European Commission

ANNEX C1: Twinning Fiche

Project title: Enhancing Critical Infrastructure Protection system, fight against Cybercrime and Cyberterrorism in Georgia

Beneficiary administrations: Office of the National Security Council, Ministry of Internal Affairs, State Security Service of Georgia

Twinning Reference: GE 18 ENI JH 04 21

Publication notice reference: EuropeAid/ 173776 /DD/ACT/GE

EU funded project

TWINNING TOOL

List of Abbreviations

AA	Association Agreement
AP	Action Plan
APT	Advanced Persistent Threat
BA	Beneficiary Administration
CIP	Critical Infrastructure Protection
CL	Component Leaders
CCG	Criminal Code of Georgia
CSB	Cyber Security Bureau
DCFTA	Deep and Comprehensive Free Trade Area
DGA	Digital Governance Agency
EU	European Union
GoG	Government of Georgia
ICC	Interagency Coordinating Council
MIA	Ministry of Internal Affaire
MoJ	Ministry of Justice
MS	Member State
NLO	NATO Liaison Office
NSC	The National Security Council
OSCE	Organization for Security and Co-operation in Europe
OTA	Operative-Technical Agency
PA	Public Administration
PL	Project Leader
PPP	Public-Private Partnership
PSC	Project Steering Committee
RTA	Resident Twinning Advisor
SCADA	Supervisory Control and Data Acquisition systems
SDG	Sustainable Development Goals
STE	Short Term Expert
SSSG	State Security Service of Georgia
ToT	Training of Trainers
UNSC	United Nations Security Council
UN	United Nations
WG	Working Group

1. Basic Information

1.1 Programme: “EU4 Security, Accountability and Fight against Crime in Georgia (SAFE)", ENI/2018/041-443 Direct Management.

For UK applicants: *Please be aware that following the entry into force of the EU-UK Withdrawal Agreement[1] on 1 February 2020 and in particular Articles 127(6), 137 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*

[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

(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

1.3 EU funded budget: 1.3 million EUR

1.4 Sustainable Development Goals (SDGs): 16. Peace, Justice and Strong Institutions

2. Objectives

2.1 Overall Objective(s):

The overall objective of the project is to further improve resilience of critical infrastructure against threats, among others, against cybercrime and other cyber-enabled offenses including cyberterrorism, in line with the EU's approach, standards and policy framework.

2.2 Specific objective:

The specific objectives of the project are:

SO1. Identification and protection system of critical infrastructure subjects established

SO2. Investigation and prevention mechanisms of Cybercrime enhanced

SO3. Cyberterrorism and Other APT threat combating capacities improved

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

The Twinning project is fully in line with the requirements of the EU - Georgia Association Agreement (AA) including Deep and Comprehensive Free Trade Area (DCFTA) and aims to support further effective fulfilment of the objectives set out in the AA.

Critical Infrastructure Protection

The **EU – Georgia Association Agreement** implies enhanced cooperation in defence policy and security field, strengthening the bilateral dialogue on the related matters, addressing common concerns, expanding collaboration to facilitate Georgia's participation in the EU crisis management operations, as well as in the Common Security and Defence Policy (CSDP) related capacity building and consultation activities. At the same time, it is foreseen to activate various EU support tools and programmes, with the aim of enhancing resilience and Georgia's capacity to stand against hybrid threats.

Under **the EU-Georgia AA Agenda 2017-2020**, Georgia has undertaken the responsibility to make efforts in order "to increase the cyber resilience of key critical infrastructure sectors and public sector organisations, drawing from relevant EU experiences and in line with EU norms" (Association Agenda 2.6. - Economic Development and Market Opportunities: Cooperation in

[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] Annex IV to the ACP-EU Partnership Agreement, as revised by Decision 1/2014 of the ACP-EU Council of Ministers (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.

the Field of Digital Economy and Society, mid-term priorities). Therefore, elaboration of threat, impact and risk assessment methodologies and their implementation in the respective critical sectors, and delivery of sectoral and national criteria for the identification of critical infrastructure subjects, as well as definition of general and sector-specific measures for the protection of critical infrastructure subjects, directly contributes to the fulfilment of the abovementioned responsibilities. The new AA Agenda that is agreed among parties also reflects issues associated with critical infrastructure.

Currently NSC Office is working on renewing National Security Concept and Threat Assessment Document in which protection of CI are highly underlined. The documents are planned to be approved no later than mid 2022. More precisely, the National Security Concept will be submitted to Georgian Parliament for its review and adoption by the end of February 2022 whereas National Threat Assessment Document will be approved by the GoG highly likely in April-May 2022.

Cybercrime

The AA sets out the obligations in relation with combating crime. Taking into account Article 2(4) of the AA, the Parties have committed themselves to the fight against the various forms of transnational organised crime; this commitment constitutes a key factor in the development of the relations and cooperation. Further, as stated in Article 17(1)(g), the Parties shall cooperate on combating and preventing criminal and illegal activities, including cybercrime.

In addition, the **EU – Georgia Association Agenda 2017-2020** prioritises enhancing cooperation in addressing cybercrime. Under the umbrella of Cooperation in the Field of Digital Economy and Society, the **Agenda** states that the Parties will cooperate to prepare for implementation of EU acquis mentioned in relevant annexes of the Association Agreement and support Georgia on efforts to increase the cyber resilience of key critical infrastructure sectors and public sector organisations. As abovementioned, the new AA Agenda that is agreed amoung parties also reflect issues associated with cybercrime.

Through its ambitious ‘20 deliverables for 2020’ reform agenda the EaP has delivered tangible results on the ground and improved people’s lives. To continue working on objectives, the new agenda **“Recovery, resilience and reform: post 2020 Eastern Partnership priorities”** sets out a new vision for the partnership with five long-term objectives, one of those being together for accountable institutions, the rule of law and security, that includes Cyber resilience and cybercrime.

One of the Top Ten Targets for 2025 will be investing in security and cyber resilience:
A strengthened framework in place for identifying and addressing hybrid threats; strengthened partners' capacities to increase cyber resilience and tackle cybercrime, including through fully Implementing the Council of Europe Budapest Convention on cybercrime.

Furthermore, the Joint Declaration of the Eastern Partnership Summit 2017 stressed the importance of enhancing fight against cybercrime in the partner countries. The 6th Eastern Partnership Summit will continue building on the discussions at the 5th Summit in 2017 and will provide further guidance and political direction on taking the EaP forward, with a renewed vision focusing on recovery, resilience and reform.

In 2008, Georgia signed the Council of Europe Convention on Cybercrime (“the Budapest Convention”), which entered into force on 1 October 2012. As a result, Georgia became the

34th state party to the Convention.The Convention 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. Under the Article 35 of the Convention, the **24/7 National Contact Point** was established in the Ministry of Internal Affairs of Georgia, which is used for the active exchange of information between the law-enforcement agencies and member countries of Budapest convention.

Moreover, In April 2017, Europol and the Ministry of Internal Affairs of Georgia signed the **Agreement on Operational and Strategic Cooperation**. The Agreement, *inter alia*, aims to expand cooperation in combating serious and organised cross-border criminal activities, including cybercrime.

The primary document for fighting cybercrime is the **National Strategy on Combating Organized Crime 2021-2025 and its Action Plan 2021-2022**, both of which include separate sections addressing cybercrime. The Strategy and Action Plan mainly refer to the development of substantive and procedural legislation, increased capacity of government agencies and institutions, international cooperation, raising public awareness, and public-private partnerships.

Cyberterrorism and Other APT Threats

The AA under Article 12 (Fight against terrorism) stresses the importance of cooperation between the Parties in the implementation of the United Nations Global Counter-Terrorism Strategy as well as relevant United Nations Security Council resolutions.

In this respect, there is growing concern over the misuse of information and communications technologies (ICT) by terrorists, in particular the Internet and cyberspace. The United Nations Global Counter-Terrorism Strategy and its Action Plan,[5] under the measures to prevent and combat terrorism, *inter alia* calls for coordinated efforts to counter terrorism in all its forms and manifestations on the Internet. Furthermore, in resolution 2341 (2017) the Security Council expresses concern that terrorist attacks on critical infrastructure could significantly disrupt the functioning of government and private sector alike and cause knock-on effects beyond the infrastructure sector; and calls upon Member States to strengthen international partnerships with various stakeholders, as appropriate, to share information and experience in this respect.[6]

Also, the AA under Article 20 (Cooperation in the fight against terrorism) reaffirms the importance of law enforcement approach to the fight against terrorism and agree to cooperation in particular by *inter alia* “exchanging experience in the prevention and suppression of terrorism, means and methods and their technical aspects, as well as on training, in accordance with applicable law”.

Furthermore, the EU – Georgia Association Agenda 2017-2020 implies enhanced cooperation in the fight against terrorism, under the foreign and security policy dimension (2.2). The counter-terrorism cooperation in the field of foreign and security policy will be duly reflected in the new AA Agenda document as well.

On national level, the National Strategy of Georgia on Fight against Terrorism 2019-2021[7] aims at establishing the vision of the state of Georgia in terms of prevention and the fight against extremism and terrorism in all its manifestations, including cyberterrorism.

[5] Available at: https://undocs.org/en/A/RES/60/288

[6] Available at: https://undocs.org/S/RES/2341(2017)

[7] Available at: https://ssg.gov.ge/uploads/pr/25.01.19/National%20CT%20Strategy%20of%20Georgia.pdf

Together with combatting cyberterrorism, Georgian Cybersecurity Strategy for 2021-2024 underpins importance to fight against other types of the cyber-attacks organized by the APT groups such as illegal access to SCADA systems, misuse of devices, interference in normal functioning and etc.

3. Description

3.1 Background and justification:

Critical Infrastructure Protection

Critical infrastructure protection (CIP), as a domain, is of utmost importance for a modern state and its society, for guaranteeing the continuity of essential services and enhancing resilience. Accordingly, the CIP field represents an inherent part of the security policy maintained by each and every single state. The same holds true for Georgia, and currently, the country heavily invests in advancing a comprehensive reform in the CIP field. Georgia's critical infrastructure has become, on multiple occasions, a vulnerable target for the malign activities implemented by adversaries. Those activities acquired a multi-dimensional character, and found their manifestation in different fields (physical infrastructure disruption, cyber-attacks, disinformation campaigns surrounding Georgian CI such as the "Lugar Lab") which can be subsumed under the umbrella of hybrid threats. Hence, the current state of affairs requires, on the Georgian part, an effective response to respective challenges.

It goes without saying that interdependencies identified for critical infrastructures (physical, cyber, geographic, logical) require a whole-of-government approach to the reform, and an active involvement of all relevant stakeholders in the working process, including the necessity of public-private partnership (PPP) element. Thus, the respective reform, in the Georgian context, encompasses all the above mentioned components and is designed as a comprehensive endeavour.

The field of critical infrastructure protection (CIP) is an issue of overwhelming importance and a priority for the Government of Georgia. The country is to start the reform from the beginning, as there is no general conceptual or legal framework on the CIP (despite the existence of particular sectoral lists and the implementation of the respective security standards/protection measures). However, Georgia has relative progress in elaborating policy and regulatory framework necessary for the protection of Critical Information Infrastructure. Namely, 4 tier list (State Agencies, Telecom Players, Other Private Business and National Defence Institutions) has been already adopted as well as minimum security requirements for those Subjects have been defined by the relevant responsible sectoral agencies (OTA, DGA or CSB).

The National Security Council (NSC)[8] is the main coordinating institution in the field of national security policy planning as well as in nationwide crisis management process in particular if the latter involves also critical infrastructure of the Country . It is a consultative body directly subordinated to the Prime-Minister of Georgia in order to make highest level decisions on national security issues.

The National Security Council was created in 2019. The legal basis for its functioning is established by the Law of Georgia on "Planning and Coordination Rules of National Security Policy".

The Council ensures providing information to the Prime-Minister on matters posing threats to national security and state interests, prepares policy decisions of the Prime-Minister, ensures

[8] https://nsc.gov.ge/en/COUNCIL/About-the-Council

planning and coordination of national security policy at the strategic level.

In 2018 – in accordance with the constitutional amendments, similarly to the State Security and Crisis Management Council – the President's consultative body, the National Security Council, was abolished.
Given the need for a coordinating agency in the field of security policy planning and coordination, the National Security Council was established in 2019 based on legislative changes.

The NSC Office's functions are: elaboration of informational and analytical materials / papers on the national security related matters; coordination of national security policy planning on the basis of conceptual documents in the field of national security; provision of the crisis management function at a strategic (political) level. At the same time, the NSC Office coordinates three important strategic project/directions in the following areas: critical infrastructure protection (CIP), cybersecurity and hybrid threats.

The current personnel of the NSC have been accompanying the CIP reform from its very beginning and they were the authors of the very first conceptual document (which was not officially approved) in the field, elaborated back in 2017 within the framework of the former Office of the State Security and Crisis Management Council. The NSC staff was also involved in elaboration of the initial gap analysis document, the review of the current legislative framework in the CIP field and the initial Action Plan for the implementation of the reform.

Absence of the explicit monitoring functions, on the part of the NSC Office, with regard to the implementation of the respective Action Plans of national strategies in the security fields, can be identified as a weakness of the current coordination framework. In practice, the NSC Office will be implementing the respective monitoring function in the areas defined as priority (i.e. in the context of the abovementioned three project directions). However, NSC successfully addressed this problem in Cybersecurity Strategy in which it is explicitly indicated that Office of NSC has monitoring function over the entire implementation of the Strategy and its Action Plan. Similarly, the NSC Office plans to apply same approaches in relation with other Strategies/Action Plans to be developed in future that can become effective balancing factor for abovementioned loophole as long as the respective legislative amendments into the statutory powers of NSC are not prepared.

At the same time, as the future CIP structural framework, to be delivered, will inevitably lead to the alteration of the current institutional setup, the reform will require the expansion of the human resources component of the NSC Office in the context of dedicated employees who will ensure the implementation of the CIP reform. As a result of the change in the respective structural framework, the NSC Office is set to enjoy the status of a coordinating agency for the functioning of the critical infrastructure. This function will entail an in-depth involvement of the Office in policy making in the field, relevant in terms of identification and categorization of the critical infrastructure subjects, elaboration of their safe and secure functioning standards and regulation of investment policy in relation to them. Accordingly, creation of an enhanced, dedicated structural unit at the NSC Office, concentrating on the coordination of the CIP reform, might become an important issue in the future.

The emerging structural setup, in the CIP field, will encompass the roles and responsibilities of the following actors: the Government of Georgia, a coordinating agency in the CIP field (i.e. NSC Office), sectoral agencies responsible for the respective (sectoral) critical infrastructure subjects and two Government Commissions responsible for the monitoring of the implementation of security standards and the monitoring of the implementation of the investment policy in relation to the critical infrastructure subjects. Accordingly, the CIP reform involves various stakeholders and actors, including the relevant sectoral agencies, regulators, private sector representatives etc.

The CIP reform encompasses two separate directions/dimensions: 1) creating a legal and conceptual framework in the field of critical infrastructure protection; 2) identification of critical infrastructure subjects, elaboration of security standards for the safe functioning of critical infrastructure subjects, regulation of investment policy with regard to critical infrastructure. This TWINNING project refers to the second dimension of the CIP reform, with the exception of the investment policy part.

The current national security-related legislation does not create a legal basis for the implementation of the CIP reform as such. Hence, one of the most important working directions will be the delivery of the general legal framework in the CIP field. The existing Georgian legislation does not provide unified regulation on the status of critical infrastructure. In contrast to that, there is a certain "sectoral approach", where the respective subjects are defined in a particular sector (e.g. critical information system subjects (general CISSs) and CISSs in the field of defence, determined on the basis of the "Law on Information Security").

In addition, there are provisions in the Georgian legislation that define the respective subjects through more "general principles" and their critical status depends on the risk level to the national security (e.g. the high risk subjects to the state security, determined on the basis of the "Law on State Security Service"). There are further pieces of legislation which indirectly refer to the subjects falling within the sphere of interest of the current CIP reform. In the latter context, the following legal acts have to be mentioned: "Law on Public Safety" (elaborating on potentially dangerous facilities and facilities of vital importance); "Law on State Property" (referring to the property exempt from privatization); "Law on Police" (entailing sections on facilities of special importance and facilities of strategic significance); Government Resolutions (entailing lists of property of special importance) and a Ministerial Decree (referring to the property of special importance in the civil aviation field). Of special importance is the legislation regulating investment activities in Georgia, being a separate component of the CIP reform, which is not a subject of this very project.

All the above mentioned documents will be directly or indirectly affected by the CIP reform implementation. At the same time, creation of a modern regulatory framework, in the field of critical infrastructure protection, will be directly in line with the process of alignment of the framework with the European system, fulfilment of international commitments related to national security, as well as the implementation of standards and recommendations that have been set, throughout the years, by NATO, EU, UN and other actors.

Cybercrime

The cybercrime is progressing at an exceptionally fast pace, with new trends constantly emerging. Complex criminal networks operate across the world, exploiting digital technology for criminal purposes. Their methods are becoming more and more agile and intricate.

In Georgia, cybercrime is dealt with by a number of agencies, such as the Digital Governance Agency under the Ministry of Justice (with a Computer Emergency Response Team), the Prosecutor's office and the Ministry of Internal Affairs of Georgia assisted by LEPL Operative-Technical Agency (part of SSSG) in investigating most complex cybercrime or cyber-enabled offenses whereas final judgement on all cybercrime or cyber-enabled criminal cases is rendered by the national courts of Georgia (primarily City/Regional Courts, Courts of Appeal and Supreme Court)

The Prosecutor's Office of Georgia is responsible for procedural guidance of criminal investigations and supporting prosecution in court (including cybercrime cases), defining guidelines for criminal policy (including cybercrime); cooperation with multinational service providers on criminal cases.

Digital Governance Agency under the MoJ prepares draft legal acts regulating cyber security; establishes relations with local and international organisations and organisations of foreign countries, public institutions and entities regarding cyber security; submits information to foreign partners and organisations about the reforms and projects implemented by Georgia in the area of cyber security etc. DGA is also responsible to detect, manage and eliminate the computer security incidents at the 3rd Tier Critical Information System Subjects.

The Ministry of Internal Affairs (MIA) is the main law enforcement agency of the country and is one of the primary actors in the security sector, the functions of which include public order, traffic safety, crime investigation, preventative activities, state border protection, immigration and provision of public services (such as permits and licenses). The main goal of the Ministry is to reduce the number of offences, ensure the safe living environment for the public and protect human rights in compliance with the democratic standards. The general competence of the Ministry of Internal Affairs is to prevent, detect and eliminate cybercrime. As already mentioned above, MIA is assisted by SSSG OTA while investigating complex cybercrimes or other cyber-enabled offenses including the ones having high societal resonance.

Within the MIA, the responsibility of combating organized crime is distributed among several specialised bodies:

- In 2012, the Central Criminal Police Department (CCPD) established the Cyber Crime Division. The Division is investigating cybercrime offenses in a narrow sense, in particular crimes provided for in Chapter 15 (Cybercrime) of the Criminal Code, as well as proving advice, guidance and technical assistance to other police units across Georgia in investigations of cybercrime and handling of electronic evidence. Within the Department also operates 24/7 Unit in accordance with the Budapest Convention to exchange information between law-enforcement agencies of the Budapest Convention member countries.
- The Forensics-Criminalistics Department of the MIA has the Computer-Digital Forensics Sub-unit, which carries out functions of first handling and forensics of digital evidences.
- In April 2020, a new Cybercrime Division was established as part of the Tbilisi Police Department. The Division is responsible for investigating cybercrime registered in the Tbilisi region, mostly classified as Internet fraud, phishing and carding.
- The MIA Academy is a Legal Entity of Public Law under the MIA that conducts education and training of specialists of the law enforcement system, retraining of police officers and re-qualifying of in-service personnel. Currently, the Academy has two trainings specialised on issues related to the fight against cybercrime.

In order to strengthen its effort in fighting crime an Interagency Coordinating Council for Combatting Organized Crime was created in 2013. The main tasks of the Coordinating Council are:

- To define general policy for the fight against organized crime (including cybercrime);
- To elaborate, update and monitor the implementation of the Georgian National Strategy for Combatting Organized Crime and It’s action plan;
- To coordinate interagency activities for facilitating the implementation of relevant measures in the process of developing Strategy and its Action Plan.

Since cybercrime is a growing problem, it is crucial to have a comprehensive approach, focusing both on interdiction as well as on prevention of these type of crimes. Personnel working on cybercrime require consistent capacity building, since lack of appropriate trainings and specialization of investigators is a direct cause of ineffective, delayed investigations. It is equally important to build a higher awareness about cybercrime threats within the society. The excessive use of mobile devices and the Internet increases the exposure of both individuals and organizations to cybercrime, therefore it is vital for people to properly assess the risks and take appropriate measures against cybercrime. The primary tool for the prevention of these types of crimes is undoubtedly education aimed at building greater awareness and knowledge.

The biggest challenge for law enforcement in Georgia and across the world is to keep up with the digitalization and progression of new technologies, which are constantly exploited by criminals. Cybercriminals continue to evolve, tailoring their attacks using new methods and means. That is why, cybercrime investigations are often delayed in time and the clearance rates are significantly low.

The transnational and multidimensional nature of the internet is contributing to a rapid uptake in online criminality. Since cybercrime is often considered as a crime that does not have borders, it is important to enhance international cooperation between law enforcement agencies across the globe. If we are to develop a safer cyber space for everyone, all relevant stakeholders must share the responsibility of cooperation. The mutual efforts and coordinated approach will help the law enforcement agencies worldwide to enhance international security.

In conclusion, it is important to ensure that objectives set out in the National Strategy and Action Plan for Combating Organized Crime together with the EU - Georgia Association Agreement (AA) including Deep and Comprehensive Free Trade Area (DCFTA) are fulfilled, in conjunction with existing challenges, it is vital to constantly develop infrastructural and institutional capacities of the Ministry of Internal Affairs of Georgia, increase awareness about cybercrime threats within society for preventive measures, and enhance international cooperation. All of the listed challenges are addressed in the project's results and corresponding components.

Cyberterrorism

The Government of Georgia (GoG) conducts the organization of the country's fight against terrorism, and provides this effort with various resources, while the State Security Service of Georgia (SSSG) is the lead agency in the unified counter-terrorism system of the country. In order to protect the country against terrorist threats, joint efforts of the state agencies of Georgia are required. All the respective state authorities are engaged in the fight against terrorism within their scope of competence, and under the coordination of the SSSG. The SSSG organizes the fight against terrorism through its Counterterrorism Center, and cooperates closely with national as well as international partners.

The Permanent Interagency Commission established by GoG is the national cooperation and coordination mechanism responsible for determining Georgia's counter-terrorism policy, as well as developing respective national strategy and its action plan. The Interagency Commission is chaired by the Head of the State Security Service and includes as members all relevant competent authorities[9] engaged in the prevention of and fight against terrorism, in response to the current challenges of terrorism.

Georgia does not belong to the number of countries with high risk of terrorist attacks[10]. Nevertheless, considering the global security landscape, like in other countries, terrorism related challenges still exist, as no country is immune from this serious threat to international peace and security. At the national level the GoG continues to take effective and comprehensive counter-terrorism measures, carry out law enforcement measures, active domestic and international coordination and cooperation, as well as prevention-oriented

[9] Permanent Interagency Commission is chaired by the Head of the SSSG and composed of high level representatives of all relevant agencies: Administration of the Government; Ministry of Defense; Ministry of Justice; General Prosecutor's Office; Ministry of Internal Affairs; Ministry of Foreign Affairs; Ministry of Internally Displaced Persons from the Occupied Territories, Labor, Health and Social Affairs; Ministry of Education, Science, Culture and Sport; Office of the State Minister of Georgia for Reconciliation and Civic Equality; Ministry of Economy and Sustainable Development; Ministry of Finance; Financial Monitoring Service; Ministry of Environment Protection and Agriculture; Ministry of Regional Development and Infrastructure; LEPL - State Agency for Religious Issues; Special State Protection Service; Georgian Intelligence Service; National Bank of Georgia.

[10] According to the Global Terrorism Index 2020 (by Institution for Economics and Peace), measuring the impact of terrorism, Georgia ranks position - 100 out of 135, and the impact of terrorism in Georgia remains to be assessed as "very low" (available at: https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf). Furthermore, according to the U.S. Department of State recent Country Reports on Terrorism of 2018 (available at: https://www.state.gov/reports/country-reports-on-terrorism-2018/) and of 2019 (available at: https://www.state.gov/reports/country-reports-on-terrorism-2019/georgia/): There were no terrorist incidents in Georgia respectively in 2019 as well as in 2018. Also, the latest CoE Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval) 2020 Report on Georgia states that: "Georgia is not amongst countries with a high risk of terrorist attacks."

various projects and programs with the aim to reduce the threat.

In this course, Georgian legislation and the Chapter on Terrorism under the Criminal Code of Georgia (CCG) has been largely amended in line with international standards, to criminalize terrorism-related activities including the use of internet and cyberspace for terrorist purposes. The CCG *inter alia* explicitly criminalizes cyberterrorism (Art.324^1) amounting to illicit possession, use or threat to use computerized information protected by the law, what poses a threat of grave consequences perpetrated to intimidate the population and/or affect the authority.[11] Also, the National Strategy of Georgia on Fight against Terrorism further aims at the protection of its cyberspace against terrorist/extremist activities and attacks (under the pillar of protection).

Georgia has a sound legal framework for international cooperation. Georgia is a party to the fourteen (14) UN anti-terrorism conventions. Also, Georgia has already concluded over 30 cooperation agreements with international organization/partner countries in the field of fight against crime, *inter alia* addressing terrorism, as well as the Agreement on Operational and Strategic Cooperation with Europol. In terms of enhancing secure information exchange capabilities, Georgia has concluded agreements on exchange and mutual protection of classified information with 24 partner countries (*most of them are NATO and EU Member States*), as well as with the NATO and EU. It is further noteworthy that in 2019 Georgia announced support to the Christchurch Call, which is a France and New Zealand-led initiative and the commitment by Governments and tech companies to eliminate terrorist and violent extremist content online.[12]

Due to the constantly developing technologies and emerging terrorism-related challenges globally, Georgia continues an active work to combat using the internet for terrorist purposes and to protect the cyberspace against terrorist threats. The SSSG as the lead agency attaches huge importance to strengthening its capabilities of readiness and response in combatting cyberterrorism.

The SSSG is the country's lead agency in fight against terrorism and chair agency of the Permanent Inter-Agency Commission, has been actively involved in the enforcement and implementation of the Strategy-set objectives, including advancing its capabilities to combat cyberterrorism. In this respect, this Twinning project will enhance the awareness and specialization of the SSSG respective personnel involved in combatting cyberterrorism in line with internationally recognized standards and best practices, as well as broaden the SSSG's international partnership and operability to analyze international regulations and EU MS legal framework and IT systems on cyberterrorism.

3.2 Ongoing reforms:

Critical Infrastructure Protection

In 2018, the Ministry of Internal Affairs (MIA) acquired a coordinating role within the framework of the Interagency Commission entrusted with elaborating a general legal framework on critical infrastructure protection (CIP).

In 2019, in the framework of the cooperation between the Ministry of Internal Affairs (MIA) and the NATO Liaison Office (NLO) Georgia, with the involvement of the MIA employees and a local expert hired by the NLO, three important documents have been elaborated in the field of CIP:

- Initial sectoral gap analysis in the field of critical infrastructure protection (CIP);

[11] U.S. Department of State in its Country Reports on Terrorism 2019 notes that: "In January, recognizing the need for a whole-of-government response to the challenges of terrorism, the Georgian government approved the National Strategy of Georgia on the Fight Against Terrorism 2019-2021 with an accompanying action plan." Furthermore, the latest CoE Moneyval 2020 Report on Georgia states that: "Georgia has made substantial amendments to the legal framework with regard to the criminalization of terrorism and TF. There is now a sound legal basis for the investigation and prosecution of these offences."

[12] Available at: https://www.christchurchcall.com/supporters.html

- Review of the current legislation in the context of critical infrastructure protection (CIP);
- An initial Action Plan for the implementation of the reform in the field of critical infrastructure protection (CIP);

Within the TAIEX assistance, the review of the gap analysis and the initial draft legislative framework was conducted in January 2021. It envisaged elaboration of a new document which defined a vision on the future framework of the critical infrastructure protection (CIP). With an explicit leading role of the NSC Office, it aimed to elaborate a comprehensive National Strategy on Critical Infrastructure Protection (CIP), together with its Action Plan (AP).

In a parallel process, the NSC Office advances a "practical working direction" with the aim of identification of critical infrastructure subjects, elaboration of security standards for the safe and secure functioning of the critical infrastructure subjects and regulation of investment policy in relation to them.

Currently, Office of NSC has developed Draft Law "On Critical Infrastructure Protection" envisaging practical measures necessary to protect the Critical Infrastructure in Georgia starting from physical and perimeter security measures ended with investment screening and suspension thereof based on national security grounds. The future Twinning Project will aslo support implementation of the legislative pieces of the Law on Critical Infrastructure Protection.

Cybercrime

To cope with the existing problems and fulfil the objectives envisaged by the Strategy and Action Plan for Combating Organized Crime a special Cybercrime Working Group was established under the Interagency Coordinating Council (ICC) for Combatting Organised Crime (July 2020). The working group is comprised of representatives of MIA's relevant departments and other governmental agencies such as State Security Service, the Ministry of Finance, Prosecutor's Office, the Supreme Court, Levan Samkharauli National Forensics Bureau, and the Digital Governance Agency under the Ministry of Justice.

The Cybercrime Working Group is responsible for coordinating all anti-cybercrime activities at the policy/strategic level and ensuring sustainability of initiated reforms. The Working Group with the support of the EU funded project "Fight against Organized Crime" elaborated the Cybercrime Road Map complementary to the new National Strategy on Combatting Organised Crime in 2021-2025 and Action Plan for 2021-2022.

Currently, Office of NSC is also negotiating with MIA to get engaged into this process with the aim to provide its input serving capacity building of the agencies involved in fighting cybercrime including through international support.

Cyberterrorism

In 2018 the GoG established (*Decree №469)* a Permanent Interagency Commission as the national cooperation and coordination mechanism responsible for determining Georgia's counter-terrorism policy, developing and monitoring the implementation of national counter-terrorism strategy and its action plan. The Permanent Inter-Agency Commission (*composed of representatives of all relevant agencies responsible for the prevention and countering terrorism in the country and chaired by the SSSG*) elaborated and on 23 January 2019, the GoG approved National Strategy of Georgia on Fight against Terrorism and its Action Plan for 2019-2021, which *inter alia* aims at the protection of its cyberspace against terrorist/extremist activities and attacks (under the pillar of protection).

Georgia continues taking steps to effectively implement its comprehensive National Strategy on Fight against Terrorism and its Action Plan. In this regard, four inter-agency thematic working groups (WG on information gathering and analysis; WG on supporting the measures in the direction of prevention; WG on supporting the measures in the directions of protection and preparedness; WG on developing legal framework and supporting international cooperation) have been created according to the main objectives[13] of the Strategy and AP. Several meetings of the WGs have been organized to facilitate proper implementation of the Strategy and its AP. Moreover, the involved agencies have developed their intra-agency mechanisms.

General Policy and legislative process

The National Policy Planning System Reform Strategy, adopted by the Government of Georgia in August 2015 recognizes the current weak link between the policy planning process and legislation drafting, the absence of practice of legislative impact assessment and the weak institutional capacity of ministries in legal drafting. The OECD/SIGMA 2018 assessment in the policy development and coordination area highlights a number of weaknesses in the quality of policy planning (costing, monitoring, coordination and public consultation), which are currently being addressed through the PAR roadmap and action plan. The document specifically notes the reoccurring problem with implementation of laws, which can be attributed to the low quality of laws due to weaknesses in the law-making process. There is a pressure to complete numerous legal reforms in the shortest possible time. Improvement of the legislative drafting process and quality of legislation is now a priority area of action for the Administration of Government under the Prime Minister (steering the policy-making process) and all line ministries. This primarily involves the Administration of Government, Ministry of Justice, and Ministry of Economy and Sustainable Development. In order to meet the targets and obligations in law making process the Government introduced changes in Law on Normative acts (amended on June 13, 2018) and Regulation of the Government (amended on August 24, 2018). These amendments put more emphasis on concordance with EU acquis and Regulatory Impact Assessment (RIA).

In line with the 2018 OECD/SIGMA recommendations, a new Government decree was adopted end 2019 and with its supporting Handbook on Public Policy Making, now lays the regulatory and procedural foundation for good evidence-based policy development. It has quickly become the primary guidance document for Ministries. Nevertheless, its implementation requires comprehensive training and support, to ensure better integration between policy and budget planning, and building the right capacities, structures and processes in the relevant ministries. Some key issues in the area are inter- and intra-institutions coordination, capacities in data analysis, policy budgeting, gender responsive budgeting. The introduction of a mandatory Regulatory Impact Assessment for specific legislation since January 2020 is also an important milestone, but also requires extensive training for proper implementation.

For increasing coordination and strengthening effectiveness of the legal approximation process in the country, on January 30, 2020 Government of Georgia adopted Legal Approximation Guidelines [14] that will provide additional guidance to all the line Ministries involved in the legal approximation process under the AA. The Guidelines prepared by the Ministry of Justice provide key principles and techniques of approximation that will assist and orient legal drafters throughout the approximation process. The Guidelines should be used consistently, not only

[13] The Strategy is composed **of seven pillars**, namely: *obtaining and analyzing terrorism, extremism and radicalization-related information; prevention; protection; preparedness; prosecution; development of legislative framework and international cooperation.*

[14] https://matsne.gov.ge/document/view/4786582?publication=0

by MoJ, but also by all line ministries, and institutions tasked with the approximation exercise. Such proceedings will help to ensure the achievement of a steady and sustainable approximation path.

3.3 Linked activities:

Critical Infrastructure Protection

In the recent years, a number of projects have been contributing (including with the support of international donors and partners) to strengthening of the CIP in Georgia:

The support, currently provided by the EU, is materialized in the ongoing assistance implemented within the TAIEX instrument (Review of the gap analysis document in the field of critical infrastructure protection (CIP) and the respective draft Legislation – 01.2021). The respective intervention concentrated on the review of the gap analysis document and the initial draft legislative framework. Hence, the respective activity will significantly contribute to the development of the legal and conceptual framework in the CIP field, which is an important component of the overall reform. This strand of action will now be flanked with the TWINNING project targeting "practical component" of the reform, i.e. identification of critical infrastructure subjects and elaboration of their security standards.

NATO Liaison Office (NLO) Georgia is planning to support the ongoing CIP reform with the respective experience sharing events related to particular reform components. The US Embassy is also supporting the NSC Office in organization of workshops on the investment screening models applicable to the critical infrastructure subjects. The US side ensures not only the experience sharing with regard to the US investment screening systems, as such, but also provides the opportunities for getting familiar with the systems of particular EU Member States in the field (e.g. at the most recent workshops, the Georgian side had an opportunity to get familiar with the German and Czech investment screening mechanisms).

Georgia counts on active cooperation, with the EU, *inter alia* within the framework of the European Programme for Critical Infrastructure Protection (EPCIP). Namely, at the very beginning of CIP Reform in Georgia, EPCIP delivered key Workshop providing insights into EU policy and regulatory framework on identification and classification of critical infrastructure subjects that was of a major use for Georgian side while drafting the Law on Critical Infrastructure Protection. Once the latter will be finally approved by the Georgian Parliament, NSC together with sectoral agencies plans to continue this cooperation in future while developing various SOPs, Incident Response and Handling Manuals stemmed from the Draft Law. Critical infrastructure protection (CIP) is an important cooperation domain in the Eastern Partnership (EaP) framework, being one of the components of EaP deliverables post 2020 Eastern Partnership priorities.

However, the assistance provided so far is not enough considering that enforcement of CIP Legislation requires intensive amendments into other regulatory framework, in particular the ones defining perimeter security, investment and equity screening at the CIP Subjects.

Cybercrime

The MIA has established cooperation and received support for combatting cybercrime from several international organisations and partner countries, including the EU, Europol, Council of Europe, OSCE, ICPO-INTERPOL, IOM, NATO, FBI, Estonia, France, Lithuania, United Kingdom, and the USA. Some of the more significant examples of international cooperation are mentioned below:

In August 2018, EU launched a project Technical Assistance to Support the Fight against

Organised Crime in Georgia. It comprises of eight specific result areas, one of which is addressing cybercrime. The project supported the MIA and the Interagency Coordinating Council to elaborate a new National Strategy and Action Plan for Combatting Organised Crime, and, as part of the National Strategy, a Road Map on building sufficient capacity within the MIA to fight cybercrime in line with European standards ("the Cybercrime Road Map").

The joint EU-Council of Europe CyberEast Project was launched in September 2019. The project aims at adopting legislative and policy frameworks compliant to the Budapest Convention on Cybercrime, reinforcing the capacities of judicial and law enforcement authorities and interagency cooperation, and increasing efficient international cooperation and trust on criminal justice, cybercrime and electronic evidence, including between service providers and law enforcement. It is implemented in the Eastern Partnership region under the European the Neighbourhood East Instrument (ENI) with Georgia participating along with Armenia, Azerbaijan, Belarus, Moldova and Ukraine. In future, Georgian side is planning to use Project's resources with the aim to deliver various certification courses and organize certifications for Georgian law enforcement and security agencies (OTA, CSB, DGA, MIA, POG, FIS, National Forensic Bureau and NSC) considering the requirements of the Law "On Information Security" enacted by 30 December 2021 given the specificity of the Twinning mandate and limits on resources of the Project in future[15].

The new project "Training and Operational Partnership against Organized Crime" financed by the European Commission commenced in 2020 year. The project aims to strengthen strategic and operational cooperation between law enforcement authorities in the EAP countries, EU MS and EU agencies; building the capacity of relevant law enforcement services of the partner countries to fight against organized and serious international crime including cybercrime.

Another project that will actively commence in the end of 2021 is "Fighting Organized Crime in the Eastern Partnership Region". The project aims to enhance expertise and skills of partner countries on the EU crime policy, strengthening operational capacities of the Eastern Partnership countries and deepening cooperation with the EU countries and agencies.

Cyberterrorism and Combatting against Other APT Attacks

Georgia is actively involved in international efforts and will continue to pursue the fight against terrorism in all its manifestations, alongside the international community. The SSSG has an efficient practice of active cooperation with the UN, NATO, EU, CoE,[16] OSCE, INTERPOL and other regional and international organizations, including being actively engaged in cooperation dialogue with them, sharing experience and best practices as well as carrying out joint activities, regular meetings, trainings and measures in the fight against terrorism in all its manifestations.

The SSSG actively cooperates and directly shares information on terrorism with relevant authorities of partner countries and international organizations, based on international multilateral or bilateral agreements and national legislation, including via regular meeting, the secure channels as well as a network of liaison officers and security/police attaches of Georgia

[15] Certification of Georgian Officers shall be conducted under internationally recognized certification frameworks that are also valid in EU Member States. The same applies to the courses provided by various commercial vendors. Namely, Georgian side will only request the trainings from those commercial entities recognized by the Twinning Partner country as well as in wider EU context, within the limitations applicable to the twinning projects implementation.

[16] It is noteworthy *inter alia:* the CoE/EU Partnership for Good Governance (PGG II) Project on "Enhancing the systems of prevention and combating corruption, money laundering and terrorist financing in Georgia".

and other countries.

Georgia has become an active member of the Global Coalition against Daesh from the very beginning, and inter alia the SSSG respective representatives have participated in the working process of the CWG Digital and Social Media Action Group of the Global Coalition against Daesh.

This project offers a valuable assistance in implementing Georgia's efforts in countering cyberterrorism, in close cooperation and experience-sharing with international partners.

Related Programmes:

This Twinning project will be implemented under the five-year "SAFE: EU4 Security, Accountability and Fight against Crime in Georgia" Programme, which focuses on the fight against crime, hybrid and emerging threats, border management, civil protection and supervision of the security sector.

Another Twinning project "Strengthening Cybersecurity Capacities in Georgia" envisaged by SAFE (Beneficiary: Digital Governance Agency of the MoJ) has started in November 2020 and will run until November 2022. The project supports the implementation of the ongoing reform in the cybersecurity field aimed at creating an enhanced structural framework in the field, with clearly defined roles and responsibilities of the respective actors. Besides the components of the reform of the information security legislation and the delivery of the draft National Cybersecurity Strategy, the project also refers to the identification of critical information infrastructures and operators of essential services. The latter working direction serves one of the most important aims of the current reform in the cybersecurity domain, namely the expansion of the list of critical information system subjects (CISSs) to the private sector. The latter strand of action will, on its part, inform the general CIP reform, as certain CISSs will eventually be entailed in the list of general critical infrastructure.

Enhancement of MIA capabilities in cooperation with the EU and its Member States through the procurement of various equipment is also envisaged under SAFE programme.

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

EU-Georgia Association Agreement aims to strengthen the Georgian public institutions' capacity to fight against organised crime, including cybercrime. **2017 – 2020 Association Agenda between the European Union and Georgia** refers to enhancing cooperation in addressing cybercrime and cyberterrorism.

Georgia implements a comprehensive reform in the CIP field, in order to ensure the compatibility of its emerging system with international standards. In the latter context, the EU **Directive 2008/114/EC** is one of the most important instruments the compliance with which will be sought.

The **Convention on Cybercrime of the Council of Europe (CETS No.185)**, known as the Budapest Convention, is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty. Under the Budapest convention, Article 35 "Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network."

Under this project Georgia aims to continue best practice-sharing, implementing EU and internationally-acknowledged standards as well as sharing experience of partner countries in line with AA under Article 12 (**Fight against terrorism**) and the United Nations Global

Counter-Terrorism Strategy as well as relevant UNSC resolutions.

3.5 Components and results per component

The results to be achieved under this Twinning are detailed below for each one of the mandatory results. There are three main beneficiaries in this Twinning project: NSC Office, MIA and SSSG; each entity will be targeted separately through the respective mandatory results / components and several sub-results.

Mandatory Result 1 / Component 1 – Sectoral and National level CI subjects identified and safe and secure functioning ensured

For the timely and adequate reaction to sustainable socio-economic development and threats of the country, it is especially important to define and protect the objects, services, systems and their parts that are functional and strategically influential for the state. If those mentioned above are being destroyed or demolished than the threat towards national interests will significantly increase, national security will also be affected, lives of citizens and their wellbeing, as well as socio economic state will all fall under a significant threat. Taking into consideration the abovementioned, identification of sectoral and national level CI subjects is priority of the country.

The support provided by the project in establishment of safe and secure functioning of CI is one of the decisive factors for successful implementation of the CI reform.

Sub-result 1.1 - Threat, impact and risk assessment methodologies including sectoral Standard Operating Procedures elaborated and implemented

Identification of CI subjects is one of the main priorities of the CIP reform. In order to elaborate the respective identification criteria, it is important to implement threat, risk and impact assessment in relevant sectors/agencies. Therefore, elaboration of the respective assessment methodologies is the issue of current importance.

Preparation, for the assessment, on the basis of elaborated methodologies, aimed at delivering sectoral and national criteria for the identification of critical infrastructure subjects will be the responsibility of the respective stakeholders and experts. The methodologies will be implemented across all the relevant sectors and in the respective agencies, with the aim of delivering CI identification criteria. Methodology documents shall also involve crisis management SOPs in critical infrastructure. NSC is currently developing general scheme of the mentioned Document.

Sub-result 1.2 Critical infrastructure identification criteria delivered

The delivery of the CI identification criteria is the key point for the development of the CIP reform. It serves the identification of the CI subjects which will be included in the national list. The respective subjects will be identified as critical for the state / society and their protection will be one of the main priorities of the security policy implemented by the state.

Sub-result 1.3 Protection standards for CI subjects delivered

Measures (controls and actions to address risks) for the safe and secure functioning of CI subjects are of overwhelming importance. They guarantee the protection of the subjects entailed in the respective national list and ensure the uninterrupted provision of vital functions / services for the state and society. Accordingly, the respective strand of action is aimed at elaboration of sectoral as well as general security standards of CI subjects. After the delivery of the abovementioned standards, monitoring of their implementation will be the responsibility of all the relevant stakeholders at all levels, from tactical to strategic. Hence, the respective CI operators, sectoral agencies, a coordinating agency as well as the Government, in general, will be involved in the process of ensuring critical infrastructure protection (CIP).

Mandatory Result 2 / Component 2: Capacities of the MIA to prevent and combat Cybercrime and other cyber-enabled offenses strengthened

Component envisages enhancing International cooperation regarding joint cybercrime cases and sharing of electronic evidence. It will focus on implementing preventive activities to inform the society about ways to protect itself from possible cyberattacks. To measure the awareness of the society and the progress achieved through information campaigns that will be carried out within the framework of the project, it is recommended to conduct two small scale surveys: 1) to measure society's current awareness regarding cyber threats and measures against it (baseline survey) and 2) a survey after the information campaigns (to measure the progress reached after preventive measures). The exact methodology to be agreed upon start of the project implementation.

Special attention to be paid to the capacity building of employees of MIA working under the Cybercrime Unit of the Central Criminal Police Department, Tbilisi Police Department, MIA Academy's relevant staff as well as members of Fight against Cybercrime Working Group through various activities such as trainings, experience sharing, etc.

The particular focus shall be given to computer forensics, malware analytics, reverse engineering and mobile forensics together with online undercover operations and network traffic capture/analytics. Considering that MIA often conducts joint operations with partner law enforcement or security agencies in Georgia, it would be of utmost importance if those capacity building activities will have inter agency character involving joint action from MIA National Security Council and State Security Service, of course, with MIA's prevailing participation. As previous practice demonstrates, for quality control and certification purposes, delivery of those trainings from internationally recognized vendors shall be the most feasible option.

Sub-Result 2.1: International cooperation of MIA in the field of Cybercrime enhanced

The sub-result will ensure that joint action regarding fight against cybercrime are put in practice on bilateral and multilateral level. In this process, set-up and operation of the Joint Investigation Teams according to EUROPOL standards and best practices is of utmost importance both on national and international levels. In line with this practice, MIA can work effectively with partner agencies (OTA, CSB, DGA and NSC) in the process of setting up and operation of Security Operations Centers during handling of major cyber incidents. Therefore, capacity building on those items from EU Member States or from Official Law Enforcement Institutions is of utmost importance.

Sub-Result 2.2: Awareness on cybercrime threats raised

Sub-result is designed to further increase public awareness regarding cyber threats within the society. The awareness could be increased via campaigns that include TV / radio / social networks advertisements; Information banners; Booklets; Informing companies through various sources. In the process, there is envisaged to carry out 2 small scale awareness raising surveys as abovementioned.

Sub-Result 2.3: Qualification of personnel working on interdiction and prevention of cybercrime increased

Sub-result envisages further capacity building activities for the MIA employees (including MIA’s partner law enforcement and security agencies) working on cybercrime cases. Such as trainings/workshops conducted by international experts; further experience sharing meetings, visits, and research papers. It should be highlighted that the MIA Academy is an important structural unit responsible for educating employees of the MIA. Sub-result will elaborate educational courses that will ensure the long term sustainability of quality education of the relevant MIA staff.

As already mentioned above, MIA attaches particular significance to the certification process of its officers taking into account that evidences gathered during the criminal investigations requires proper research and authentication at the trials for which official proof of competence on behalf of forensic examiners or investigators attains additional value. The latter is even higher when internationally recognized vendors are engaged in this process.

Following the same rationale, MIA suggests these trainings to have interagency dimension including MIA, NSC and SSSG, since partner law enforcement or security agencies regularly work with MIA on various cybercrime, cyber-enabled offenses and necessary digital forensics thereof.

Mandatory Result 3 / Component 3: Resilience against cyberterrorism by advancing capacities for SSSG,CSB, DGA, NSC further improved

The component will focus on improving and advancing SSSG, as primary agency when combatting cyberterrorism and other APT threats. However, other sectoral agencies such as CSB and DGA are also responders when such incidents occur. Involvement of the NSC, which is the major national security policy planning agency including on cybersecurity matters together with other actors in the awareness and capability building activities especially considering the challenges of constantly changing landscape of terrorism and current developments in digital era is of utmost importance.

Sub-result 3.1: Capacity of SSSG and other CIP subjects’ relevant staff (and other relevant Sectoral Agencies) involved in combatting cyberterrorism and other APT attacks strengthened

This sub-result will focus on specialized and advanced training courses for SSSG, NSC and other relevant Sectoral Agencies, also experience sharing activities conducted by highly experienced institutions/ specialized research centers having experience of working with security sector domain, in line with internationally recognized standards and best practices;
Special attention will also be given to the awareness about cybersecurity threats, such as e.g. Data Wiping attacks against SCADA systems, Info Storage and Data Bases and etc.

Sub-result 3.2: International Cooperation of SSSG enhanced

This sub-result will focus on broadening international partnership with similar EU member state institutions to increase SSSG’s analysis on regulating cyberterrorism in line with current developments and emerging trends

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

The project will be implemented in the form of a TWINNING contract between the Beneficiary Country and EU Member State(s). Implementation of the project requires the engagement of one Project Leader (PL) with responsibility for the overall coordination of project activities and one Resident Twinning Adviser (RTA) to manage implementation of project activities, as well as Component Leaders (CL) and pool of short-term experts within the limits of the budget. It is essential that the team has sufficiently broad expertise to cover all areas included in the project description.

Proposals submitted by the EU Member State shall be concise and focused on the strategy and methodology and an indicative timetable underpinning this, the administrative model suggested, the quality of the expertise to be mobilised and clearly show the administrative structure and capacity of the Member State entities. Proposals shall be detailed enough to respond adequately to the TWINNING Fiche, but are not expected to contain a fully elaborated project. They shall contain enough details about the strategy and methodology and indicate the sequencing and mention key activities during the implementation of the project to ensure the achievement of overall and specific objectives and mandatory results/outputs.

The interested Member State(s) shall include in their proposal the CVs of the designated Project Leader (PL) and the Resident Twinning Advisor (RTA), as well as the CVs of the potentially designated Component Leaders-(CLs).

The TWINNING project will be implemented by close co-operation between the partners aiming to achieve the mandatory results in a sustainable manner.

The set of proposed activities will be further developed with the TWINNING partners when drafting the initial work plan and successive rolling work plan every three months, keeping in mind that the final list of activities will be decided in cooperation with the TWINNING partner. The components are closely interlinked and need to be sequenced accordingly.

3.6.1 Profile and tasks of the PL:

The Member State PL should have the capacity to lead the implementation of the project and the ability to mobilize the necessary expertise in support of project's efficient implementation. She/he will be expected to devote a minimum of 3 days per month to the project in his/her home administration. In addition, as co-chairperson, he/she will coordinate from the Member State side the work of the Project Steering Committee (PSC), which shall meet in Georgia on a quarterly basis at least.

Profile:

- A current managerial level official of a Member State administration in a relevant field;
- University level education in a relevant discipline, or equivalent professional experience in a related field of 8 years;
- Relevant managerial position in policy development/implementation/coordination in the respective field;
- At least 3 years' experience in the field of critical infrastructure protection (CIP);
- Good understanding of regulatory/institutional system of the CIP, and its organisational model in the respective EU Member State;
- Previous experience in the field of project management, with a demonstrable record of organisational leadership and reform implementation;

- Knowledge of EU CIP-related legislation and the respective standards;
- Good knowledge of legal approximation process, relevant EU legislation and institutional requirements related to various components of this project;
- Experience in international collaboration in the CIP field;
- Experience in the domain of identification of critical infrastructure subjects and elaboration of their security standards would be an asset;
- Good understanding of cybercrime and cyberterrorism field would be an asset;
- Excellent command of spoken and written English;
- Good communication, presentation and interpersonal skills;
- Good leadership and managerial skills;
- Excellent Computer literacy.

Tasks:

- Overall direction, supervision, guidance and monitoring of the project;
- Mobilization of the necessary expertise in support of the efficient implementation of the project;
- In cooperation with the PL counterpart signing and submission of the interim quarterly and final project reports prepared with the support of the RTA to the concerned authorities;
- Formal signing of project work plan(s) and/or their updates;
- Ensuring timely achievement of the project results;
- Provision of legal and technical advice whenever needed;
- Co-chairing of project steering committees.

3.6.2 Profile and tasks of the RTA:

The RTA will be located in the premises of the NSC office on a fulltime basis and will be responsible for the direct implementation of the project under the overall supervision of the MS Project Leader.

He/she will work closely with the BC Project Leader and the RTA Counterpart to deliver the project outputs.

The RTA will maintain day-to-day cooperation with the beneficiary administration and coordinate the work performed by the STEs for the whole duration of the project implementation. The RTA will have a key role in the coordination of the inputs required for the successful implementation of all the project activities.

The RTA should be supported by a permanent RTA Assistant. The RTA assistant should work in close collaboration with the beneficiary administration BA. The RTA assistant will perform general project duties and will be providing translation and interpretation services as necessary, practical arrangements for the project, such as organizational issues of expert missions, conferences, training, seminars, maintaining project records and etc. Until the RTA can select and hire an assistant, the Beneficiary administration will make a member of its staff available to support the RTA in his/her daily tasks.

A full-time language assistant should also be recruited. She/he should perform most of the required interpretation/translation services. She/he will provide day-to-day interpretation/translation to the RTA and project experts during missions.
Whenever required and needed for simultaneous interpretation during seminars and workshops, translation of large volume of documents additional interpretation may be procured and funded by the project.
Minimum two visibility events will be organized in the course of the implementation of the project. Kick-off meeting at the start of the implementation and the Final meeting at the end of the implementation of the project activities. These will have to be coordinated with the EU Delegation to Georgia.

Profile:

- University level education in a relevant discipline or equivalent professional experience in a related field of 8 years;
- Proven contractual relation to a Member State administration or mandated body;
- At least 3 years of professional experience in the CIP field;
- Good knowledge of legal approximation process, relevant EU legislation and institutional requirements related to various components of this project;
- Sound knowledge of CIP, management, quality control and supervision;
- Working experience on EU CIP legislation and policy, in a Member State, would be an asset;
- Experience in the domain of identification of critical infrastructure subjects and elaboration of their security standards would be an asset;
- Experience in the elaboration and implementation of risk, threat and impact assessment methodologies, with the aim of identification of critical infrastructure subjects (optional but if present, preferential for the project purposes);
- Collaboration experience with international organisations / actors, in the CIP field, would be an asset;
- Good understanding of cybercrime and cyberterrorism field would be an asset;
- Good team-working, communications, presentation and interpersonal skills;
- Good organisational and project management skills;
- Strong analytical and report writing skills;
- Excellent command of spoken and written English;
- Good Computer literacy;
- Previous experience in project management would be an asset.

Tasks:

- Overall coordination of project implementation and of all activities;
- Development of initial and subsequent work plans, and project progress reports, together with PL, to be submitted to the Steering Committees;
- Coordination of activities of the team members in line with the agreed work plan

to monitor quality of their outputs and enable timely completion of project outputs;

- In coordination with MS PL, liaise with PL counterparts and daily contacts with RTA counterpart;
- Liaise with EUD Project Manager and Programme Administration Office (PAO);
- Liaise with key stakeholders, other relevant projects and relevant Georgian institutions.
- Contribute to the work of the sector development process set up in the Beneficiary Country.

3.6.3 Profile and tasks of Component Leaders*:*

To achieve coherence in the implementation of all activities pertaining to the specific components and accomplish mandatory results/outputs, Component Leaders (short-term experts) will be designated to each specific component who will coordinate the intervention of all other Member State experts mobilized for the same component. Beneficiary institution will assign a Component Leader counterpart for each component who will be the permanent interlocutor of the MS Component Leader coordinating the specific component. The Component Leaders will work in close collaboration with the RTA and the Beneficiary counterparts in order to achieve mandatory results/outputs pertaining to the specific component and to contribute to overall success of the project.

The profile, exact number and specific Terms of Reference for each Component Leader along with the names and functions of the Component Leader counterparts will be defined at the Work Plan preparation stage by the MS Project leaders and/or the RTA and its counterpart. The ToR will specify the detailed inputs of the Component Leaders and the duration of their missions.

Component 1: Sectoral and National level CI subjects identified and safe and secure functioning ensured:

Profile:

- University level education in a relevant discipline or equivalent professional experience in a related field of 8 years;
- At least 3 years of professional experience in the CIP field;
- Sound knowledge of CIP related governance models and controlling/supervisory institutional structures in their MS;
- Good knowledge of strategy and policy issues, legal approximation process, relevant EU legislation and policy, as well as institutional requirements related to this component;
- Good understanding of legal and policy issues, operational procedures relevant to this component;
- Demonstrated skills for effective negotiation, inter-personal, inter-institutional and political dialogue;
- Experience in the domain of identification of critical infrastructure subjects and elaboration of their security standards would be an asset;
- Experience in the elaboration and implementation of risk, threat and impact

assessment methodologies, with the aim of identification of critical infrastructure subjects (optional but if present, preferential for the project purposes);

- Strong analytical and report writing skills;
- Good organisational and mentoring skills;
- Good team-working, communication, presentation and advisory skills;
- Fluency in written and spoken English;
- Computer literacy.

Tasks:

- Component coordination, guidance and monitoring;
- Provide technical advice, support and assist the BC institution in the context of the project's components;
- Provide practical expertise/advice to relevant staff for execution of different tasks related to the project;
- Contribute to the project reporting, to drafting the notes and other documents and reports on experts missions;
- Contributing to preparing and conducting training programs, information and dissemination seminars with various stakeholders;
- Contributing to the interim and final reports.
- Liaise with PL, RTA and their counterparts.

Component 2: Capacities of the MIA to prevent and combat Cybercrime strengthened

Profile:

- University level education in a relevant discipline or equivalent professional experience in a related field of 8 years;
- At least 3 years of professional experience in the cybercrime investigation;
- Good knowledge of strategy, legal approximation process, relevant EU legislation, as well as institutional requirements related to this component;
- Good understanding of policy issues, operational procedures relevant to this component;
- Experience in developing of training modules and materials, good record in training delivery;
- Experience in awareness raising, information campaigns and knowledge of different communication tools;
- Demonstrated skills for effective negotiation, inter-personal, inter-institutional and political dialogue;
- Strong analytical and report writing skills;
- Good organisational and mentoring skills;
- Good team-working, communication, presentation and advisory skills;
- Fluency in written and spoken English;

- Computer literacy.

Tasks:

- Component coordination, guidance and monitoring;
- Provide technical advice, support and assist the BC institution in the context of the project's components;
- Provide practical expertise/advice to relevant staff for execution of different tasks related to the project;
- Contribute to the project reporting, to drafting the notes and other documents and reports on experts missions;
- Contributing to preparing and conducting training programs, information and dissemination seminars with various stakeholders;
- Contributing to the interim and final reports.
- Liaise with PL, RTA and their counterparts.

Component 3: Resilience against cyberterrorism by advancing capacities for SSSG further improved

Profile:

- University level education in a relevant discipline or equivalent professional experience in a related field of 8 years;
- At least 3 years of professional experience in the cyberterrorism field;
- Good knowledge of component-related EU legislation, strategy and policy issues, as well as institutional structures in their MS;
- Good understanding of legal and policy issues, operational procedures relevant to this component;
- Good knowledge of relevant IT systems applied in cyberterrorism;
- Good communication, coaching and mentoring skills;
- Strong analytical and report writing skills;
- Good organisational and managerial skills;
- Good team-working, presentation and advisory skills;
- Fluency in written and spoken English;
- Computer literacy.

Tasks:

- Component coordination, guidance and monitoring, in close collaboration with SSSG;
- Provide technical advice, support and assist the SSSG in the context of the project's components;
- Provide practical expertise/advice to relevant staff for execution of different tasks related to the project;

- Contribute to the project reporting, to drafting the notes, reports and other documents, in close collaboration with SSSG;
- Contributing to preparing and conducting capacity-building and experience-sharing activities with various stakeholders;
- Preparing timely proposals for effective execution of this component;
- Contributing to the interim and final reports;
- Liaise with PL, RTA and their counterparts.

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

In order to provide the full range of expertise necessary, short-term experts will be drawn from different skill sets to assist the RTA on specific activities. Based on the project results, there might be the need of having different STEs possessing the following professional experience depending on their area of intervention:

Profile:

- University level education in a relevant discipline or equivalent professional experience in a related field of 8 years;
- At least 3 years of professional experience in the fields relevant to the project;
- Specific knowledge and working experience on legal approximation and policy issues, with focus on identification of critical infrastructure subjects and elaboration of their security standards;
- Experience in harmonizing national law of any Member State with the EU Directive 2008/114/EC would be an asset;
- Specific knowledge of organisational structure, statutory models and institutional capacities in the CIP field in MSs;
- Experience in the domain of identification of critical infrastructure subjects and elaboration of their security standards would be an asset;
- Experience in the elaboration and implementation of risk, threat and impact assessment methodologies, with the aim of identification of critical infrastructure subjects (optional but if present, preferential for the project purposes);
- Sound knowledge and particular skills in strategy and policy development;
- Experience in awareness raising, information campaigns and knowledge of different communication tools;
- Specific knowledge and working experience on legal and policy issues, with focus on technical requirement for combatting and investigating the cybercrime and cyberterrorism;
- Sound knowledge and particular skills in material-technical development and capacity building in combating cybercrime and cyberterrorism;
- Experience in developing of training modules and materials, good record in training delivery;
- Experience in awareness raising, information campaigns and knowledge of different communication tools;
- Good knowledge of relevant IT systems applied in cyberterrorism;
- Coaching, training and facilitator skills;
- Previous experience in similar projects would be considered as an asset.
- Good team-working, communication, presentation and interpersonal skills;
- Fluency in written and spoken English;

- Good computer literacy.

Tasks:

- Contributing in drafting project related legal and policy documents (methodologies) in their respective fields;
- Contributing in preparation of guidelines, operational procedures and manuals/instruction handbooks related to their field of expertise;
- Assistance with the preparation of trainings, conferences, workshops, seminars etc.;
- Contributing to the sustainability of the project by ensuring that aspects of the project related to their field of expertise are implemented timely and properly;
- Provision of legal and/or technical advice and consultations whenever needed in their respective fields;
- Preparing timely proposals for any corrective measures;

Proposals shall include only the CVs of the proposed PL, of the RTA and of the Component Leaders (STEs CV should not be included in the MS proposal).
The Project Leader/RTA are free to propose additional STEs as they see fit, based upon the needs of the project and in agreement with the beneficiary.

4. Budget

The budget for this grant is EUR 1.300.000 (one million three hundred thousand Euro).

5. Implementation Arrangements

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

The EU Delegation to Georgia will be responsible for tendering, contracting, payments and financial reporting and will work in close cooperation with the Beneficiary Administration. The person in charge of this project, within the EU Delegation to Georgia, is:

Ms. Lali Chkhetia

Programme Officer

Delegation of the European Union to Georgia

64b, Chavchavadze Avenue

0179 Tbilisi, Georgia

Tel.: +995-32-2 364 364

E-mail: Lali.CHKHETIA@eeas.europa.eu

5.2 Institutional framework

This Twinning Project has multi-stakeholder dimension from institutional standpoint, considering the diverse nature of national security, including cyber-security related challenges globally, as well as the high significance of further advancing resilience of Georgia against cybercrime, cyberterrorism and other threats to critical infrastructure protection.

The **NSC Office** is comprised of four structural units / departments and for the time being, the coordination of the CIP reform directly falls within the purview of competencies of the largest structural unit of the NSC Office, namely the Internal and External Security Affairs Department. More precisely, it is a responsibility of the Division on Socio-economic and Energy Security Affairs. Of course, there already are certain cross-cutting issues which also fall under the purview of competencies of other structural units, especially the National Crisis Management Centre (Department), but the coordination function, as such, is ascribed to the Department of Internal and External Security Affairs. Donor assistance through the SAFE Program and the present TWINNING project, as such, will not lead to a change in the institutional framework. Please find annex 2 about institutional structure of the beneficiary.

The **Ministry of Internal Affairs (MIA)** is the main law enforcement institution in the country and is one of the primary actors in the security sector. In relation to this project, the general competence of the Ministry of Internal Affairs is to prevent, detect and eliminate cybercrime. The departments involved in the project implementation are Central Criminal Police Department, the Tbilisi Police Department, the Information-analytical Department and Legal Entity of Public Law – Academy of the Ministry. These units will be actively engaged in the working process with close cooperation with the International Relations Department (IRD) of the MIA. Specifically, the Project Management Division of the IRD will ensure proper coordination and smooth implementation of the project. Please find annex 2 about institutional structure of the beneficiary.

In the course of multi-stakeholder approach under this Project, **the State Security Service of Georgia** will act as direct beneficiary for cyberterrorism component. Namely, the SSSG coordinates the country’s counter-terrorism measures through its Counterterrorism Center. Hence, the Counterterrorism Center which has the competence to detect, deter, investigate and respond to terrorism threats and incidents, will be involved in the project implementation along with the SSSG LEPL - Operative Technical Agency of Georgia, the latter has no investigative or intelligence functions and is solely responsible for ensuring IT support to the law enforcement and security services in line with the legislation requirements, as well as along with the SSSG LEPL – Training Center and SSSG Administration, while the latter will ensure the overall coordination of the project implementation at the SSSG level. Furthermore, the SSSG, within its competence, will closely collaborate with other involved institutions under the overall Project framework.

5.3 Counterparts in the Beneficiary administration:

The PL and RTA counterparts will be staff of the Beneficiary administration and will be actively involved in the management and coordination of the project.

5.3.1 RTA Counterpart:

Mr. Grigol Modebadze
Head of Socio-Economic and Energy Security Affairs Division
Internal and External Security Affairs Department
Office of the National Security Council
7 Ingorokva Str., 0114 Tbilisi, Georgia

5.3.2 Contact person from NSC:

Mr. Giorgi Tielidze
Head of Information and Cybersecurity Department

Office of the National Security Council
7 Ingorokva Str., 0105, Tbilisi, Georgia

5.3.3 PL counterpart:

Mr. Sergo Turmanidze
Head of Internal and External Security Affairs Department
Office of the National Security Council
7 Ingorokva Str., 0105, Tbilisi, Georgia

5.3.4 **Contact persons from MIA**:

Ms. Natia Japaridze
Head of Project Management Division, International Relations Department
The Ministry of Internal Affairs of Georgia
10, G. Gulua str, 0114, Tbilisi, Georgia

Mr. Akaki Kuprashvili
Chief Specialist, International Relations Department
The Ministry of Internal Affairs of Georgia
10, G. Gulua str, 0114, Tbilisi, Georgia

5.3.5 **Contact persons from SSSG:**

Ms Gulnara Topchishvili
Head of International Relations Unit, International Relations Division, Administration
State Security Service of Georgia
72, Vazha-Pshavela Avenue, 0186, Tbilisi, Georgia

Mr Omar Mtivlishvili
Chief Specialist at International Legal Unit, International Relations Division, Administration
State Security Service of Georgia
72, Vazha-Pshavela Avenue, 0186, Tbilisi, Georgia

6. Duration of the project

Duration of the execution period: 27 months. The execution period will end 3 months after the implementation period of the Action, which will take 24 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

The Project Steering Committee (PSC) will be created at the beginning of the project, comprising of the representatives of the NSC Office, MIA, SSSG, Member State partner institutions, the EU Delegation to Georgia and Programme Administration Office (PAO) of the Ministry of Foreign Affairs of Georgia, as well as the representatives of the relevant sectoral agencies.

The PSC shall oversee the implementation of the project. 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 discussion of the updated work plan. The PSC meetings could be attended by the representatives of current ongoing related projects or representatives of the relevant institutions, with respect to the project aims and objectives. Those stakeholders can be involved in the PSC with the observer status.

The Steering Committee will meet at regular quarterly intervals. It will be co-chaired by the Project Leaders (EU Member State and Beneficiary Country). Discussions and important decisions, taken during the meetings will be kept in the official minutes in English with the possibility to disseminate among the committee members afterwards. Other details concerning the establishment and functioning of the PSC are described in the TWINNING Manual.

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.

Monitoring and Evaluation of the project will be conducted, using the project-specific logical framework, to be encoded in the EU projects monitoring system OPSYS. The contractor should report on the results at impact, outcome and output levels, linked to sources of verification presented in the logical framework. Reporting will be carried out through Progress, Interim and Final Reports as laid down in the terms of reference / project description and general conditions. For the better quality of the log frames and indicators, the contractors are encouraged to get familiar with DG NEAR guidelines on Indicators - P. 45 and the EU Results Framework. Wherever an indicator set out in the project log frame is also reflected in the EU Results Framework, project reporting will also cover it.

8. Sustainability

Sustainability of the project results in regard to CI will be ensured by NSC in terms of enacting the list of critical infrastructure subjects, as an outcome of the project, which will be approved by the Government of Georgia. This goal will be attained on the basis of elaboration of sectoral and national criteria for the identification of critical infrastructure subjects. The development of security standards, will be ensured on the basis of relevant legal acts / policy papers elaborating on general security standards. At the same time, the respective matters will be included in the Action Plans, maintained by the respective operators of critical infrastructure subjects and referring to the individual abovementioned subjects.

The mandatory results related to the Cybercrime are fully in line with the national strategic priorities and documents in the field of cybercrime, as well as, the the Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention. The Ministry of Internal Affairs of Georgia will take responsibility for maintenance of the achievements and results of the Twinning project. The existing interagency working group for fighting cybercrime will ensure sustainability of initiated activities and reforms.

Under Component on cyberterrorism, the mandatory results and outcomes of the project are in full compliance with the national strategic policy and priorities as enshrined in the National Counter-Terrorism Strategy of Georgia. Sustainability will be ensured by enhancing personnel and material-technical capacity of SSSG in line with best practices and international standards in the field of cyberterrorism. This will positively influence EU-Georgia association process and will ensure sustainable long-term cooperation between beneficiary administration and respective twinning partners and their agencies.

The outputs produced by this project (in areas such as legal and regulatory, documents, standards, training materials, etc.) will be distributed among the relevant stakeholders.

Beneficiary administrations will ensure institutionalization of working groups with dedicated staff members from respective sectors / agencies. Human resources development, in the field of CIP, cybercrime and cyberterrorism will be the key policy and strategic component for the institutions involved. Sustainability will also be ensured in terms of maintaining the employees involved in the implementation of the project.

Last but not least, the institutional sustainability of the project achievements will be embedded in the routine functions and working directions of the respective agencies.

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

The results achieved within the project has its direct and profound impact on day-to-day activities and functioning of modern societies. This impact is registered in different domains. For example, in terms of elaboration of secure functioning standards of critical infrastructure subjects, prevention of cybercrime and cyberterrorism cases, which eventually leads to a better environment. Hence, the present project is of relevance for the variety of domains.

The principles of the equal opportunity will be applied to all involved parties throughout the project implementation process.

10. Conditionality and sequencing

The present TWINNING Project Fiche has been drafted with direct participation and high involvement of the National Security Council NSC, Ministry of Internal Affairs MIA and State Security Service of Georgia.
The signature of the contract is subject to the adoption of relevant legislative framework for establishing and functioning of the democratic supervision and effective oversight system in the Cyber security domain (notably the Information Security Law but also the Law on Personal Data Protection, and possibly other pieces of legislation that could also be relevant, depending on the system model developed) by the end of the 2022 spring session of the Parliament, as well as other relevant developments on security sector reform in line with commitments made within the framework of the Association Agenda.

The beneficiary institutions will ensure the provision of an input to all project activities provided for in the Fiche, as well as coordinate activities with interlinked state and private stakeholders, in order to achieve all mandatory results of the project. Namely:

- Provide strong commitment and support for the management of the project implementation;
- Assign relevant skilled staff, at all levels, as component leaders and experts;

- Ensure participation of the relevant staff members, as well as other stakeholders, in project events;
- Ensure coordination between relevant sectoral agencies and other stakeholders of the project;
- Ensure access to important information, regulations, legislation, all supporting documentation relevant to the project;
- Implement other activities relevant for the appropriate project implementation.

Beneficiary acknowledges that the success of the project greatly depends on the readiness of the respective stakeholders / staff members to cope with the intensive workload in the complex fields.

The concrete sequencing of project components will be discussed and agreed with the selected EU MS partner(s) before the start of the project implementation and during the elaboration of the Initial as well as Rolling work plans.

11. Indicators for performance measurement

Mandatory Result 1/Component 1 – Sectoral and national level CI subjects identified and Safe and secure functioning ensured

Indicator(s) of performance:

- Number of sectors in which sectoral and national level CI subjects are identified
- Availability of general and / or sector-specific standards for the protection of critical infrastructure subjects

Sub-result 1.1 - Threat, impact and risk assessment methodologies including sectoral Standard Operating Procedures elaborated and implemented

Indicator(s) of performance:

- Status of methodology documents on threat, impact and risk assessment
- Number of sectors in which threat, impact and risk assessment implemented

Sub-result 1.2 Critical infrastructure identification criteria delivered

Indicator(s) of performance:

- Availability of sectoral and national criteria, for the identification of critical infrastructure subjects

Sub-result 1.3 Protection standards for CI subjects delivered

Indicator(s) of performance:

- Status of protection standards for critical infrastructure subjects
- Number of sectors in which safe and secure functioning of CI subjects is implemented

Mandatory Result 2 / Component 2: Capacities of the MIA to prevent and combat Cybercrime and other cyber-enabled offenses Strengthened

Indicator(s) of performance:

- Number of joint investigative operations
- The number of trained/retrained personnel working on fight against cybercrime
- Level of awareness of the population in regard to the cybercrime

Sub-results 2.1: International Cooperation of MIA in the Field of Cybercrime Enhanced

Indicator(s) of performance:

- Avalability of Joint Investigation Teaming Framework
- Number of shared intelligence (requests)
- Availability of recommendations for fight against cybercrime

Sub-Result 2.2: **Awareness on cybercrime threats raised**

Indicator(s) of performance:

- Availability of survey results (small scale) measuring perception on cybercrime in the society
- Availability of awareness raising campaigns and information materials

Sub-Result 2.3: **Qualification of personnel working on interdiction and prevention of cybercrime increased.**

Indicator(s) of performance:

- The number of trained/retrained employees via specialized trainings
- Availability of the gap analysis report
- Number of training courses developed at the MIA Academy and other Law Enforcement/Security Specialised Educational Institutions
- Availability of relevant materials and resources.

Mandatory result 3 / Component 3 – Resilience against cyberterrorism by advancing capacities for SSSG,CSB, DGA, NSC further improved

Indicator(s) of performance:

- Availability of professional capacities and technical capabilities at SSSG, CSB, DGA and NSC

Sub-result 3.1: **Capacity of SSSG and other CIP subjects' staff (and other relevant**

Sectoral Agencies) involved in combatting cyberterrorism and other APT attacks strengthened

Indicator(s) of performance:

- Availability of training modules
- Number of employees of SSSG and other Partner Agencies trained in various directions of combatting cyberterrorism (e.g. investigation, analytical, operational, IT directions) and other APT attacks
- Number of CIP subjects' staff and other sectoral Agencies trained in ToT in the field of cybercrime

Sub-result 3.2: International Cooperation of SSSG enhanced

Indicator(s) of performance:

- Availability of analysis of international regulations and EU MS legal framework including existing IT systems on combating cyberterrorism
- Number of MoUs/cooperation agreements initiated with EU MS respective institutions

12. Facilities available

The NSC Office commits itself to provide the following facilities:

- Adequately equipped office space for the RTA and the RTA assistant(s) for the entire duration of their secondment;
- Full technical supply of the office room (including access to computer, telephone, internet, printer etc.);
- Adequate conditions for the STEs to perform their work while on mission;
- Suitable venue for the meetings that will be held under the project (within the NSC Office, as well as on the basis of outsourcing activities);
- Security-related issues will be assured, according to the standards and practices applicable for all Georgian public institutions.

ANNEXES TO PROJECT FICHE

1. The Simplified Logical framework matrix
2. Organisational Charters of the NSC Office and MIA. *Note: SSSG refused to disclose their charter at this stage, since this is not a public information.*

Annex 1: Simplified Logical Framework

Project Title: Enhancing Critical Infrastructure Protection system, fight against Cybercrime and Cyberterrorism in Georgia	**Programme name and number:** “EU4 Security, Accountability and Fight against Crime in Georgia (SAFE)", ENI/2018/041-443 Direct Management.	
Beneficiary Institution: The National Security Council of Georgia (NSC) The Ministry of Internal Affairs of Georgia (MIA) The State Security Service of Georgia (SSSG)	**Total budget:** 1,300,000 EUR.	**EU ENI financing** (100 %)

	Description	**Indicators (with relevant baseline and target data)**	**Sources of verification**	**Risks**	**Assumptions (external to project)**
Overall objective	Further improve resilience of critical infrastructure against threats, among others, against cybercrime and other cyber-enabled offenses including cyberterrorism, in line with the EU’s approach, standards and policy framework.	-Interoperability of Georgian CIP system with EU relevant practice on CIP Identification and Security Regimes Baseline**:** 2021 - Critical information system subjects and relevant security standards available. No general CIP framework in place Target**:** Critical infrastructure protection system created and developed by 2024-2025	EU and other international organizations relevant reports		
	SO1: Identification and protection system of critical infrastructure subjects established	Availability of relevant laws and secondary legislation	Legislative Herald of Georgia - Matsne.gov.ge Respective legal policy	Restrictions and limitations caused by Covid-19	Stable political environment

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
Specific Objectives		Baseline: 2021 - Conceptual document available Target: The relevant laws and secondary legislation elaborated within the CIP reform implementation period	documents entailing: a) methodology for identification of sectoral and national level critical infrastructure subjects; b) general and /or sector-specific security standards, for safe and secure functioning of the critical infrastructure subjects c) Establishment of the criticality levels inside the list of Critical Infrastructure Subjects. Project reports	Lack of commitment from respective actors and/or decision makers Weak coordination between project partners Lack of absorption capacity	Strong commitment from Institutions responsible on CIP, Cybercrime and Cyberterrorism at political level ensured Timely decisions made by Government Co-operation with relevant stakeholders
	SO2: Investigation and prevention mechanisms of Cybercrime enhanced	Availability of Joint (both Interagency and Intraagency) Investigative Framework Baseline: 2021 – Joint Investigative Framework not existent Target: Joint Investigative Framework established by the end of the project Number of joint investigative operations with partner countries and internally with partner law enforcement and security agencies. Baseline: 2021 – 1 joint operation Target: At least 3 joint	Official statistics of the MIA Project reports Reports on joint operations		

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
		operations conducted till the end of the project Index of solved cases Baseline: 2021 - 19 % of the cases are solved Target: 22% of the cases are solved by the end of the project			
	SO3: Cyberterrorism and other APT threatscombating capacities improved	Level of participation of Georgia in international initiatives on combating cyberterrorism and other APT threats Baseline: 2020-2021 – participation of SSSG and NSC respective staff in 12 international events Target: Participation of SSSG respective staff and experience sharing at least in 5 international initiatives on combating cyberterrorism by the end of the project	International initiative statements, documentation, etc. SSSG official website Project reports		
Mandatory results/outputs by components	Component 1: Sectoral and national level CI subjects identified and Safe and secure functioning ensured	-Number of sectors in which sectoral and national level CI subjects identified Baseline: 2021 – Not existent	Assessment reports by relevant experts Respective policy documents entailing: a) methodology for	Delays during project implementation Lack of awareness, on the part of involved stakeholders, with regard to the CIP, Cybercrime	Strong support and commitment from twinning partner(s); Relevant staff of the beneficiary available and involved in the project;

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
		Target: By the end of the project – At least 3 sectors where sectoral and national level CI subjects identified -Availability of general and / or sector-specific standards for the protection of critical infrastructure subjects Baseline: No general and /or sector-specific security standards, for safe and secure functioning of the critical infrastructure subjects in place Target: General and / or sector-specific standards for the protection of critical infrastructure subjects elaborated and agreed by relevant parties by the end of the project	identification of sectoral and national level critical infrastructure subjects; b) general and /or sector-specific security standards, for safe and secure functioning of the critical infrastructure subjects. Reports on stakeholder consultations Project documentation: institutional analysis reports, recommendations, workshop reports, STE mission reports etc.	and Cyberterrorism as well as other APT cyber threat related matters being the subject of the present project Lack of involvement from BAs' stuff and other stakeholders Lack of proactiveness from MS representatives Lack of project specific data/documentation/information	Timely decisions made by relevant stakeholders; Co-operation with relevant stakeholders Availability of relevant information/materials/ documentation. Proactive cooperation of Twinning partner(s) ensured.
	Component 2: Capacities of the MIA to prevent and combat Cybercrime and other cyber-enabled offenses Strengthened	-Number of shared intelligence (requests) Baseline: 2021 - 64 shared intelligence requests Target: Shared intelligence requests till the end of the project increased at least	MIA internal statistical data Assessment reports and recommendations by EU institutions / relevant experts.		

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
		by 10% - Share of trained/retrained personnel working on fight against cybercrime Baseline: 2021 – 105 employees Target: retrained police officers increased at least by 15% -Level of awareness of the population in regard to the cybercrime Baseline: 2021 – Not existent Target: Small scale survey conducted at the beginning of the project; final small scale survey conducted at the end of the project.	Project reports Survey results		
	Component 3: Resilience against cyberterrorism and other APT threats by advancing capacities for SSSG, CSB, DGA, NSC further improved	Availability of professional capacities and technical capabilities at SSSG, CSB, DGA and NSC Baseline: 2021 – existing capabilities and capacities not fully responding to the rapidly evolving developments in countering cyberterrorism Target: Enhanced	SSSG, CSB, DGA and NSC Project reports Project documentation: (list of training participants. Training materials, analysis reports etc.).		

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
		capacities and capabilities of SSSG relevant staff in line with international standards and EU MS best practices by the end of the project			
Sub-results per component (optional and indicative	1.1 Threat, impact and risk assessment methodologies including sectoral Standard Operating Procedures elaborated and implemented	-Status of methodology documents on threat, impact and risk assessment <u>Baseline:</u> Not existent <u>Target:</u> Risk, threat and impact assessment methodologies, applicable to the respective sectors / agencies elaborated and agreed with respective authorities by the end of the project -Number of sectors in which threat, impact and risk assessment implemented <u>Baseline:</u> Not existent <u>Target:</u> At least 2 threat, impact and risk assessment implemented in respective sectors by the end of the project	Assessment reports by EU relevant experts. Sector specific and general policy documents Methodology documents	Delays during project implementation Delays in approval of Methodology documents Lack of coordination among involved stakeholders Lack of commitment from respective actors and/or decision makers. Delays in elaboration of sectoral and national criteria Lack of cooperation between law enforcement teams Difficulties in structuring efficient surveys' methodologies measuring perception on cybercrime in the society Limitations caused by pandemic for the implementation of specific activities (trainings, awareness	Commitment from relevant decision makers side; High involvement of the stakeholders ensured. All relevant information and documentation available.
	1.2 Critical infrastructure	-Availability of	Assessment reports by		

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
	identification criteria delivered	sectoral and national criteria, for the identification of critical infrastructure subjects Baseline: 2021- Not existent Target: Sectoral and national criteria, for the identification of critical infrastructure subjects elaborated and agreed with respective authorities by the end of the project	relevant experts Project documentation (list of workshop participants, workshop reports, materials, recommendations etc.); Report on consultation with stakeholders Sectoral and national criteria documents	raising events)	
	1.3 Protection standards for CI subjects delivered	-Status of protection standards for critical infrastructure subjects Baseline: 2021- Not existent Target: Sector-specific security standards and tailor-made levels of additional security measures for the protection of critical infrastructure subjects agreed and reflected in the respective documentsby the end of the project	Assessment reports by relevant experts Project documentation (list of workshop participants, workshop reports, materials, recommendations etc.) Report on consultation with stakeholders Sector-specific security standard documents		

	Description	**Indicators (with relevant baseline and target data)**	**Sources of verification**	**Risks**	**Assumptions (external to project)**
		-Number of sectors in which safe and secure functioning of CI subjects is implemented Baseline: 2021- Not existent Target: at least 3 sectors in which safe and secure functioning standards for of CI subjects are implemented and reflected in the respective documents by the end of the project			
	Sub-results 2.1: International Cooperation of MIA in the Field of Cybercrime Enhanced	Avalability of Joint Investigation Teaming Framework Baseline: 2021 – Joint Investigation Teaming Framework not existent Target: Joint Investigation Teaming Framework established by the end of the project - Number of joint meetings between law enforcement teams; Baseline: 1 joint meeting Target: at least 4 by the end of the project - Availability of recommendations for fight	Assessment reports by EU relevant experts Notes of the joint meetings Project documentation (list of workshop participants, workshop reports, materials, recommendations etc.)		

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
		against cybercrime Baseline: Not existent Target: relevant recommendations for fight against cybercrime elaborated by the end of the project.			
	Sub-Result 2.2: Awareness on cybercrime threats raised	-Availability of survey (small scale) results measuring perception on cybercrime in the society Baseline: Not existent Target: 2 small scale surveys conducted during the project implementation phase -Availability of awareness raising campaigns and information materials Baseline: Limited amount of awareness raising and information materials Target: Wide variety of awareness raising and information materials by the end of the project	Survey questionnaire Survey results and analysis report awareness raising and information materials		
	Sub-Result 2.3: Qualification of personnel working on interdiction and	-Number of trained/retrained employees via specialized trainings	Internal statistical data of the MIA		

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
	prevention of cybercrime increased	<u>Baseline</u>: 64 employees <u>Target</u>: Number of retrained police officers increased at least by 15% - Availability of the gap analysis report <u>Baseline</u>: 2021 - Not existent <u>Target</u>: gap analysis conducted by the mid of the project implementation - Number of training courses developed at the MIA Academy and other Law Enforcement/Security Specialised Educational Institutions <u>Baseline</u>: 2021 - 1 <u>Target</u>: at least 2 courses developed by the end of the project -Availability of relevant materials and resources <u>Baseline</u>: 2021 - limited <u>Target</u>: Various new materials and resources elaborated by the end of the project	gap analysis report Project documentation (list of training participants, training evaluations, training materials, recommendations etc.) new educational materials and resources		

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
	Sub result 3.1 Capacity of SSSG staff (and other relevant Sectoral Agencies) involved in combatting cyberterrorism and other APT attacks strengthened	-Availability of training modules Baseline: 2021 – Not existent Target: The relevant training modules elaborated by the end of the project - Number of employees of SSSG and other Partner Agencies trained in various directions of combatting cyberterrorism (e.g. investigation, analytical, operational, IT directions) and other APT attacks Baseline: 2020-2021 – 2 trainings undergone by SSSG counterterrorism center employees Target: At least 10 employees trained in various directions of combating cyberterrorism and other APT Attacks by the end of the project Number of CIP subjects' staff and other sectoral Agencies trained in ToT in the field cybercrime Baseline: 2021-0	Project documentation (list of training participants, training evaluations, training materials, recommendations etc.) Training modules SSSG official website		

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
		Target: 10 relevant employs trained in ToT in the field cybercrime by the end of he project			

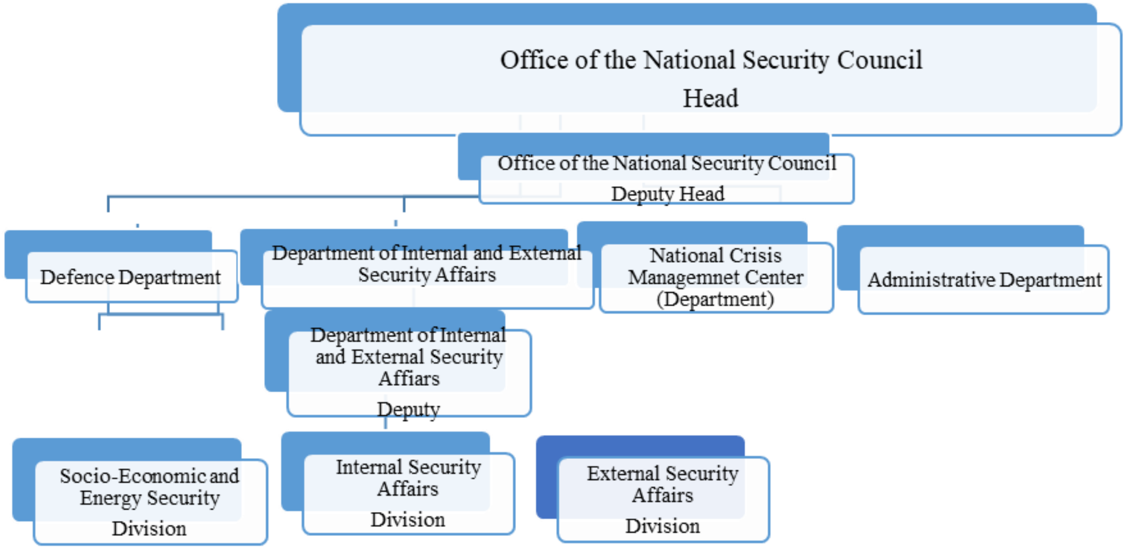
	Sub-result 3.2: International Cooperation of SSSG enhanced	-Availability of analysis of international regulations and EU MS legal framework including existing IT systems on combating cyberterrorism
		Baseline: 2021 – Not existent
		Target: Analysis of international regulations and EU MS legal framework including existing IT systems on cyberterrorism elaborated in the first half of the project implementation
		-Number of MoUs/cooperation agreements initiated with EU MS respective institutions
		Baseline: by 2021 by 2021 – 62 MoUs/cooperation agreements[17] concluded with partner countries
			MOUs/Cooperation agreements;
			documentation of internal legal procedures available at LEPL Legislative Herald of Georgia;
			SSSG official website;
			SSSG annual reports		

[17] Includes information sharing agreements, interagency cooperation agreements, inter-state/inter-governmental agreements on fight against fight.

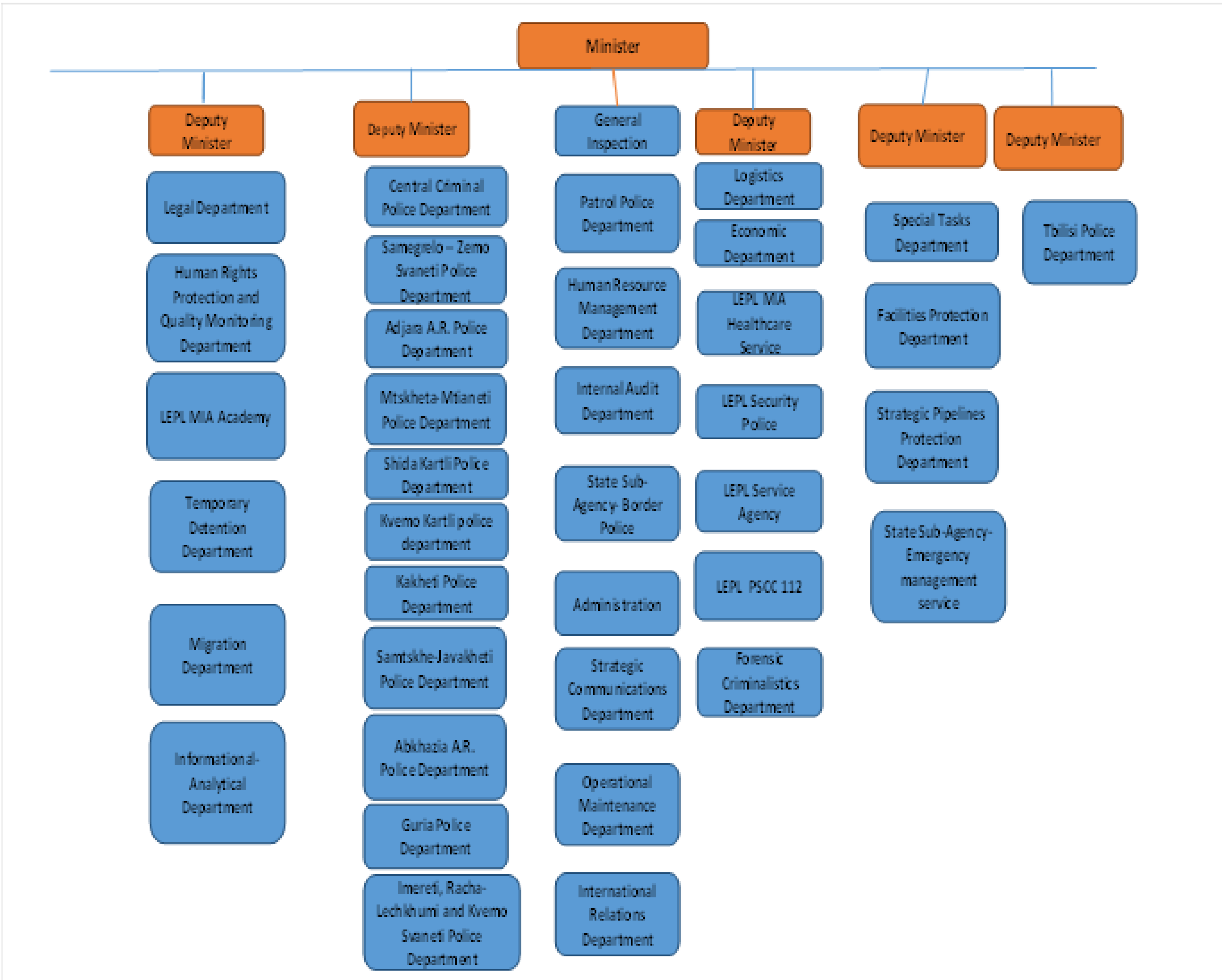
	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
		Target: At least 2 of MoUs/cooperation agreements initiated with EU MS respective institutions by the end of the project			

Annex 2:

Office of the National Security Council:


Office of the National Security Council
Head
Office of the National Security Council
Deputy Head
Defence Department
Department of Internal and External Security Affairs
National Crisis Managemnet Center (Department)
Administrative Department
Department of Internal and External Security Affairs
Deputy
Socio-Economic and Energy Security
Division
Internal Security Affairs
Division
External Security Affairs
Division

MIA organizational chart:


Minister
Deputy Minister
Legal Department
Human Rights Protection and Quality Monitoring Department
LEPL MIA Academy
Temporary Detention Department
Migration Department
Informational-Analytical Department
Deputy Minister
Central Criminal Police Department
Samegrelo – Zemo Svaneti Police Department
Adjara A.R. Police Department
Mtskheta-Mtianeti Police Department
Shida Kartli Police Department
Kvemo Kartli police department
Kakheti Police Department
Samtskhe-Javakheti Police Department
Abkhazia A.R. Police Department
Guria Police Department
Imereti, Racha-Lechkhumi and Kvemo Svaneti Police Department
General Inspection
Patrol Police Department
Human Resource Management Department
Internal Audit Department
State Sub-Agency- Border Police
Administration
Strategic Communications Department
Operational Maintenance Department
International Relations Department
Deputy Minister
Logistics Department
Economic Department
LEPL MIA Healthcare Service
LEPL Security Police
LEPL Service Agency
LEPL PSCC 112
Forensic Criminalistics Department
Deputy Minister
Special Tasks Department
Facilities Protection Department
Strategic Pipelines Protection Department
State Sub-Agency- Emergency management service
Deputy Minister
Tbilisi Police Department