, 7/14 – CC and 44/14), Article 45, Paragraph 1.
- Decision on Cash Flow Management ("The Official Gazette of theRepublic of Serbia ", No. 60/2012, 64/2013 and 115/2013)

b) Institutional framework in the sector

The beneficiaries of the project are:
The Ministry of Interior (MoI), The Criminal Police Directorate (Service for Combating organized crime), Department for Combating High-Tech Crime, Republic Public Prosecution Office (RPPO), Special Prosecution Office for High-Tech Crime.

The sector lead institution for the HA sector is the Ministry in charge of Interior. It has the main responsibility of leading the relevant sector institutions in the process of elaborating, implementing, monitoring/reporting on sector policies.

c) Situation analysis

Cybercrime has become a global phenomenon, hand in hand with the economic, technological and social progress facilitated by the global interconnectedness of the Internet. Furthermore, the pervasive use of technology in our everyday life has also increased the number of cases where electronic evidence is key to prove or disapprove a fact in court. **Criminal activities committed through the use of Internet impact countries and communities on multiple fronts and with dire and diverse consequences: from the individualloss of privacy, social and professional victimisation, to loss of personal funds, to sustained attacks on a country's infrastructure and informational systems.**
« In a world where more than 4.5 billion people are online, more than half of humanity is at risk of falling victim to cybercrime at any time » and « Information is the key enabler that can bring us together and make us stronger in the fight against cybercrime »indicates Interpol. In addition, recent findings from 2020 have made clear that cybercriminals around the world have been able to capitalize on the global COVID-19 pandemic, turning the health crisis into an opportunity. The pandemic has accelerated the digital transformation and increased our

reliance on connectivity and digital tools. With rapid developments in the global cyber landscape, closer collaboration between law enforcement and the public and private sectors to deal with the ever-changing nature of cybercrime has become increasingly pressing.Victims of cybercrime do not always realize they should report these crimes to police in the same way they would if, for example, their home was robbed. The following online crimes, which have been identified as the key global threats, will be covered : Phishing, Ransomware, Sextortion, Cryptojacking, Business email compromise (BEC) fraud, Online crimes against children, sexual abuse of minors and children for pornographic purposes on the Internet, Criminal offences in which information and communication technologies are abused are increasing, as a consequence of the rapid development of IT technology, such as those related to the security of computer data, crimes in relation to cryptocurrencies, fraud via the Internet, unauthorized use of copyright and related rights, threats to security, terrorism and violent extremism leading to terrorism.
Serbia has ratified and implemented **the Council of Europe Convention on Cybercrime (Budapest Convention)**[5]in 2009 (but should further align its legislation with Directive 2013/40/EU on attacks against information systems. **Serbia should develop a coherent strategic and long-term vision on how it intends to address cyber-criminality, including on-line child sexual abuse, in line with the EU strategic and operational approach against cybercrime.**The EU common position also notes that cyber criminality is becoming an increasing problem in Serbia and that Serbia has so far not developed a strategic vision on how to address this. In this area, Serbia has no long-term strategy; the level of inter-agency cooperation, information flow and exchange between law enforcement agencies needs to be further improved.

The legal mechanisms to fight cybercrime are in place. The Criminal Code provides norms on criminal offences in accordance with legal frameworks of the CoE and the EU. **While legislation on cybercrime, electronic evidence and search, seizure and confiscation of online crime proceeds was strengthened considerably in the recent years, further reform is needed to allow for effective cybercrime investigation and prosecution in the light of the latest technological developments as well as the fast changing pace of the modus operandi of cybercrime.** Serbia started to implement the new economic chapter of the criminal code and the Law on organisation and jurisdiction of state authorities in the fight against organised crime, terrorism and corruption and adopted a cybercrime strategy for 2019-2023. It aims, among other things, at strengthening Serbia's institutional capacity, and thus envisages the creation of specialised 33 units within the Security Information Agency, the military police and the customs office, as well as the reinforcement of existing units with the MoI. Cybercrime appears to be related to financial crime too. Efforts to investigate wider criminal networks and to process money-laundering cases still need to be stepped up. Some progress was made through strengthening the legal framework to address money laundering.
The level of inter-agency cooperation, information flow and exchange between law enforcement agencies needs to be further improved. However, internal cooperation between the police and the special prosecutor's office for cybercrime is improving. Serbia participates also to regional Western Balkans initiatives and projects to fight Cyber-crime (concerning EU funded regional projects, there is the IPA project titled "Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime" and iPROCEEDS is another joint project of the EU and the CoE implemented under the umbrella of the IPA II Multi-country action programme 2014. The beneficiaries are the same as in the CyberCrime@IPA project with the exception of Croatia (since it has in the meantime joined the EU).

According to the **Cybercrime Strategy for 2019-2023**, Serbia will establish several units within the police, military and customs to fight online crimes. The strategy is a continuation and expansion of activities aimed at strengthening the efficiency of all entities in the field of

[5]https://www.coe.int/fr/web/cybercrime/the-budapest-convention

suppression of high-tech crime. The document, which covers the period between 2019 and 2023, says that by 2020, Serbia will form anti-cybercrime units within the intelligence agency, the BIA, Military Police and Customs Bureau, and also employ more people in existing units with the police. It also added that Serbia will purchase new IT equipment but also specialised software for the police and prosecution. It states that Serbia will also adopt operational procedures to collect and provide electronic evidence. In accordance with the Strategy civil servants will participate in training, which will be also held for parents, in schools, in the media, and for bank clients, focusingalso on childpornography and internet security. This strategy determines the institutional response to emerging forms of high-tech crime, defines the roles and responsibilities of state bodies, identifies goals and determines the basic directions for action to suppress all types of high-tech crime.

The EC Progress report 2020 indicates that "on cybercrime, convictions were rendered against 49 individuals (first instance). The operational capacity within the police to effectively address cybercrime was strengthened, including through the establishment of special investigative units which deal with abuse of credit cards, e-commerce and e-banking and suppress illegal and harmful content on the internet. Staff in the cybercrime department increased (from 15 to 22). Serbia's cybercrime strategy, adopted in late 2018, is being implemented".

A central criminal intelligence system and harmonised statistics have yet to be set up. Cooperation between the police and the Special Prosecutor's Office for High-Tech Crimeis improving. Within the Ministry of Interior there is Department for Combating operating within the Service for Combating Organized Crime. Department for Combating High-Tech Crime is still understaffed and has insufficient technical resources.

The development of a new national serious and organised crime threat assessment (SOCTA) is in its final stage. The capacities of the Service for Crime Analysis need to be strengthened.
The EC Progress report 2020 indicates that Serbia has signed an inter-ministerial cooperation agreement on the establishment of a National Criminal Intelligence System, as a first step towards improving inter-agency cooperation in the fight against organised crime. The establishment of a single centralised criminal intelligence system, advanced further in terms of technical preparations. An inter-institutional cooperation agreement was signed in September 2019. This system will serve as a safe and unified platform for managing and exchanging data in the field of serious and organised crime between law enforcement and judicial authorities and should improve inter-agency cooperation.

Cooperation between the police and the Special Prosecutor's Office forHigh-Tech Crime has improved. However, the Department for fight against High-Tech Crime is stillunderequipped, especially considering the wide range of complex criminal activity it is expected to investigate. In addition, equipment and methods for fight against cybercrimeneed to be constantly updated in order to keep up with the modern crime trends that evolve even at daily basis.

The **Service for Combating Organised Crime – (**SCOC) is structured with organisational units involved in combating organised crime, in terms of narcotics, financial investigation, anti-corruption, human smuggling and tracking in human beings, cybercrime, smuggling of fire arms as well as any other form of organised crime. Financial investigation, cybercrime and drug smuggling units have been established within the Ministry of Interior allowing greater specialization and expertise. Main challenges are related to the fact that national institutions, due to insufficient budget, cannot afford providing equipment for more effective work. **Concerning IT equipment, all government authorities with jurisdiction to combat organized crime are characterized by lack of modern technical equipment to meet the**

standards of the work required in the fight against cybercrime. The current technical capacity in the area oforganized crime, financial investigation and cyber-crime is limited in terms of hardware- workstations, software and storage, due to budget restrictions. The servers and database storage cannot support analysis application for business intelligence solutions and this fact results with delays and lagging in daily work, which eventually ends up with slow and false information flow. Workstations are used by administrators and developers for the purpose of improving and developing a system for criminal analysis, which is vital for policy development and decision making in police work and the work of the RPPO in the fight against crime.

The Crime Analysis Service (CAS) is responsible to ensure quality crime data collection and analysis, the application of scientific and technical methods and achievements to provide efficient support to the fight against all forms of crime, especially organized crime, corruption, terrorism and extremism. The Service provides support in the areas of operational and intelligence activities, as well as in strategic analysis and crime risks and threats assessment. The database of the Crime Analysis Service provides a unique database of criminal investigations conducted at the national level, which is the responsibility of the Criminal Police of the Republic of Serbia.

According to Annual Work Program and Plan for 2020 High-Tech Crime Department was established in the Republic Public Prosecution`s Office. This department is competent for fulfilling obligations envisaged by theLaw on ratification of Convention on Cybercrime, to coordinate work of Special Prosecution Office for High-tech Crime and also to coordinate work of public prosecutions of general jurisdiction in cybercrime cases.

Organization and jurisdiction of the **Special Prosecution Office for High-Tech Crime** is regulated by the Law on the Organization and Competences of State Authorities for Combating High-Tech Crime.This Prosecution Office is competent for investigation and prosecution of high-tech crime. Its specificity is reflected in its subject matter and territorial jurisdiction. Namely, the subject matter jurisdiction of this prosecution office is established by the aforementioned laws by the listing of groups of criminal offenses which, under certain conditions and manner of execution, fall within the subject matter competence of the Special Prosecution Office for High-Tech Crime.Besides criminal offences against security of computer data set forth in the Criminal Code, this Prosecution Office is competent for criminal offences against intellectual property, property, economy and legal instruments, where computers, computer systems, computer data and products thereof in hard or electronic form appear as the objects or the means of committing a criminal offence, if the number of copies of authors' works exceeds 2,000 or the resulting material damage exceeds the amount of RSD 1,000,000; criminal offences against freedoms and rights of man and citizen, sexual freedoms, public order and constitutional order, and security of the Republic of Serbia, which, due to the manner in which they are committed or means used, may be considered cybercrime offences.As for the territorial jurisdiction, the Special Prosecution Office shall have the jurisdiction for the territory of the Republic of Serbia to proceed in the cases of the criminal offences. Special Prosecutor for High-Tech Crime, five Deputy Public Prosecutors and five Prosecutorial Assistants work in this Prosecution Office. However, there is still not enough administrative stuff necessary to coordinate administrative work concerning increasing number of cases. Also, technical equipment - all segments of the operating systems that will be used forinvestigation and prosecution of criminal offenses in this field and to successfully present evidence before the court was not provided yet.

In accordance with the Criminal Procedure Code (Chapter XV of the CPC. Art 285) "**The public prosecutor** leads the pre-investigation phase. The public prosecutor may assign to the police the undertaking of certain actions aimed at detecting criminal offences and locating suspects. The police are required to execute the order of the public prosecutor and to inform

him regularly about actions undertaken. In case the police do not comply with the order, the public prosecutor act in accordance with article 44 par 2 and 3 of this Code. During the pre-investigation proceedings the public prosecutor is authorised to assume from the police the performance of an action which the police had undertaken on its own pursuant to the law".

The Administration for the Prevention of Money Laundering (APML is the Financial Intelligence Unit - FIU) is recognised to be a necessary member of any task force. To date, APML took part in four task forces. Specifically, APML staff was engaged in collecting financial documentation, analysing it and monitoring the execution of transactions involving certain legal entities. A coordination body for fight Money Laundering and terrorism financing has been established. In this context, the financing of terrorism is a core component of the EU's strategy in the fight against terrorism. As terrorists and their supporters constantly modify their ways to collect, move and gain access to funds, it is needed to adapt its instruments and measures to deprive them from the possibility to engage in criminal activity.

Thestrategic framework includes also the **IOCTA 2019 (Internet Organized Crime Threat Assessment).** This annual assessment of the cybercrime threat landscape highlights the persistence and tenacity of a number of key threats.

***Several weaknesses*have been identified in the Serbian system to fight cyber-crime:**

- *Lack of specialized and operational trainings in relation with crypto currencies and misuse of internet*

Specialised trainings are needed in several fields in relation with internet transactions and crypto-currencies, money laundering (bit coins, etc.), online payments.

- *Lack of cooperation between institutions (at strategic level and operational levels) relevant for financial investigations.*

Cooperation between all stakeholders involved in fight against financial crime, terrorism financing and organised crime is needed. Main institutional actors are from various institutions and line ministries (Ministry of Interior, Ministry of Justice and Ministry of Finance). These require a permanent coordination and exchange of information.

- *Legal framework in relation to cybersecurity and information security (CS/IS) not completely in line with EU standards*

The legal framework has been harmonized in recent years but it is still needed to continue the amendment of the legal framework in order to be in line with EU standards.

- *Cooperation with the private sector and CSOs on cybersecurity matters remains at an early stage of development for a development of a "cybersecurity culture"*

A policy dialogue and consultations with the private and civil sectors are not sufficiently developed for a development of a "cybersecurity culture" among various stakeholders

3.2 Ongoing reforms:

Main challenges in on-going sector reforms are related to the need to strengthening capacities of individual institutions as well as strengthening inter-institutional cooperation for better fight against organized, crime. Cyber-crime appears to be related to Financial crime. The implementation of the **Action Plan 24** has created the need for HR reorganisation in many Institutions in the sector and the need to build capacities on new competences related to on-going reforms from the AP Chapter 24[6]. The **National Serious and Organised Crime Threat Assessment (SOCTA)** has been developed and is a basis for the selection of priorities and the adoption of strategic and operational decisions. It presentsongoing reforms in the

[6] (see http://arhiva.mup.gov.rs/cms_cir/oglasi.nsf/ap-p24.pdf)

sector. This project will support reforms in the field of fight against cyber-crime. Ongoing reforms in this area are in line with the Strategy to fight cyber-crime 2020-2023.

3.3 Linked activities:

The list below describes the main projects relevant to this twinning project, all of which have been funded by the EU under IPA.

EU funded projects

Title: "Project against money laundering and terrorist financing in Serbia".
Donor: EU - IPA 2010
Budget: 2.2 million EUR
Duration: 36 months
Type: Service
Description: This assistance was geared at assisting Serbia in the strengthening of the anti-money laundering and counter-terrorist financing system in terms of legislation, skills and operational capacities.

Title: "Establishment of efficient system for prevention and suppression of illegal migrations in the Republic of Serbia".
Donor: EU - IPA 2010
Budget: 1 million EUR
Duration: 27 months
Type: Twinning
Description: The purpose of the project was "In accordance with the Serbian legal, procedural and technological framework and with a view to compliance with EU standards, to enhance special investigative techniques, in the field of cyber-crime and illegal migration and in the treatment of illegal migrants

Title: "Countering Serious Crime in the Western Balkans"
Donor: EU –Multybeneficiary IPA 2017
Budget: 14.500.000 EUR for all WB countries
Duration: End in 2020
Type: MB IPA
Description:T he project is an integral part of the process of integrated internal security management, that is, an initiative to combat serious and organized crime in the Western Balkans.

Title: "Enhancing the quality and efficiency of Suspicious Transactions Reporting and Administration for the Prevention of Money Laundering core functions"
Donor: EU – IPA 2015
Budget:1.4 million EUR
Duration: 2 years
Type: Service
Description: The Project should lead to an increased quantity and quality of SARs; better cooperation of all AML/CFT stakeholders; increased quality of financial intelligence analysis and of ITC system of the APML. There will be improvements to financial intelligence work, track-record keeping, ML and TF risk assessment, expertise and IT capacities of the APML.

Title: Regional Co-operation in Criminal Justice: Strengthening capacities in the fight against cybercrime
Donor: EU (IPA)
Description: The objective of the project was to "strengthen the capacities of criminal justice authorities of project areas to cooperate effectivelyagainstcybercrimebased on the Budapest Convention on Cybercrime and other standards and tools". Overall, according to the final

report of the project, the progresswas made on all the recommendations, mostnotably in raisingawareness, enhancingcooperationbetween the public and privatesectors as well as increasingregional and international cooperationagainstcybercrime.

Other donors

Title: "Strengthening national capacities in fight against misuse of internet for terrorism"
Donor: OSCE
Budget: 311.528 EUR
Duration:2019 - 2021
Type: Service, Supply
Description: The aim of the project is to fight terrorist activities on internet. Within the project, study visits will be organized, purchase of IT technical equipment and software solutions.

Title: "Regional Programme for South Eastern Europe: Building Regional Anti-Money Laundering and Counter Financing of Terrorism Capacity in South Eastern Europe".
Donor: EU
Budget: 2,631,578.95EUR
Duration: December 2017 - December 2019
Type: UNODC
Description: One of the goals of the project is to decrease treats related to organized crime and terrorism in the South East Europe region through fostering regional cooperation. In February 2018, a regional coordination meeting has been organized at CEPOL with participation of representatives from the Ministry of Interior (MoI), Criminal Police Directorate, Service of combating organized crimeand contact person for CEPOL from the Human Resources Department. Three additional coordination meetings have been organised to plan further activities. Training has been organised in February 2018 in Belgrade and a direct exchange of information with the company Western Union has been initiated with aim to collect information on financial transactions with details of persons involved in transactions.

Title: "The iPROCEEDS project" I and II phase
Donor: EU –Multi-beneficiary
Budget: I phase 5.560.000 EUR , II phase 4.945.000 EUR
Duration: I phase January 2016 - June 2019, II phase January 2020- June 2023
Type: MB IPA
Description: The scope of the project is to further strengthen the capacity of authorities in project countries and areas to search, seize and confiscate cybercrime proceeds and prevent money laundering on the Internet and to secure electronic evidence.

Title: "Protection and Enforcement of Intellectual Property Rights in Serbia".
Donor: EU
Budget: 1,499,998.61 EUR
Duration: February 2019–February 2021
Type: Service
Description: The scope of the project is to support the Republic of Serbia in aligning the standard of protection and enforcement of Intellectual Property Rights with EU Best Practice in order to effectively conduct accession negotiations and successfully manage overall EU integration and pre-accession assistance. One of the project`s components is related to online investigation of criminal acts against intellectual property rights committed via internet or by using computers or other IC technologies.

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

This project is linked to following Union standards/norms/Acquis: As regards EU integration of Serbia, the Ministry of the Interior manages the work of the Negotiation Subgroup for

Chapter 24 and the draft of the Action Plan (AP 24) which will include and thoroughly develop all the activities which should be implemented for the full harmonisation with the EU norms and provision of the capacities for the implementation of the harmonised regulations.

- **Directive (EU) 2013/40/EU on attacks against information systems**
- **Directive (EU) 2015/849** on preventing the use of the financial system for money laundering or terrorist financing (4th Anti-Money Laundering Directive)
- **Directive (EU) 2019/1153** of the European Parliament and of the Council
- **Regulation (EU) 2015/847** on information on the payer accompanying transfers of funds – makes fund transfers more transparent, thereby helping law enforcement authorities to track down terrorists and criminals.
- **Directive (EU) Anti-trafficking Directive** 2011/36/EU
- **5th Anti-Money Laundering Directive** (Amendments to the 4th Anti-Money Laundering Directive). The 5th Anti-Money Laundering Directive, which amends the 4th Anti-Money Laundering Directive, was published in the Official Journal of the European Union on 19 June 2018. The Member States must transpose this Directive by 10 January 2020.
- **Directive (EU) 1371 -** Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law
- **The Council Framework Decision** 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime.
- **The framework decision**, EU 2007/845/JHA
- **The Council Framework Decision** 2005/212/JHA on Confiscation of Crime-Related Proceeds Instrumentalities and Property
- **The Framework Decision** 2003/577/JHA on the Execution in the European Union of Orders Freezing Property or Evidence
- **The Framework Decision** 2001/500/JHA on Money Laundering, the Identification, Tracing, Freezing, Seizure and Confiscation of Instrumentalities and Proceeds of Crime
- **The Framework Decision** 2005/214/JHA on the Application of the Principle of Mutual Recognition of Financial Penalties
- **The Framework Decision** 2014/42/ЕУ on the Freezing and Confiscation of Instrumentalities and Proceeds of Crime in the European Union.
- **Directive (EU) 2015/849** of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing
- **Directive 2005/60/EC** of the European Parliament and of the Council and Commission Directive 2006/70/EC2)
- **Directive 2009/110/EC** of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing
- Directive 2000/46/EC
- **Directive2017/541** of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
- **Council Framework Decision** 2002/475/JHA and amending Council Decision 2005/671/JHA 4) Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 5. Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community

- **Regulation (EU) No 1210/2010** on the authentication of euro coins and handling of euro coins unfit for circulation), and euro banknotes (Decision ECB/2010/2014)

As regards EU integration of Serbia, the Ministry of the Interior manages the work of the Negotiation Subgroup for Chapter 24 and the draft of the action plan which will include and thoroughly develop all the activities which should be implemented for the full harmonisation with the EU norms and provision of the capacities for the implementation of the harmonised regulations.

3.5. Components and results per component

This project is divided into two components:

Component 1: Capacity building for Criminal Police Department and Special Prosecution Office in combating cyber-crime

This component will be implemented in accordance with following expected results:

Result 1.1. Enhanced capacities of institutions involved in fight against cyber-crime
Result 1.2. Staff knowledge and competences to deal with cybercrime improved
Result 1.3. Awareness rising on fight cyber-crime and development of "cybersecurity culture" targeting the private sector and CSOs.

Component 2: Strengthening institutional, analytical and legal framework to fight against cybercrime and support implementation of Strategy's Action plan to fight cybercrime.

This component will be implemented in accordance with following expected results:

Result 2.1. Preparation of analysis and assessment on relevant topics related to fight against cyber-crime and cyber related crimes.
Result 2.2. Legal framework related to fight against cyber-crime and cyber related crimes assessed and amended.
Result 2.3. Institutional framework for new competences of bodies for fight cyber-crime enhanced.

3.6 Means/input from the EU Member State Partner Administration(s)*:

The Project Leader and RTA (Resident Twinning Advisor) shall provide support to the responsible Serbian authorities in strengthening their capacities as well as in the implementation of this project. Resident Twinning Adviser (RTA) is responsible for management and implementation of the foreseen project activities and shall provide support to the responsible Serbian authorities in the implementation of this project, thus in strengthening of their capacities.

3.6.1 Profile and tasks of the PL:

The MS Project Leader will manage the project team as elected member state(s) and co-ordinate the implementation of activities.

Basic skill requirements,

- University degree in the field of Law or Security Studies or Police Academy or equivalent professional experience of 8 years.
- At least 3 years of specific experience in the area offight against cyber, cyber related and financial crime.

- Experience in project management - coordination of national and international project related to capacity building;
- Excellent working knowledge of English language;
- Computer literacy.

Tasks of the Project Leader:

- Responsible for the overall guidance and implementation of the project in cooperation with the BCPL;
- Supervises the RTA;
- Project reporting
- Overall management and coordination with relevant stakeholders as indicated above
- Ensuring backstopping and financial management of the project in the MS;
- Ensuring timely, effective and efficient implementation of the project and achievement of results through proposed activities;
- Coordination of deployment of short-term experts;
- Coordination with RTAs, from the Member Stateside, the Project Steering Committee meetings, which will be held in Serbia every 3 months;
- Participation at the Steering Committee meetings (every 3 months).

3.6.2 Profile and tasks of the RTA:

He/she will liaise with the BC Project Leader and will report to the MS Project Leader. The RTA will also be responsible for ensuring that experts' input and distribution of their working days will be used in the most efficient and effective way and in line with the agreed work plan to enable timely completion of project results. Duration of his/her secondment will be 24 consecutive months. The RTA will work closely with the Serbian RTA Counterpart to deliver the project, as specified in the Twinning Contract, and part of the task will be to negotiate the Contract and work plan after the project has been awarded. The RTA will be responsible for the selection and supervision of the RTA Assistant and the management and performance of the STEs while in Serbia. She/he will be responsible for drafting the quarterly and final project reports for the Steering Committee.

Basic skills requirements:

- University degree in the field of Law, Security, Police or equivalent professional experience of 8 years
- At least 3 years of specific professional experience in suppressing cyber, cyber related and financial crime.
- Project management experience: managing or assisting in management in at least 1 EU funded projects (preferably twinning) would be considered as an asset.
- Working knowledge of English language
- Computer literacy - Knowledge of Microsoft Office.

Tasks of the RTA:

- Ensures timely reporting to the Contracting Authority, with special attention to all difficulties that may jeopardize the implementation of the project and the achievement of its results.
- Responsible for organization of the Project Steering Committee meetings and reporting on the project progress in close cooperation with the Project leader
- Project management and coordination of the activities of the team members in line with the agreed Work plan to enable timely completion of project results and delivery of outputs;

- Selection, mobilisation and supervision of the short-term experts, together with the Project Leader;
- Facilitation of the contacts with peer institutions in EU member states in order to stimulate a proper exchange of information, data, and experience;
- Establish and maintain cooperation with all beneficiaries involved in the implementation of the project and other related projects (ensuring the avoidance of overlapping), in close coordination with the Project Leader;
- Organization of visibility events (kick-off and final event)

3.6.3. Profile and tasks of Component Leaders:

The project is divided into two Components. One Component Leader for every of the aforementioned 2 components (and Results per component). These Component Leaders will ensure continuity and consistency within each of the fields concerned. While Component Leaders will not be resident in Serbia, they are expected to work in Serbia with the RTA and with the beneficiary institutions at least 3 times per working year. CV's and proposed activities of each Component Leader shall be an integral part of the MS proposal. The detailed expert input shall be established when drawing up the Twinning Work Plan.

Component 1 Leader:

Basic skills requirements:

- University degree in the field of Social or interdisciplinary or security science or equivalent professional experience of 8 years.
- At least 3 years of professional experience in suppressing cyber, cyber related and financial crime.
- Project management experience: managing or assisting in management in at least 1 EU funded projects (preferably twinning) would be considered as an asset.
- Fluency in English language.
- Minimum 3 years of experience in Capacity building and/or organisation of trainings and training of trainers.
- Computer literacy - Knowledge of Microsoft Office.

Tasks of the Component 1 Leader:

- Support in implementation of activities and results related to component 1
- Preparation of TNA and Training programme
- Coordination of trainings
- Coordination of Training of trainers
- Support to RTA in reporting related to activities related to component 1
- Support to RTA in coordination short-term experts for activities related to component 1

Component 2 Leader:

Basic skills requirements:

- University degree in the field of legal or security science or equivalent professional experience of 8 years.
- At least 3 years of specific professional experience in suppressing cyber, cyber related and financial crime.
- Project management experience: managing or assisting in management in at least 1 EU funded projects (preferably twinning).
- Fluency in English language.
- Computer literacy - Knowledge of Microsoft Office.

Tasks of the Component 2 Leader:

- Support in implementation of activities and results related to component 2
- Support in Preparation of Proposal for Strategy on financial investigations and Action Plan
- Support in Preparation of Proposal for Strategy on fight against financing terrorism and Action Plan
- Support to RTA in reporting related to activities related to component 2
- Support to RTA in coordination short-term experts for activities related to component 2

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

Other specialist staff will be made available by the Twinning Partner to support the implementation of activities. Specific and technical matters not directly covered by the Resident Twinning Adviser can be taken over by a pool of short-term experts within the limits of the budget. The detailed expert input shall be established when drawing up the twinning work- plan.

STE Profiles

General experience:

- University degree in a relevant subject.
- Minimum of 3 years of experience in EU Member body in the field of supressing cyber, cyber related and financial crime.
- Good command of written and spoken English.

Tasks of the Short-Term experts:

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

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

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

The twinning partners are invited to define the specific STE profiles during the preparation of the twinning contract.

4. Budget

Maximum Budget available for the Grant

IPA community contribution 100% - 1.000.000 EUR

National Cofinancing 0%

5. Implementation Arrangements

5.1 Implementing Agency responsible for tendering, contracting and accounting (AO/CFCE/PAO/European Union Delegation/Office):

Ministry of Finance
Department for Contracting and Financing of EU Funded programs (CFCU)
Sremska St, No. 3-5
11000 Belgrade, Serbia
Mr. Marko Jovanovic, Head of Contracting Authority, Assistant Minister
Phone: +381 11 20 21 -115
E-mail:marko.jovanovic@mfin.gov.rs
Mr. Darko Vasić, Twinning National Contact Point
Phone: +381 11 2021 412
E-mail: twinnning@mfin.gov.rs

5.2 Institutional framework

Project SteeringCommitteeand modalities are set out in 5.2.4 of the twinning manual.
The lead beneficiary is the **Ministry of Interior – The Criminal Police Directorate** (Service for combating organised crime)

5.3 Counterparts in the Beneficiary administration:

5.3.1 Contact person:

Ms Tatjana Đurašković
Department for suppression of Cybercrime
Service for combatting organised crime
Criminal Police Directorate
Ministry of Interior

5.3.2 PL counterpart

The BC Project Leader will manage a project team at the Serbian side and will assure that the decision makers at the national level will be informed properly on the implementation of the project. He will ensure close co-operation and overall steering and coordination of the project. He will be also responsible for drafting reports and other documents, related to project management at the Serbian side and will chair Steering Committee meetings.

Mr Vladimir Vujic
Head of Department for suppression of Cybercrime
Department for suppression of Cybercrime
Service for combating organised crime Criminal Police Directorate
Ministry of Interior

5.3.3 RTAcounterpart

Ms Tatjana Đurašković
Department for suppression of Cybercrime
Service for combating organised crime
Criminal Police Directorate
Ministry of Interior

6. Duration of the project

6.1. Duration of the execution period 18 months (implementation period) + 3 months

7. Management and reporting

7.1 Language

The official language of the project is the one used as contract language under the instrument English. All formal communications regarding the project, including interim and final reports, shall be produced in the language of the contract.

7.2 Project Steering Committee

A project steering committee (PSC) shall oversee the implementation of the project. The main duties of the PSC include verification of the progress and achievements via-à-vis the mandatory results/outputs chain (from mandatory results/outputs per component to impact), ensuring good coordination among the actors, finalising the interim reports and discuss the updated work plan. Other details concerning the establishment and functioning of the PSC are described in the Twinning Manual. The PSC will be composed of following members: MS Project Leader, BC Project Leader, RTA, RTA BC counterpart, representatives of the Ministry of Finance, Department for Contracting and Financing of EU Funded Programs (CFCU), representatives of the IPA Unit, representatives of the Ministry for European Integration (MEI) and the representatives of other key institutions involved in the project. Representatives of the EUD will be invited as observer(s). If deemed necessary, representatives of other institutions with relevant expertise or key experts who can enhance the quality of the project should be invited to join the Steering Committee Meetings as observers.

7.3 Reporting

All reports shall have a narrative section and a financial section. They shall include as a minimum the information detailed in section 5.5.2 (interim reports) and 5.5.3 (final report) of the Twinning Manual. Reports need to go beyond activities and inputs. Two types of reports are foreseen in the framework of Twining: interim quarterly reports and final report. An interim quarterly report shall be presented for discussion at each meeting of the PSC. The narrative part shall primarily take stock of the progress and achievements via-à-vis the mandatory results and provide precise recommendations and corrective measures to be decided by in order to ensure the further progress.

8. Sustainability

Strengthening the capacity and efficiency of the services and institutions responsible for financial investigation, fight terrorism financing and fight organised crime will play an important role in Serbia's EU integration process. (Chapters 23 and Chapters 24, Chapter 32)
Institutional sustainability through this project, supported by organisation of several Training or Trainers (ToT) programmes, support to coordination between institutions and preparation of strategic framework with action plan.

Twinning modality has been chosen for the support because it is expected that twinning will enable exchange of experience with MS and maintain further cooperation between the beneficiary institutions and the twinning partner.

The goal of establishing and ensuring the sustainability of an efficient system to fight cyber, cyber related and financial crimerequires coordination of all stakeholders which will be secured during all stages of project implementation. This project is also linked to a FWC contract for purchase of supply. Linkages between both projects are required.

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

Cross-cutting issues will be addressed in the project so as to comply with the best EU standards and practice in that area and in a way which demonstrates how they will be dealt with within the project's framework, its activities, and outputs.

Equal Opportunities and non-discrimination

The basic principle of equal opportunities will be adhered to as reflected in Serbian legislation. Gender equity principles will be respected in the implementation of all Project

activities. The project will promote high standards of equality and gender mainstreaming both in strengthening the relevant legislative framework in line with international and EU standards as well as in its training component, especially encouraging active participation of the female staff in all activities. In the reporting, a gender disaggregated data will be kept and followed. The Project will be implemented in a non-discriminatory manner with equal opportunities observed and firm guarantees that distinctions will not be drawn on the basis of sex, race, ethnicity, religion or other possible grounds in any regard. Gender equity principles will be respected in the implementation of all Project activities.

Environment and climate change
N/A
Minorities and vulnerable groups
N/A

Civil Society/Stakeholders involvement
Financial Investigations, fight against terrorism financing and fight against organised crime involve civil society organisations through their work on specific topics (e.g. related to organised crime: anti-corruption, fight human beings trafficking, drugs, etc. and financial crime: money laundering, etc.). They will be informed about project activities and will be involved through project visibility activities). The result 2.4 of the project will focus on public awareness. In addition CSOs will also be involved through risk analysis of the NPO (non profit organisations) sector (e.g. in relation to terrorism financing, etc.). In addition religious communities will also be involved in the project through risk analysis in relation to terrorism financing.

Stakeholder's involvement. The project includes many direct stakeholders presented as beneficiaries of this project: The Ministry of Interior (MoI), The Criminal Police Directorate, Service for combating organized crime, Ministry of Finance, Customs, Administration for the Prevention of Money Laundering (APML is the Financial Intelligence Unit - FIU), AFCOS, Tax administration, Ministry of Justice, Public Prosecutors offices, Courts, Anti-corruption Agency. Other stakeholders can be also mentioned as indirect beneficiaries: National Bank of Serbia, Professional Associations, Universities, etc.

10. Conditionality and sequencing
No prior conditions have to be fulfilled nor preceding projects/activities completed before project implementation commences.

11. Indicators for performance measurement

Overall objective: To contribute to meeting the EU accession requirements under Chapter 24 of the *Acquis* – Justice, freedom and security and to contribute to strengthening legislative framework and institutional capacities, for fulfilling the requirements of EU membership.

Indicators
Rate of transposition of the EU *Acquis*, as measured by the % of the implementation of the Serbian National Programme for Approximation with the *Acquis.*
Progress made towards meeting the accession criteria as measured by relevant *Acquis* negotiation chapters.

Specific objective:
To strengthen capacities of Criminal Police Directorate, Service for combating organized crime, Department for Combating High-Tech Crime and Special Prosecution Office for High-Tech Crime

Indicators
Degree of implementation of the related Chapter 24 Interim benchmarks
Degree of implementation of Serious and organised crime threat assessment (SOCTA)

Component 1: Capacity building for Criminal Police Department and Special Prosecution Office in combating cyber-crime

Result 1.1. Enhanced capacities of institutions involved in fight against cyber-crime
Indicators
1.1.1. – Status of Training Needs Analysis (TNA) and Training curriculum
1.1.2. - Number of trainings delivered (joint/mixed trainings, trainings for MoI, Public Prosecution and other competent agencies, basic trainings, advanced trainings, specialised trainings) (Minimum 40 trainings)
1.1.3. – Number of trainings with workshops organised for children, parents, schools and official representatives involved in fight cyber-crime on children sexual abuse. (5 trainings with workshops organised in biggest cities with minimum 100 children on each training).
1.1.4. Status of the curriculum for the judicial academy
1.1.5. Number of trainings from the curriculum for the judicial academy in relation to cyber crime and cyber related crimes carried out (with participation of prosecutors and judges)
1.1.6. Number of people trained in MoI and Public Prosecution Office and other competent agencies

Result 1.2. Staff knowledge and competences to deal with cybercrime improved
Indicators
1.2.1. At least 3 training of trainers organised (Minimum 1 ToT (Training of Trainers) on fight against cyber-crime, 1 ToT on fight cyber related crimes, 1 ToT in relation to Judicial Academy)
1.2.2. Number of Criteria for selection of participants to Training of Trainers developed.
1.2.3. Number of certificates delivered to participants of Training of Trainers.

Result 1.3. Awareness rising on fight cyber-crime and development of "cybersecurity culture" targeting the private sector and CSOs.

Indicators
1.3.1. Number of publications (Manuals) on relevant topics in relation to cyber-crime prepared, published and disseminated (Minimum 5 topics defined during the inception phase)
1.3.2. Number of promotion material printed and disseminated (Minimum 100.000 printed and disseminated) on topics in relation to children sexual abuse through internet and other topics in relation to cybercrime agreed during the inception phase with beneficiaries.
1.3.3. Number of printed awareness material - Minimum 100.000 printed stickers with information on children sexual abuse and 100.000 cover camera stickers.
1.3.4. Number of training and Conference material (Number of Pens, notebooks, USB with logo in line with EU visibility rules and beneficiaries distributed to all trainings and workshops participants)

Component 2: Strengthening institutional, analytical and legal framework to fight against cyber crime

Result 2.1.Preparation of analysis and assessment on relevant topics related to fight against cyber-crime and cyber related crimes with presentation to relevant stakeholders.

Indicators

2.1.1. One comparative legal analysis with lessons learned from EU Member States in relation to fight cyber-crime prepared
2.1.2. One comparative legal analysis on confiscation of digital property
2.1.3. One legal assessment analysis of the current situation and the threat of cybercrime in Serbia with projections for coming years prepared (assessment analysis on cyber-crimes prepared and presented to key stakeholders)
2.1.4. Number of workshops organised for presentation legal analysis results and recommendations to relevant stakeholders (Minimum 3 workshops)

Result 2.2. Legal framework related to fight against cyber-crime and cyber related crimes assessed and amended.

Indicators
2.2.1. Review of existing legal framework / legislation with recommendations prepared and presentation of findings and recommendations.
2.2.2. Law of competences of bodies for fight cyber-crime updated
2.2.3. Table of concordance for the laws in relation with cyber-crime and cyber related crimes which are required to be harmonized with EU and international standards prepared
2.2.4.. Number of related sub-laws in relation to fight cyber-crime and cyber related crimes prepared to amendment.

Result 2.3. Institutional framework for new competences of bodies for fight cyber-crime enhanced.
2.3.1. Functional analysis in line with Law of competences of bodies for fight cyber-crime with recommendations prepared.

12. Facilities available
One Office with workstation for RTA for his/her daily work and assistant/s will be provided in accordance with the Twinning Manual in kind. A Meeting room will be available for the project as well as a Training room**.**

ANNEXES TO PROJECT FICHE

1. The Simplified Logical framework matrix

Overall Objective	Objectively verifiable indicators	Sources of Verification	Risks	Assumptions
Overall objective: To contribute to meeting the EU accession requirements under Chapter 24 of the *Acquis* – Justice, freedom and security and to contribute to strengthening legislative framework and institutional capacities, for fulfilling the requirements of EU membership.	Rate of transposition of the EU *Acquis*, as measured by the % of the implementation of the Serbian National Programme for Approximation with the *Acquis* Progress made towards meeting the accession criteria as measured by relevant *Acquis* negotiation chapters	EC Annual Reports NPAA Reports		
Project Purpose	**Objectively verifiable indicators**	**Sources of Verification**		
To strengthen capacities of Criminal Police Directorate, Service for combatting organized crime, Department for Combatting High-Tech Crime and Special Prosecution Office for High-Tech Crime	Degree of implementation of the related Chapter 24 Interim benchmarks Degree of implementation of Serious and organised crime threat assessment (SOCTA)	EC Annual Reports SIGMA reports	Difficulties in project implementation due to the pandemic Covid 19 Lack of availability of civil servants for participating in project activities	Continuous support of the GoS to European Integration process; Continuous support of the Member States to Serbia's European Integration process; Annual budget allocation by the government of appropriate levels of human and financial resources; Sufficient dedicated and qualified staff available at beneficiary institutions.
Results	**Objectively verifiable indicators**	**Sources of Verification**		**Assumptions**
Component 1: **<u>Capacity building for Criminal Police Department and</u>**	1.1.1. – Status of Training Needs Analysis (TNA) and Training 1.1.2. - Number of trainings	All Twinning project reports EC Annual Report	Lack of availability of civil servants for participating in capacity building activities	Fight against -cybercrime remain a high priority for the Government Sustained relative political

Special Prosecutor's Office in combating cyber-crime **Result 1.1.** Enhanced capacities of institutions involved in fight against cyber-crime **Result 1.2.** Staff knowledge and competences to deal with cybercrime improved **Result 1.3.** Awareness rising on fight cyber-crime and development of "cybersecurity culture" targeting the private sector and CSOs. **Component 2: Strengthening institutional, analytical and legal framework to fight against cyber- crime** **Result 2.1.** Preparation of analysis and assessment on relevant topics related to fight against cybercrime and cyber related crimes with presentation to relevant stakeholders. **Result 2.2.** Legal framework related to fight against cybercrime and	delivered (joint/mixed trainings, trainings for MoI, Public Prosecution and other competent agencies, basic trainings, advanced trainings, specialised trainings) (Minimum 40 trainings) 1.1.3. – Number of trainings with workshops organised for children, parents, schools and official representatives involved in fight cyber-crime on children sexual abuse. (5 trainings with workshops organised in biggest cities with minimum 100 children on each training). 1.1.4. Status of the curriculum for the judicial academy 1.1.5. Number of trainings from the curriculum for the judicial academy in relation to cyber crime and cyber related crimes carried out (with participation of prosecutors and judges) 1.1.6. Number of people trained in MoI and Public Prosecution Office and other competent agencies 1.2.1. At least 3 training of trainers organised (Minimum 1 ToT (Training of Trainers) on fight against cyber-crime, 1 ToT on fight cyber related crimes, 1 ToT in relation to Judicial Academy) 1.2.2. Number of Criteria for selection of participants to Training of Trainers developed.	Chapter 24 EU Monitoring Reports Strategy and its Action plan National and Regional SOCTA Reports	Lack of cooperation between institutions for participating in common activities	stability in Serbia Continuation of the EU integration process Legal framework relevant for fight cyber-crime to be amended

cyber related crimes assessed and amended. **Result 2.3.** Institutional framework for new competences of bodies for fight cyber-crime enhanced.	1.2.3. Number of certificates delivered to participants of Training of Trainers. 1.3.1. Number of publications (Manuals) on relevant topics in relation to cyber-crime prepared, published and disseminated (Minimum 5 topics defined during the inception phase) 1.3..2.. Number of promotion material printed and disseminated (Minimum 100.000 printed and disseminated) on topics in relation to children sexual abuse through internet and other topics in relation to cyber crime agreed during the inception phase with beneficiaries. 1.3.3. Number of printed awareness material - Minimum 100.000 printed stickers with information on children sexual abuse and 100.000 cover camera stickers. 1.3.4.. Number of training and Conference material (Number of Pens, notebooks, USB with logo in line with EU visibility rules and beneficiaries distributed to all trainings and workshops			

	participants) 2.1.1. One comparative legal analysis with lessons learned from EU Member States in relation to fight cyber-crime prepared 2.1.2. One comparative legal analysis on confiscation of digital property 2.1.3. One legal assessment analysis of the current situation and the threat of cybercrime in Serbia with projections for coming years prepared (assessment analysis on cyber-crimes prepared and presented to key stakeholders) 2.1.4. Number of workshops organised for presentation legal analysis results and recommendations to relevant stakeholders (Minimum 3 workshops) 2.2.1. Review of existing legal framework/ legislation with recommendations prepared and presentation of findings and recommendations. 2.2.2. Law of competences of bodies for fight cyber-crime updated 2.2.3. Table of concordance for the laws in relation with cyber-			

	crime and cyber related crimes which are required to be harmonized with EU and international standards prepared 2.2.4. Number of related sub-laws in relation to fight cyber-crime and cyber related crimes prepared to amendment. 2.3.1. Functional analysis in line with Law of competences of bodies for fight cyber-crime with recommendations prepared.			