ANNEX C1: Twinning Fiche

Project title: Strengthening Cybersecurity Capacities in Georgia

Beneficiary administration: LEPL Data Exchange Agency, Ministry of Justice of Georgia

Twinning Reference: GE 18 ENI JH 01 20

Publication notice reference: EuropeAid/168-164/ACT/GE

EU funded project
TWINNING TOOL

List of Abbreviations

AA	Association Agreement
BA	Beneficiary Administration
BC	Beneficiary Country
BI	Beneficiary Institution
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure (includes Operators of Essential Services and Digital Service Providers)
CSB	Cyber Security Bureau
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
DCFTA	Deep and Comprehensive Free Trade Area
DEA	Data Exchange Agency
ENI	European Neighbourhood Instrument
EQA	External Quality Assessment
EQC	External Quality Control
EQM	External Quality Management
EU	European Union
EUD	EU Delegation to Georgia
FIRST	Forum of Incident Response and Security Teams
GCSCC	Global Cyber Security Capacity Centre
GoG	Government of Georgia
GUAM	Organisation for Democracy and Economic Development with four member-states: Georgia, Ukraine, Azerbaijan, and Moldova.
JAS	Jobs Action Sheet
LA	Legal Approximation
LEPL	Legal Entity of Public Law
MIA	Ministry of Internal Affairs
MoD	Ministry of Defence
MoJ	Ministry of Justice
MoU	Memorandum of Understanding
MS	Member State
NCA	National Competent Authority
NCSS	National Cyber Security Strategy
NSC	National Security Council
NGO	Non-governmental organisation

NIS	Directive (EU) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)
OTA	Operational Technical Agency
PAO	Programme Administration Office
PL	Project Leader
PSC	Project Steering Committee
PT	Professional Testing
RAMA	State Regulation Agency for Medical Activities
RTA	Resident Twinning Advisor
SAFE	EU4 Security, Accountability and Fight against Crime in Georgia
SOP	Standard Operating Procedure
SPOC	Single Point of Contact
SSSG	State Security Service of Georgia
STE	Short Term Expert
TA	Technical Assistance
TAG	Technical Advisory Group
TAIEX	Technical Assistance and Information Exchange Instrument
TI	Trusted Introducer
ToR	Terms of Reference
TTI	Transfusion Transmissible Infection
UNDP	United Nations Development Programme

1. Basic Information

1.1 Programme:

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

1.2 Twinning Sector: Justice and Home Affairs

1.3 EU funded budget: EUR 1 300 000

2. Objectives

2.1 Overall Objective

The overall objective of the project is to strengthen Georgia’s preparedness and resilience towards cyber threats and attacks, by capacity building of Georgian stakeholders and creating enabling cybersecurity frameworks, in line with the EU’s approach, standards, and relevant legal and policy framework, notably but not limited to the NIS Directive.

2.2 Specific objective:

The specific objective of the project is to strengthen Georgia’s cybersecurity legal and institutional framework to increase its security level of networks and information systems, as well as its level of prevention, preparedness, reaction and resilience to cyber incidents and threats. The benchmark for this will be the EU’s relevant policy and legal framework, namely the NIS Directive and the EU’s external cyber capacity building guidelines. The project will carefully follow the EU’s approach to promoting a rules-based cybersecurity governance in full respect of Human Rights and Fundamental Freedoms. It will take into consideration a whole-of-government and whole-of-society approach for an inclusive and accountable policy and decision-making process, involving CSOs, civic actors and the private sector. All this will benefit the citizens, the whole information society and digital economy of Georgia.

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 implementation and fulfilment of the objectives set out in the AA. Furthermore, cybersecurity features as one key element of Deliverable 12 on security of the **’20 Deliverables for 2020’** framing the EU-EaP regional policy dialogue.

Enhancement of cybersecurity ecosystem in Georgia will directly contribute to the development of information society and digital economy, provision of safe and reliable electronic public services will result in increased trustworthiness of electronic government. Cooperation in the field of information society is one of the important fields of EU-Georgia relationship as reflected in Chapter 8. Article 324 of the **EU-Georgia Association Agreement**. The action is also fully in line with the provisions of the EU-Georgia Association Agreement, of which Chapter 8 specifically addresses “Cooperation in the field of information society”. Under this chapter, Article 325 (a) stipulates that cooperation will cover: “exchange of information and best practice on the implementation of national information society initiatives including inter alia those aiming at promoting broadband access, improving network security and developing public online services.”

The **EU – Georgia Association Agenda** implies enhanced cooperation in defence policy and security field, strengthening the bilateral dialogue on the related matters, addressing the common concern themes, widening collaboration to facilitate Georgia’s participation in the EU crisis management operations as well as in Common Security and Defence Policy (CSDP) related capacity building and consultation activities; activation of various EU support tools and programmes for assisting the resilience and Georgia's capacity enhancement to stand against the 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 the Field of Digital Economy and Society, mid-term priorities).

In accordance with the draft document "**2019-2021 National Action Plan for Georgia's Integration in EU"**, Georgia is committed to approximate Information Security law with EU NIS Directive (Directive (EU) 2016/1148).

General needs and targets for improvement of cybersecurity frameworks in Georgia are reflected in the strategic documents of the country and international agreements as follows:

Georgia, as well as other EaP countries, under the umbrella of Declaration of the Second EaP Ministerial Meeting on the Digital Economy agreed to improve resilience of the critical information infrastructure in different key sectors of the economy for the benefit of citizens, businesses and public administrations, as well as development of national cybersecurity strategies and operational national CERTs in line with the EU best practices. Within EU-EaP cooperation format, namely within **"Eastern Partnership - 20 Deliverables for 2020 Focusing on key priorities and tangible results"** Georgia is committed to (a) reinforcing protection of critical infrastructure; (b) enhancing public/private and international cooperation on cybersecurity; (c) developing the capacity to respond to cybersecurity incidents.

Alignment of Georgian cybersecurity systems with European models and for that purpose the use of the NIS Directive as a toolkit was reflected in "**Georgian Cyber Security Strategy and Action Plan 2017-2018**" adopted by Prime Minister of Georgia. Strategy highlighted Georgia's interest in using the NIS Directive and EU Cyber Strategic framework as key directions for considerations. All relevant stakeholders in the field of cybersecurity have been working on the draft national strategy: **"Georgian National Cybersecurity Strategy and Action Plan 2020-2022",** which is expected to be adopted in early 2020 (please see Section 3.2 of this document for the detailed information).

3. Description

3.1 Background and justification

3.1.1 Background

Like many other countries worldwide, over the last decade Georgia has experienced a significant boost in digital economy and e-government development, increase of information society services and connectivity dependency. According to the International Telecommunications Union (ITU), in 2017 60.49% of the population in Georgia had access to the Internet that needs a safe environment for operation.

The increased numbers of cyber-attacks and cyber threats, as well as cyber espionage cases and cyber war of 2008[1], clearly showed to Georgia that the protection of cyberspace is as important for national security as land, maritime, and air defence. A "massive" cyber-attack against multiple targets in Georgia has taken place on 28 October 2019[2]. Not only has this seen thousands of websites impacted

[1] Shadow server report on 2008 war: https://wiki.shadowserver.org/wiki/pmwiki.php/Calendar/20080811?logdate=201005

[2] See details on BBC.com: https://www.bbc.com/news/technology-50207192; See details on france24.com: https://www.france24.com/en/20191028-2-000-georgia-websites-hacked-in-cyber-attacks

but two Georgian TV broadcasters were temporarily taken offline as well. Critical national infrastructure, however, would appear not to have been affected.[3] The case is still under investigation.

As information technologies rapidly evolve, critical information infrastructure is becoming more dependent on them. The Government of Georgia (GoG) dedicated all its organisational and institutional capacities for making the Georgian cyberspace safe and secure place for information society services and for developing a system of information security that is able to minimise harmful effects of any cyber-attack and allow rapid recovery of information infrastructure to full operation in the aftermath of such attacks. Resilience of the cyber domain remains the key priority for the GoG and it strives to direct its nation-wide efforts in building up comprehensive frameworks enabling safe and reliable, trusted digital environment for the benefit of the information society, public and private sectors at large.

Georgia considerably foreruns all Eastern Partnership Countries and even some of Eastern European EU Member States in the field of Trust and Security of Cyberspace, ensuring ICT security and data protection and provision of electronic trust services. Georgia is one of the few countries where cybersecurity development is ahead of ICT development, according to international rankings and indicators that assess states worldwide based on internationally agreed methodology and standards[4]. Thus, the Global Cybersecurity Index (2017) shows that Georgia has fulfilled 82% of its criteria for the development of its cyber capabilities. In 2017, the International Telecommunication Union also ranked Georgia 8th of 165 countries globally for its cyber-security preparedness (up from 16th position in 2014), and 3rd of 41 countries assessed by the National Cyber Security Index. The assessment of 2018 ranks Georgia on the 9th position in the region and on the 18th worldwide.

The 2018 edition of the National Exposure Index, which seeks to approximate the potential openness of countries to cyberattacks through port scanning, ranks Georgia 87th, out of the 187 countries reviewed.[5] In the more comprehensive assessment of the uptake and contributions of information and communication technology to national welfare conducted through the ITU ICT Development Index and the World Economic Forum's Network Readiness Index (NRI) Georgia ranks 74th and 58th, respectively.

Over the last decade the cyber-ecosystem in Georgia has begun to evolve across government, the private sector, and society in general. The GoG has utilised comprehensive approach and whole-of-government spirit to all major building blocks of cybersecurity which can be grouped in following priority areas: Strategic development, enforcement of legal framework, increase of cyber competences and e-skills of information society, establish a trust based public-private partnership, development of international partnerships.

Georgia began formal implementation of its first national cybersecurity strategy in 2013. Georgia's first cybersecurity strategy was based on Georgia's Threat Assessment Document 2010-2013 and the National Security Concept of Georgia[6]. The strategy called for the creation of major principles of such a cybersecurity system, which not only facilitated the protection of the information infrastructure against cyber threats but also helped the socio-economic development of the country. The second Georgian National Cybersecurity Strategy and its Action Plan for 2017-2018 was adopted by Prime-Minister's Decree in 2017 and sets all critical policy priorities and strategical concept for the development of the Georgian cybersecurity domain. The strategies enlisted the following seven principles that are necessary to achieve a better protected cyberspace: uniform government approach; government and private sector cooperation; research and analysis; new legislative and regulatory framework; institutional coordination for ensuring cybersecurity; public awareness, education and training; international cooperation.

[3] https://www.forbes.com/sites/daveywinder/2019/10/29/georgia-ill-be-back-cyber-attack-terminates-tv-takes-down-15000-websites/

[4] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

[5] The National Exposure Index ranks countries according to exposure, with a higher rank in the index implying a greater level of exposure. Rapid 7 Labs (2018). *National Exposure Index 2018*, p.51. Available at: https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf

[6] https://mod.gov.ge/uploads/2018/pdf/TAD-ENG.pdf

Despite of the fact that the following key governmental authorities are assigned with cybersecurity roles and responsibilities, Georgia still needs to strengthen the governance model and ensure a "whole-of-society"[7] approach, which means that cybersecurity cannot be delegated to any single independent agency.

A number of factors have affected the implementation of the previous strategies that should be considered. Most notably, no specific budget has been put into place to support national level cybersecurity activities. Funding allocated to the **Data Exchange Agency (DEA)** – the agency responsible for implementing information security policy – is mostly dedicated to operational, day-to-day cybersecurity activities and limits the DEA's financial capacity to perform strategic initiatives and its ability to be involved in other long-term programs. In the past, implementation of strategies in particular had to contend with the repeated dissolution of coordinating bodies due to larger structural reforms, which have included the redistribution of authorities previously concentrated under the presidency. Yet, not all relevant stakeholders have hitherto been equally involved in efforts to improve the country's cybersecurity posture. This applies particularly to private sector and civil society representatives. While the national cybersecurity strategies recognised the education sector as one of its pillars, resource constraints limit progress in translating this strategic priority into practice.

Georgian cybersecurity stakeholders and government authorities are in the process of drafting the third National Cybersecurity Strategy 2020-2022[8]. Georgia expects to have strategy ready for adoption by the Government in December 2019. As Georgia strives to make its national frameworks compatible with Euro-Atlantic systems, strategic development process is heavily consulted by the EU experts and like-minded country consultants. The EU and CoE guidance are also reflected in this process.

Organisations throughout Georgia have achieved considerable advances in operational capacity, with technical coordination on cybersecurity matters surpassing cooperation on many other security issues, largely thanks to strong informal and personal networks.

The principal government organisation responsible for public and private sector (non-military) cybersecurity in Georgia is the Data Exchange Agency (DEA) - Legal Entity of Public Law, subordinated to the Ministry of Justice. It began operations in January 2010. The Agency's core functions are the development of e-Government, the creation and development of data exchange infrastructure, security of the information and cyber space, increase awareness, setting ICT standards for the public sector and elaborating information security policies, working on strategy, legal and regulatory frameworks for ICT. An important part of the Agency's mandate is information security for the public sector and private critical information infrastructures. DEA conducts awareness raising activities and training courses; supports government agencies in adopting and implementing information security policies; and also develops state-wide standards and procedures for information security through legislation and by-laws. Under DEA, **Georgia's national and governmental Computer Emergency Response Team (CERT)** has become operational. The main function of CERT.GOV.GE is to offer consultancy regarding cyber incidents, monitor the cyber environment in public and private sectors, register and analyse existing and potential cyber threats, and provide recommendations on how to eliminate and avoid them. CERT.GOV.GE is an active member of all major international organisations (accredited member of Trusted Introducer (TI) and full member of FIRST, exchanging information on incidents with EU CERT on a daily basis) and is a distinguished member of all international and the EU cyber fora (OSCE CBM national PoC, International Conference on Theory and Practice of Electronic Governance (ICEGOV), European Dialogue on Internet Governance (EuroDIG)).

The Cyber Security Bureau (CSB) is a Legal Entity of Public Law (LEPL) under the Ministry of Defence (MoD) created in 2014 as a result of the strong governmental commitment to strengthening

[7] One of the approaches of Security Sector Reform, Council of the European Union conclusions on EU-wide strategic framework to support Security Sector Reform (SSR), 14 November, 2016 https://www.consilium.europa.eu/en/press/press-releases/2016/11/14/conclusions-security-sector-reform/

[8] Please see the final draft of the strategy at: https://dea.gov.ge/uploads/National_Cybersecurity_StrategyofGeorgia_final%20draft.pdf

the cybersecurity dimension within the defence sphere. The mission of the Bureau is to establish and develop a robust and reliable information security system, which will minimise harmful consequences of any cyber-attack or/and computer security incident and will allow rapid ICT restoration. Fundamental principle and mandate of the organisation encompass security of the CISS (Critical Information System Subject) of the defence domain plus initiation of the different ICT standards. At the initial stage of the development, in conjunction with the NATO allies and partners CSB elaborated its first Cyber Security Policy that clearly indicated the core functions and targeted areas. Due to the complexity of the issue, CSB continues the process of sophistication by strengthening areas, ranging from strategy development, legal and human capacity to technological advancement. As for some technicality, in order to detect and prevent cybersecurity incidents, the Computer Security Incident Response Team (CSIRT) of the CSB conducts proactive and reactive services on a daily basis, as well as digital forensics, malware analyses, IT audits, live response and threat hunting.

The Ministry of Internal Affairs (MIA) of Georgia is responsible for cybercrime law enforcement. This activity is carried out by Cyber Crime Division (CCD) under the Central Criminal Police Department (CCPD) since December 2012. The MIA has also established the Special Sub-unit for Computer-Digital Forensics within the Forensics-Criminalistics Main Division. This sub-unit is the first handler of digital forensic evidence. Georgia is part of the Budapest Convention and carries out cybercrime law enforcement functions in accordance with EU and CoE standards.

The National Security Council of Georgia (NSC) is an eight-member advisory body responsible for national security policy planning and coordination. The Office of the NSC is responsible for cybersecurity inter-agency coordination and cooperation, as well as supervision over policy and strategy development process.

After the structural reforms in 2015, **Security Service of Georgia (SSSG)** was established as independent entity and is vested with the power to acquire, process and collect information regarding threats to national security. The activities of the SSSG are focused on identification, prevention and deterrence of potential threats, as well as within its competence to carry out relevant measures in order to fully protect the State’s national interests as well as the safety of each citizen. **LEPL Operative-Technical Agency (OTA)** is under the supervision of the SSSG, also accountable to the PM and guarantees conducting covert investigative activities and electronic surveillance measures when addressed by the relevant investigative, intelligence and counterintelligence agencies equipped with the appeal in line with respective legislative procedures and norms.

Georgian achievements are not limited to technical, but also include organisational and legal capacities. Georgia enacted an e-friendly and cybersecurity and data protection enabling legal eco-system. Georgia is the first EaP country who is in most instances compliant with Union *acquis* in eGOV and ICT. In 2017 Georgia fully integrated the eIDAS Regulation in its new law on Electronic Document and Electronic Trust Services, thus establishing rules and conditions for using qualified electronic signature, secure digital authentication and other qualified trust services similar to the EU requirements. The aforementioned makes a good opportunity for Georgia no initiate acknowledgement of Georgian trust services by the EU Member States and thus to start process of Georgia’s integration into the EU Digital Single market.

Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been implemented and legislation protecting the rights of individuals and organisations in the digital environment has been adopted in Georgia. Laws address the protection of critical information infrastructure (CII), liability of ISPs, incident reporting obligations and the security of e-transaction. The key law that sets the ground for information and cybersecurity frameworks is the Information Security Act of Georgia. The law is supplemented by a number of so-called sub-normative acts that define and further develop the legal provisions for practical implementation.

Despite an existing legal framework, the cybersecurity legislation has a few gaps that require relevant consideration from the respective authorities. Namely, there is an urgent need to develop an inclusive framework for the classification of critical information infrastructure assets that include private sector. The methodology and principles for identifying those critical information infrastructures should be conducted in conformity with the NIS Directive and available EU best practice. There is an immense requirement for developing strong enforcement mechanisms to ensure Critical Information System Subjects' (CISS) compliance with new legal regime of cybersecurity; nowadays lack of cyber security safeguards for CISS is a challenge in terms of availability, integrity and confidentiality of critical information systems and services. In addition to the aforementioned, the existing legal framework does not provide for incident reporting and vulnerability disclosure rules and procedures. Incident taxonomy rules and response schemes are also missing; there is no central registry of national-level cybersecurity incidents.

Difficulties remain in replicating existing cybersecurity endeavours at scale due to a lack of affordable training programmes and educational opportunities. Despite developments, lack of trained personnel is a common problem. The need to train professionals in cybersecurity has been recognised by the Government and has been documented in the cybersecurity strategy of Georgia. Within public institutions, training in cybersecurity, both for IT and general staff, is very limited and very low numbers of public servants have undergone it. Cybersecurity awareness and cyber-consciousness are also often absent in the mind-set of employees in the government sector. Private sector offerings for cybersecurity training are limited to non-existent. A high demand for cybersecurity certification[9] is almost exclusively serviced through the invitation of instructors from abroad or through online programmes.

Georgia's cybersecurity strategy for 2017–2018 improved public awareness and established an education base as key directions for cybersecurity in Georgia and outlined concrete actions to achieve these objectives. A national programme for cybersecurity awareness raising is yet to be established, as currently cybersecurity awareness raising efforts are sporadic and not supported by dedicated budgetary allocations. The DEA serves as the lead public organisation in organising cybersecurity awareness-raising events for public, private and civil society while CSB is implementing the same within the defence sector[10].

The GoG efficiently increases the cyber professionalism of its cybersecurity teams. In 2017, DEA's staff went through the certification process of internationally acknowledged certification institutions like SANS/GLEG and ISO 9001:2015 Lead Auditor and successfully passed the respective exams. Moreover, the CERT.GOV.GE participation in the international cybersecurity competition "CyberEx2017" resulted in the 8th place among all participants globally.

The GoG successfully uses the public-private multi-stakeholder platform as a tool for creating trust among all stakeholders and sharing information and knowledge, getting new initiatives, as well as enabling private sector engagement in policy and strategy development process. Georgian Cybersecurity Forum is an important platform for exchange of initiatives and proposals for the improvement of resilience and security of Georgian cyberspace. The Forum has been meeting twice a year for past five years. The DEA is leading the public-private cooperation process, has conducted numerous workshops and meetings in the course of 2019 with the financial, energy and telecommunication sectors in order to enrol preparatory consultations for critical information infrastructure identification process.

Strengthening bilateral, regional and international cooperation with like-minded states and international institutions in the field of cybersecurity has been high on the political agenda for the GoG. Key multilateral cooperation partners for Georgia in this field are: the UN, the EU, the CoE, NATO and the OSCE. From a regional perspective, the GoG would like to strengthen partnership and cooperation initiatives under the umbrella of the Organisation for Democracy and Economic Development (GUAM) and within the EaP cooperation model. On a bilateral basis, Georgian CERT.GOV.GE established partnership and cooperation agreements with the following countries: Romania, Bulgaria, Estonia, Latvia, Lithuania, Armenia, Azerbaijan, Moldova, Ukraine, Italy, Austria, Turkey, Poland, Belarus and Hungary.

[9] E.g. Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Certified Information Security Manager (CISM)

[10] E.g. (a) Awareness program for ordinary employees and managers of the Ministry of Defence; (b) face to face intensive and comprehensive lectures and utilizing E-Learning platform; (c) integrating of Cyber elements in MoD educational programs.

3.1.2 Justification

The GoG assumes its responsibility for security and trust in cyberspace. In addition, as Georgia aspires to closer integration with the EU, it aims to conduct and develop the cybersecurity framework in accordance with the EU standards. The NIS Directive is well suited as a tool to establish cybersecurity in a targeted and innovative way in Georgia. Moreover, Georgia is a strong and reliable aspirant state, moving toward the European and Euro-Atlantic integration. The Georgian state shares the fundamental principles of Western society.

Significant as these achievements are, Georgia still faces substantial challenges in its cybersecurity development process. The GoG fully acknowledges that it needs to take more comprehensive steps and holistic approach towards cybersecurity. The above reasons and the increased number and sophistication of attacks targeting key societal systems and critical services are motivating the Georgian cyber stakeholders to invest in national cybersecurity development and cooperate with EU Member States.

The Twinning project will be an instrumental tool for the revision and update of Georgian national Cyber Security Strategy and substantial legal framework in line with the NIS Directive; institutional framework on strategic, operational and tactical levels will be operationalised; interagency coordination and cooperation schemes will be further elaborated. Since skilled cyber resources are scarce in Georgia a key enabling factor for the NIS implementation and the successful raising of cyber posture will be increasing qualifications of key members of the Georgian authorities.

3.2 Ongoing reforms:

The Georgian National Cybersecurity Strategy and Action Plan 2020-2022 is expected to be adopted in early 2020[11]. Key components of the strategy are interrelated with the Twinning project as regards public-private cooperation in the field of critical information infrastructure protection, awareness raising and capacity building of key stakeholders and affected industry representatives, building of a sustainable and well-functioning institutional-organisational framework for better cybersecurity in the country. The main part of the draft document focuses on goals, objectives and activities: (1) Bolster the development of cyber-culture among information society and organisations, to support resilience to threats and incidents in cyberspace; (2) Sustainability of cybersecurity governance system and enhancement of the public-private cooperation; (3) Strengthening cyber capabilities and development of strong cyber workforce; (4) Strengthen Georgia’s position as a net contributor to international cyber security at an international scale.

Relevant Georgian government authorities (MoJ, MIA, MoD and SSSG) are in the process of developing methodology and a questionnaire for the identification of critical information infrastructures. Currently information and cybersecurity legal requirements are mandatory only for 40 public critical institutions. While vital systems/services definitely exist in the private economy, including the financial sector, communication, energy and transportation companies, no private sector organisations are currently designated as critical information infrastructure. Incorporating the private sector into the official framework for critical information infrastructure protection is a crucial reform for the GoG. Beside the methodology, Georgia aims to develop the new incident classification taxonomies in order to classify attacks into specific categories and improve consistency around the incident response.

General Policy and Legislative Process

The National Policy Planning System Reform Strategy, adopted by the Government of Georgia in August 2015 recognises 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 current (policy-making) and legislative

[11] Please see the final draft of the strategy at:
https://dea.gov.ge/uploads/National_Cybersecurity_StrategyofGeorgia_final%20draft.pdf

process. The assessment will also feed into the new action plan for the implementation of the Public Administration Reform (PAR) roadmap. 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: "This situation inevitably places enormous pressure on the combined law-making resources of the Government and the Parliament and leaves little time for essential elements of a well-ordered law-making process, such as regulatory impact assessments or proper consultation with civil society." 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.)

To sustain the legal approximation process the Ministry of Justice (MoJ) with the EU assistance (through “Facility for the Implementation of the Association Agreement in Georgia” and “Legislative Impact Assessment, Drafting and Representation” projects) elaborated Legal Approximation Guidelines and Manual. These documents provide key principles and techniques of approximation that will guide and orient legal drafters throughout the approximation process.

The documents are under finalisation and after official adoption by the Government should be used consistently, not only 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.

Along the legislative process the Government is proceeding with the rational organisation of state administration and clear accountability lines between institutions, including supervision and reporting between line ministries and agencies. The Civil Service Bureau is tasked with the development of uniform civil service state policy. Functional reviews of the line Ministries have been already done and currently the Civil Service Bureau is performing an analysis of state agencies with the intention of identifying and putting forward reforms to improve the organisation of PA, to streamline their mandates, enforcement mechanism as well as policy making process.

In this regard the project will ensure consistency between the review of the organisational set-up of the beneficiary institution with the national legislation regulating the organisation of the state administrations and above-mentioned analysis of the state agencies.

3.3 Linked activities:

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

A Memorandum of Understanding (MoU) on Cybersecurity Cooperation between the Government of Georgia and the Government of the United Kingdom was signed in 2019 and aims to further develop the long-term and large-scale cooperation in the field of cybersecurity. Under the umbrella of this MoU Cybersecurity Capacity Review was conducted by the Global Cyber Security Capacity Centre (GCSCC)[12], the third National Cybersecurity Strategy Development process has started and discussions among stakeholders on identification of critical information infrastructures have commenced. Recommendations from the review were thoroughly reflected in the National Cyber Security Strategy development process.

[12] Capacity Review document is unavailable right now, but will be available to the selected EU MS during the project work plan preparation process. See detailed information about the review: https://www.oxfordmartin.ox.ac.uk/cyber-security/

UNDP, USAID, NATO (HQ and Liaison Office), GIZ and other international donors and local partners are helping DEA and other cyber authorities to perform systematic and ongoing awareness raising and training activities during the last five years for building up cyber professionalism and proficiency directed to different target groups[13]. CSB is participating in different NATO initiatives[14] in order to enhance cyber defence capacities and capabilities.

The five-year "SAFE: EU4 Security, Accountability and Fight against Crime in Georgia"[15] Programme focuses on the fight against crime, cyber and hybrid threats, border management, civil protection and supervision of the security sector. SAFE envisages to implement this Twinning project by the DEA and CSB of the MoD under component 2 – Hybrid and Emerging Threats. Another Twinning project on Cybercrime and Critical infrastructure is planned under the same component.

Implementation of the new regional programme '**EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries'**[16] has been recently launched. It will contribute to improving the cyber-resilience and criminal justice response of the EaP countries. The programme has two key building blocks: First, the development of technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks; second, the full implementation of an effective framework to combat cybercrime, including: substantive and procedural criminal legislation; law enforcement and judicial authorities' capacity to investigate, prosecute and adjudicate cases of cybercrime; measures to enable international cooperation; and cooperation between public authorities and private entities. The Budapest Convention continues to provide the benchmark for an effective framework. The proposed actions will be implemented, when appropriate, at regional level but also at country level to address specific needs of the individual EaP countries according to the differentiated approach of the revised European Neighbourhood Policy. The programme is implemented through the following two projects: **'Action on Cybercrime for Cyber Resilience in the Eastern Partnership region'** (CyberEast) implemented by the Cybercrime Programme Office of the Council of Europe (C-PROC)[17] that started its implementation in 2019 and Technical Assistance project

[13] E.g. (a) In May, 2019 the forth National Cyber Olympiad - CyberCube 2019 was held for 120 participants (pupils and students from schools and universities from Tbilisi and regions). (b) For cyber professionals so called "Red and Blue Team" exercises CyberEx2019 will be held already in autumn of 2019 for the fourth consecutive time. (c) Students are offered 8-week internship in Data exchange Agency where they are working together with Computer Emergency response Team (CERT.GOV.GE) on technics and tools for identifying and handling cyber incidents. "Cyber Class" will be conducted in October-November 2019 for the fifth year. (d) Data Exchange Agency has designed online platform for cybersecurity courses that can be used by universities and training centres. (e) In the course of 2019 CERT.GOV.GE conducted cyber hygiene trainings for students and teachers, media representatives and NGO communities in different regional cities of Georgia; (f) Georgian Cybersecurity Forum took place systematically in 2014-2019 as public-private multi-stakeholder platform, creating trust among all stakeholders and sharing information and knowledge, getting new initiatives, as well as enabling private sector engagement in policy and strategy development process.

[14] E.g. NATO Smart Defence initiative which is an ongoing way of cooperation aimed at generating modern defence capabilities that the alliance needs, in a more cost-efficient, effective and coherent manner. Since 2016 Cyber Security Bureau (CSB) is actively involved in NATO Smart Defence two projects: (a) NATO Multinational Malware Information Sharing Platform MISP – becoming a full member of the platform will enable bureau to eliminate duplication of analytical work, faster threat detection and improve threat intelligence and attribution Involvement. Cyber Security Bureau will become a hub on information sharing between NATO and national actors, which will facilitate closer interagency cooperation; (b) NATO Multinational Cyber Defence Education and Training MNCD E/T – The aim of the Project is to help nations identify education and training needs and fill gaps created by their cyber defence capability development processes. Project also intended to develop a cyber defence curriculum that will be a valuable supporting tool for the future NCI Academy.

[15] The SAFE Programme Action Document https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/eni_2018_041443_eu4security_accountability_and_fight_agaisnt_crime.pdf

[16] Action Document for EU4Digital https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/c_2018_8184_f1_annex_en_v1_p1_1000418.pdf

[17] https://www.coe.int/en/web/cybercrime/home

‘EU4Digital: Improving Cyber Resilience in the EaP Countries – Cybersecurity Component’ implemented by a consortium led by GFA Consulting Group[18] launched in January 2020.
Twinning project **"Promote the strengthening of E-Governance in Georgia (E-Government Georgia”)**. Overall objective of the project was to build capacity of Georgian Administration in implementation of reforms and democracy for the benefit of people by using of ICT. Project purpose was to strengthen the capacities of Data Exchange Agency to consequently implement the best and the most suitable e-policies in Georgia based on EU practice. Budget of the project: EUR 1.2 million. Duration: 11/2012 - 08/2014.

Twinning project **"Strengthening E-Governance in Georgia II"** – supporting the institutional development of the DEA and enhancing the necessary skills and knowledge of the Agency’s staff on providing training, consultancy, benchmarking and promotion of e-government and information security in line with the European Union standards. Budget of the project: EUR 1.3 million. Duration: 09/2015 - 06/2017.

Related Programmes and Projects

The reform of Public Administration (PAR) is of utmost importance for the country and the process is supported through donor community. The EU total contribution to the **“Support to the Public Administration Reform in Georgia”** 2016-2019, is EUR 30 million. Out of which EUR 20 million is budget support share and EUR 10 million for complementary support. The objective of the programme is to improve the efficiency, accountability and transparency of the public administration of Georgia, in line with the key Principles of Public Administration that have been developed by OECD/SIGMA in close cooperation with the European Commission. It has a particular focus on the improvement of the policy planning and coordination capacities and processes in the central public administration. The professionalization of the civil service (including the reform of the civil service training system) is also supported through the programme. The **Public Administration Reform Action Plan 2019-2020** adopted by Government Decree N. 274 of June 10th, 2019 directly highlights government efforts to be undertaken for cyber protection of critical information networks and infrastructures: “In order to ensure the high standard of governance, the high level of safety and security of critical information infrastructures and information systems are also very important. New action plan defines the activities, which will ensure the safety and security of such systems and in general, will raise the awareness regarding the cyber and information security.” (Chapter 4, Public Administration Reform Action Plan 2019-2020). In particular it includes the following activities: development of the methodology for defining the critical information system subjects, implementation of intrusion detection system in public sector, creation of curricula for cyber hygiene in the schools and relevant updated training materials for e-learning platform (https://elearning.dea.gov.ge/).

“Support to the Public Administration in Georgia"- EU funded; Duration: 2019-2021; Description: The objective of the project is to improve the efficiency, accessibility, accountability and transparency of the Georgian Public Administration in accordance with European principles of Public administration and best practices. More specifically, the project is mainly focused on improving the results-based approach in policy planning, development, coordination, monitoring and evaluation, increasing the awareness of the Civil servants and streamlining the implementation of the civil service reform in public institutions, improving the intra and inter-ministerial business processes related to policy making and service delivery enhancing thus the efficiency of the administration and the quality of service delivery, strengthening policy development and implementation of the anti-corruption and transparency national policies, thus increasing the accessibility, accountability and transparency of the executive branch and combating corruption, establishing an efficient, accountable and transparent institutional and legal framework for efficiently, timely and reliably delivered public and electronic services and raising public awareness and increasing visibility of the Government’s public administration reform agenda as well as on available public services.

Twinning project **“Capacity Building of the Civil Service Bureau of Georgia to Implement the Civil Service Reform” -** EU funded; Duration: 2018-2020. Description: The objective of the project

[18] https://www.gfa-group.de

is to enhance the professionalism of the civil service in Georgia. More specifically, the project aims to strengthen the institutional and Human Resource (HR) capacities of the Civil Service Bureau to manage the implementation of the Civil Service Reform, through the reinforcement of the legal framework, introduction of modern Human Resource Management (HRM) information system, tools and techniques, development of training scheme for HR managers and improvement of Assets Declaration Monitoring system.

"Facility for the implementation of the Association Agreement in Georgia" - EU funded; Duration: 2015-2018; Description: The project provided policy advice and capacity building support to the GoG in coordinating the implementation of the Association, strengthening the institutional capacities of the line ministries and other public institutions to carry out the required reforms, including on policy development and legal approximation processes.
Since February 2019, phase II of the aforementioned project has been launched. Duration: 2019-2021. The project provided assistance to DEA through expert mission to support identification of relevant and important aspects of NIS Directive to be taken into consideration while approximation process and Twinning project preparation stage.

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

EU-Georgia Association Agreement aims to strengthen the Georgian public institutions' capacity. 2017 – 2020 Association Agenda between the European Union and Georgia[19] (2.6. Economic Development and Market Opportunities, sub-part: Cooperation in the Field of Digital Economy and Society) refers to "efforts 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". It is expected that this Twinning project will cover all priorities stipulated in the Agenda, in particular the following Union *acquis*:

- EU External Cyber Capacity Building Guidelines – Council Conclusions and Operational Guidance.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive);
- Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 as regards managing the risks by digital service providers posed to the security of network and information systems and determining a substantial impact of incident.

In addition, new regulations, normative acts, rules and standards should be developed and implemented in order to cover existing gaps between national and EU legislation.

3.5 Components and results per component

At the completion of the project the following results are expected to be achieved under this Twinning project:

Mandatory Result 1 / Component 1: Georgian national cybersecurity institutional governance model strengthened

Development of cybersecurity framework requires creation of well-defined, properly structured and adequately functioning institutional governance model. In order to approximate the national relevant legal and policy frameworks to the NIS Directive, it will be necessary to adjust the current institutional setting, including: the definition of political sponsorship and leadership; establishment of interinstitutional cooperation and coordination platforms; designation of governmental authorities for strategic and operational levels; identification of key private stakeholders (e.g. critical information

[19] https://eeas.europa.eu/sites/eeas/files/annex_ii_-_eu-georgia_association_agenda_text.pdf

infrastructures, CSIRTs, academia, training and education resources.) as part of the national cybersecurity ecosystem and enact a national level strategic document on cybersecurity that will define strategic objectives and goals on high political level. Sustainable cybersecurity governance architecture will provide a solid precondition for smooth transposition of NIS Directive into national frameworks as well as a must step for cybersecurity development of the country.

The Twinning project will play a crucial role in the proper definition of the institutional-organisational model for NIS transposition taking into account existing governance framework and redistribution of cyber powers. As a result of this Component, policy and legal amendments on renewed institutional architecture will be designed, agreed among stakeholders and promoted for approval by the relevant authorities and in addition the Twinning project will play a crucial role in the reviewing of the next NCSS for NIS implementation. In order to align the Georgian NCSS with the requirements set forth by the NIS Directive, it will be necessary to perform a review of the draft of the third revision and to update and amend it accordingly where required. As a result of this Component, revised and renewed NCSS document will be available and agreed among stakeholders and promoted for approval by the relevant authorities.

Sub-Result 1.1: National competent authority/authorities (including CSIRT) designated and fully functional to take the role, tasks and responsibilities required by NIS Directive

Specifically, the process of delivering this sub-result will focus on developing the institutional framework and respective supporting legal documents for establishment/designation of the Single Point of Contact (SPOC) - the competent national authority/authorities with the legal powers to development national cybersecurity strategic, legal and policy documents, lead and participate in coordination groups, set regulatory norms for national critical information infrastructures and provide cybersecurity services and other relevant functions in accordance with NIS Directive. One or more well-functioning CSIRT(s) has to be designated, which will be authorized to fulfil the tasks according to the NIS Directive (including receiving notifications of incidents). The designated CSIRT(s) will also function as interface to European CSIRTs network and will guarantee effective and compatible capabilities to deal with incidents and risks.

Sub-Result 1.2: National cybersecurity coordination framework created

A national coordination structure for political, strategic and operational coordination activities concerning cybersecurity needs to be defined and put operational in order to transform political goals in cybersecurity strategies, define national cybersecurity policies, action plans, priorities and key initiatives, and develop situational awareness and cyber crisis management procedures.

Sub-Result 1.3: Public-private cooperation platform established

As private entities (critical information infrastructures, academia, civil society organisations, private initiatives, training and consulting entities, etc.) play a critical role in the cybersecurity ecosystem, an inclusive approach for communication and alignment with private stakeholders will be established in order to strengthen the overall security posture and to assure consensus from private stakeholders on nation-wide cyber goals and initiatives.

Sub-result 1.4: The third Georgian NCSS reviewed in the context of the requirements of the NIS Directive

The Georgian NCSS is the most important document among the cyber and information security policy documents and is legally substantiated by the resolution of the government of Georgia. The process of delivering this sub-result will concentrate on reviewing and updating the draft of the third Georgian NCSS and the annexed action plan accordingly. The process betokens going through the document, finding all the incompliances with the NIS Directive (article 7) and updating accordingly with the involvement of multi stakeholder group.

Mandatory Result 2 / Component 2: Legal, operational and technical frameworks developed enabling the protection of critical information infrastructures (CIIP) and operators of essential services (OES) as per the NIS Directive.

As an aspiration to closer integration with the EU, Georgia aims to design legal, operational and technical architecture enabling protection of critical information infrastructures that will be interoperable with EU analogue systems. The NIS implementation and associated to this process of critical information infrastructures' protection, requires the creation and setup of comprehensive legal instruments, operational measures and technical processes as well as definition of proper policies and tools. In order to properly identify all relevant and important legal, operational and technical components, Georgia will require EUMS technical support in defining and building-up the key constituencies, analysing and reviewing related regulatory constraints in accordance with NIS process.

Sub-result 2.1: Critical information infrastructures and operators of essential services identified and notified

Georgia will need to carry out an identification process, which will ultimately determine which sectors and individual companies belong to the type of entities listed in Annex II of NIS Directive and have a legal establishment on the territory of Georgia. This identification process will involve a national risk assessment, requiring the national authorities to assess whether a cyber-incident would have a significant disruptive effect on the provision of the service as well as evaluation of several cross-sectorial factors that need to be taken into account when defining questionnaire and methodology for critical information infrastructure identification process. As a result, the identification and notification process and methodology will be described, thresholds for critical information infrastructures will be composed, cross-sectoral dependencies between critical information infrastructures will be identified and the list of critical information infrastructures defined.

Sub-result 2.2: Incident notification requirements and procedures defined

Beneficiary will need to design the process, methodology and tools for cyber incident notification among the stakeholders effected by NIS Directive; namely, it is required to set-up the legal, operational and technical frameworks for incident notification requirements for critical information infrastructures and their interactions with CERT/CSIRTs and other state authorities; also, cyber incident taxonomy, parameters and thresholds need to be specified that have to be taken into account when defining the substance, significance and notification requirement of a cyber incident. Consequently, based on the defined parameters and thresholds, notification requirements, templates and processes, incident notification infrastructure/platform has to be established.

Sub-result 2.3: Mandatory security requirements for critical information infrastructures and operators of essential services defined

Beneficiary will need to design the legal requirements for defined critical information infrastructures in accordance with the NIS Directive. Those mandatory legal requirements will ensure that critical information infrastructures, having regard to the state of art, take appropriate and proportionate cyber and information security measures, technical and organisational actions to manage the risks and threats posed to the security of network and information systems which the organisations use in the provision of their services. EUMS will help Georgia in defining mandatory security requirements for critical information infrastructures that will be reflected in respective legal documents.

Sub-Result 2.4: Procedures for review and audit of security requirements for critical information infrastructures and operators of essential services defined

It is necessary that the competent authorities have the necessary powers and means to assess the compliance of critical information infrastructures with their legal obligations defined in accordance with NIS Directive and the effects thereof on the security of network and information systems. Therefore, it is necessary to define audit rules, legal procedures for assessment and review of the maturity of cybersecurity of critical information infrastructures according to the Georgian law and NIS security requirements.

Mandatory Result 3 / Component 3: Operational Cyber related capacities & capabilities of the national cybersecurity authorities and other stakeholders strengthened

The implementation of the NIS Directive imposes many requirements on the cyber capacities and capabilities of Georgia. The definition, creation and operations of the policies, procedures and structures required by the NIS Directive requires building adequate capacities at all key stakeholders involved in the cyber ecosystem of Georgia. Since skilled cyber resources are scarce in Georgia, a key enabling factor for NIS implementation in Georgia and successful raising of cyber posture will be increasing qualifications of key members of the Georgian authorities, especially at the national competent authority. In addition to qualification of authorities and key stakeholders, it will be essential for the long-term effectiveness of the NIS implementation to develop a broad awareness for cybersecurity in the GoG as well as in the Georgian economy and society as a whole.

Sub-result 3.1: Qualification requirements of cybersecurity professionals identified/skill pipeline developed

This sub-result will focus on defining of qualitative and quantitative cybersecurity skill requirements of beneficiary and other relevant cyber authorities according to their defined responsibilities; mapping of cybersecurity skill requirements to existing cybersecurity training profiles and curricula (courses and certifications) will be conducted.

Sub-result 3.2: Cybersecurity capacity building activities performed

After qualification needs assessment of key authorities, respected cybersecurity training and capacity building activities will be performed. As a result, cyber specialists will be trained and certified accordingly.

Sub-result 3.3: Strategy for building cyber awareness and education capacities within Georgia's information society elaborated

A mid- to long-term strategy for building education, awareness-raising and training programmes system for ensuring needful capacities will be developed. It may also be integrated into the NCSS of Georgia covering cyber awareness and education in the society and economy of Georgia. This shall assure a long-term increase of cyber awareness and knowledge among the information society of Georgia.

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). The implementation of the project requires 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, 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 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 detail 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 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 inter-linked and need to be sequenced accordingly.

3.6.1 Profile and tasks of the PL:

Profile:

- A high ranking current official of a Member State administration in relevant field
- University level education in a relevant discipline (e.g. Cyber and/or Information Security, Computer Sciences, IT Law), or equivalent professional experience in a related field of 8 years;
- Relevant managerial position in policy development/implementation/coordination of ICT, cyber / information security or other relevant field;
- At least 3 years’ experience in the field of cyber and information security;
- Good understanding of regulatory/institutional system of cybersecurity, and its organisational model in their Member State;
- Previous experience in the field of project management, with a demonstrable record of organisational leadership and reform implementation;
- Knowledge of EU cyber related legislation;
- 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 field of cybersecurity;
- 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 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;

- Co-chairing of project steering committees.

3.6.2 Profile and tasks of the RTA:

Profile:

- University level education in a relevant discipline (e.g. Cyber and/or Information Security, Computer Sciences, IT Law) 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 field of Cyber/information security or relevant fields;
- Good knowledge of legal approximation process, relevant EU legislation and institutional requirements related to various components of this project;
- Sound knowledge of cybersecurity, management, quality control and supervision;
- Working experience on EU cyber and/or information security legislation in a Member State would be an asset;
- Collaboration experience with ENISA, CoE, EC and other relevant EU/international organisations 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;
- Develop the initial and subsequent work plans, and project progress reports together with PL to be submitted to the Steering Committees;
- Coordinate 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.

3.6.3 Profile and tasks of Component Leaders:

Component 1: Georgian national Cyber security institutional governance model 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 field of IT, Cyber and/or Information Security or other related areas;
- Sound knowledge of cyber 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 institutional requirements related to this component;
- Good understanding of legal and operational procedures for the enforcement of laws and sub laws relevant to this component;

- 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.

Component 2: Legal, operational and technical frameworks developed enabling the protection of critical information infrastructures (CIIP) and operators of essential services (OES) as per the NIS Directive

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 field of IT, Cyber and/or Information Security or other related areas;
- Knowledge of technical and operational issues at their MS level;
- Experience and/or good understanding of cybersecurity.

Tasks:

- Conducting analysis of the area relevant to the component
- Identification and notification system of critical information infrastructures;
- Defining incident notification requirements, procedures and taxonomies;
- Defining mandatory security requirements for critical information infrastructures;
- Defining procedures for review and audit of security requirements for critical information infrastructures.
- Contributing to the interim and final reports

Component 3: Operational cyber related capacities & capabilities of the national cybersecurity authorities and other stakeholders strengthened

Profile:

- University level education in public administration, education policy or other relevant discipline/equivalent professional experience in a related field of 8 years;
- At least 3 years of professional experience in the field of public administration, education policy, cyber and/or information security (with focus on human resources management and professional development would be an asset);

- Relevant experience in capacity building activities and human resources development relevant to the scope of this component;
- Good knowledge of legal approximation process, relevant EU legislation and institutional requirements related to this component;
- Good understanding of legal and operational procedures for the enforcement of laws and sub laws relevant to this component;
- Good communication, coaching and mentoring skills;
- Strong analytical and report writing skills;
- Good managerial and organisational skills;
- Good team-working, presentation and advisory skills;
- Fluency in written and spoken English;
- Computer literacy.

Tasks:

- Component coordination, guidance and monitoring;
- Conducting analysis of the area relevant to the component;
- Drafting thematic/technical contributions and documents relevant for the results of the component, in close collaboration with BC counterparts and relevant project experts, and Georgian institutions;
- Identifying qualification requirements;
- Drafting thematic/technical contributions and documents relevant for the results of the component, in close collaboration with BC counterparts and relevant project experts, and Georgian institutions;
- Preparing and conducting training programs, information and dissemination seminars with various stakeholders;
- Preparing and conducting workshops with various stakeholders;
- Performing cybersecurity qualification measures;
- Defining mid- to long-term strategy for building training and education capacities in Georgia's society and economy;
- Drafting thematic/technical contributions and documents relevant for the results of the component, in close collaboration with BC counterparts and relevant project experts, and Georgian institutions;
- Preparing timely proposals for any corrective measures;
- Contribution in report writing relevant to this component;
- 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 (e.g. Cyber and/or Information Security and/or IT Law/ public administration) or equivalent professional experience in a related field of 8 years;
- At least 3 years of professional experience in the relevant field;
- Specific knowledge and working experience on legal approximation issues with focus on technical requirement for cyber and information security;
- Experience in harmonizing national law of any member state with NIS Directive would be an asset;
- Specific knowledge of organisational structure, statutory models and institutional capacities of cybersecurity ecosystem in their MSs;
- Sound knowledge and particular skills in strategy and policy development;
- Experience in awareness raising, information campaigns and knowledge of different communication tools;

- Coaching, training and facilitator skills;
- Experience in developing of training modules and materials, good record in training delivery;
- Previous experience in EU-funded Twinning Project 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 documents in accordance with the national rules for legislative development in their respective fields;
- Contributing in preparation of strategy documents, 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

The EU Delegation to Georgia will be responsible for the 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

The following Twinning Project is a multi-angle form institutional standpoint considering the diverse nature of cybersecurity and numerous parties involved in the cybersecurity ecosystem; Moreover, the

NIS Directive itself is structurally very complex and it requires that different authorities are involved in its implementation process. Although beneficiary of this project is the whole Government of Georgia with its cybersecurity mandate, for the project management purpose as it is required by Twinning Manual and applicable practice, LEPL Data Exchange Agency will act as a primary and direct beneficiary administration for the project.

The DEA (up to 15 directly involved staff members and totally 45 employees) will closely collaborate with the Cyber Security Bureau of the Ministry of Defence of Georgia, Ministry of Internal Affairs of Georgia, its cybercrime investigation Unit and Analytical Department, State Security Service of Georgia and its Operation-technical Agency, all line ministries and other private, civil society organisations and academic stakeholders in the field.

Bearing in mind experience of managing two Twinning projects in the past, for the smooth and timely implementation of the project, DEA will designate responsible structural units and within those units assign different project related roles and function to its employees. The preliminary structure, alongside Project Leader’s and RTA counterpart’s roles, most probably will be following:

a) Legal Division – will be responsible for the general management of the project, direct contact with RTA, Component Leaders and field short-term experts; Legal Division will take charge of leading legal component of the Twinning project with all its legal related expertise (incl. law-making process). (3 colleagues);

b) Information Security Team – will be responsible on cybersecurity policy, methodology for critical information infrastructure identification and private stakeholder engaging topics and other interrelated aspects. (3 colleagues);

c) CERT.GOV.GE - will provide technical expertise and act as direct counterpart for the project technical cybersecurity related work (5 colleagues);

d) Administrative Division – will support RTA and its staff in logistical and administrative side of the project, arranging workshops and meetings with Georgian stakeholders (2 – 3 colleagues);

All abovementioned divisions with its staff members will be involved in the implementation of the Twinning project components within the scope of their competencies.

In order to ensure multi-stakeholder approach and involvement of all relevant parties in the Twinning project, DEA will organise thematic working groups with CSB, NSC, MIA and SSSG/OTA representatives as well as invite subject-matter experts from private sector in different project activities. Although SSSG/OTA and MIA do not have cybersecurity authority that will be directly influenced by the Project, considering the fact that cybercrime investigation as well as cyber intelligence are closely interrelated with cybersecurity domain, active involvement in project related work, will give all of them a good information sharing opportunity.

5.3 Counterparts in the Beneficiary administration

5.3.1. Contact Person / RTA Counterpart:

Ms. Nata Goderdzishvili

Head of Legal Unit at LEPL Data Exchange Agency

Ministry of Justice of Georgia

17 Giorgi Danelia Street, Tbilisi 0186, Georgia

5.3.2. Project Leader Counterpart:

Mr. Nikoloz Gagnidze

Head of LEPL Data Exchange Agency

Ministry of Justice of Georgia
17 Giorgi Danelia Street, Tbilisi 0186, Georgia

5.3.3. Contact Person from CSB:
Mr. Luka Mgeladze
Analyst at Information Security Policy and Risk Assessment Division at LEPL Cyber Security Bureau
Ministry of Defence of Georgia
30 Dadiani Street, Tbilisi 0105, Georgia

6. Duration of the project

The duration of the project execution period: 27 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 DEA, CSB, SSSG/OTA, MIA, NSC, Member State partner institutions, the EU Delegation to Georgia and Programme Administration Office (PAO) of the Ministry of Foreign Affairs of Georgia.

The PSC shall oversee the implementation of the project. The main duties of the PSC include verification of the progress and achievements via-à-vis the mandatory results/outputs chain (from mandatory results/outputs per component to impact), ensuring good coordination among the actors, finalising the interim reports and discuss the updated work plan. The PSC meetings could be attended by the 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 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

The mandatory results and outcomes of the project are in full compliance with the national strategic priorities in the field of cyber and information security. Sustainability will be ensured by enacted legal framework and institutional background, redistributed and clearly defined authorities that unambiguously split rights and responsibilities among key actors; After completion of the project, Georgia will be one of the few non-EU Member States with EU interoperable cybersecurity legal framework which, of course, 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 either published for public access or spread among the relevant stakeholders.

Beneficiary administration will ensure that necessary financial resources are annually allocated for the capacity building/upgrade of its cyber professionals in order to equip them with new skills and knowledge for better performance of their cybersecurity functions. Human resources development in the field of cybersecurity will be the key policy and strategic component for the beneficiary administration.

Last but not least, the institutional sustainability of the project achievements will be embedded in the routine functions and works of the Data Exchange Agency and other stakeholders.

9. Crosscutting issues

The principles of the equal opportunity will be insured during the project implementation period. The principles of equal opportunities will be applied to all involved parties and stakeholders through the project implementation process as well as will be reflected in all documents developed during the project.

10. Conditionality and sequencing

This Twinning Project Fiche has been drafted with direct participation and high involvement of the Data Exchange Agency and Cyber Security Bureau. The DEA insures to provide input to all project activates stated 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, DEA will:

- Provide strong commitment and support of DEA management to the Project implementation
- Assign relevant skilled staff at all levels, as component leaders and experts
- Ensure participation of the relevant DEA staff members as well as other stakeholders in project events
- Ensure coordination between departments and other stakeholders of the project. Beneficiary administration together with CSB will coordinate project activities with the National Security

Council, SSSG/OTA and MIA and when relevant with other government and private cyber stakeholders.

- Ensure access to important information, regulation, legislation, all supporting documentation relevant to the Project

As mentioned above in order to ensure multi-stakeholder approach and involvement of all relevant parties in the Twinning project, DEA will organise thematic working groups with CSB, NSC, MIA and SSSG/OTA representatives as well as invite subject-matter experts from private sector in different project activities. Based on its duties in the Cyber Defence sector, CSB has the greatest role to play together with DEA in the Twinning implementation process, for that reason, DEA-CSB will establish clear communication policy on planning and running Twinning activities, all agreements will be made on a mutually respectful manner and considering common goals and whole-of-government approach.

Beneficiary acknowledges that success of the project greatly depends on the readiness of its administration to handle the intensive workload of the project and absorb project resources in most efficient manner.

It is anticipated that the results of the project will strengthen DEA, CSB and other key government stakeholders in managing their respectful cybersecurity authorities. The project envisages designation of the National Competent Authority in accordance with NIS Directive, which may entail number of institutional (functional or/and structural) changes in the cybersecurity governance model.

The project outcomes will be stemmed from the sequencing of legal amendments, strategic insights and institutional adjustments that could therefore be initiated early on. The concrete sequencing of project components will be discussed and agreed with the selected EU MS during the work plan negotiation phase.

11. Indicators for performance measurement

The project MS and BC partners will ensure the smooth implementation of project activities and assess performance measurement in line with the logical framework. Through the project operation phase the project counterparts will meet regularly to ensure consistency of project implementation and achievement of the results.

Component 1 – Georgian national Cyber security institutional governance model strengthened

Indicator(s) of performance:

- Status of legal amendments and regulatory documents redefining cybersecurity governance model;
- Usage of the coordination mechanism among government actors;
- Usage of the formalized public-private communication/cooperation mechanism on all relevant spheres of cooperation.

Sub-Result 1.1: National competent authority/authorities (including CSIRT) designated and fully functional to take the role, tasks and responsibilities required by NIS Directive

Indicator(s) of performance:

- Availability of set of recommendations on the enhancement of the institutional-organisational structures and authorities (including CSIRT) according to NIS Directive;
- Status of amendments to Georgian information security law and secondary legislation;
- Status of amendments to CSIRT(s) regulatory acts.

Sub-Result 1.2: National cybersecurity coordination framework created

Indicator(s) of performance:

- Availability of set of recommendations on defining authorities for different cyber incidents scenarios;
- Status of legal or policy document(s) on coordinating authority roles and coordination scheme.

Sub-Result 1.3: Public-private cooperation platform established

Indicator(s) of performance:

- Availability of memorandum of understanding (MoU)[20] for cybersecurity cooperation and collaboration between relevant public and private organisations;
- Number of cooperation actions between public and private stakeholders.

Sub-Result 1.4: The third Georgian NCSS reviewed in the context of the requirements of the NIS Directive

Indicator(s) of performance:

- Status of the assessment document comparing the existing NCSS with NIS requirements.

Component 2 - Legal, operational and technical frameworks developed enabling the protection of critical information infrastructures (CIIP) and operators of essential services (OES) as per the NIS Directive.

Indicator(s) of performance:

- Critical information infrastructures' operational and technical capabilities to handle cyber threats and incidents.

Sub-Result 2.1: Critical information infrastructures and operators of essential services identified and notified

Indicator(s) of performance:

- Status of the draft policy document on critical information infrastructures' identification methodology;
- Availability of the draft list of critical information infrastructures;
- Share of critical information infrastructures participating in communication/collaboration mechanisms/platforms.

Sub-Result 2.2.: Incident notification requirements and procedures defined

Indicator(s) of performance:

- Availability of parameters and thresholds for incident classification;
- Availability of incident notification templates and procedures;
- Availability of manuals/guidelines on incidents classification and reporting;

[20] Memorandum of Understanding (MoU) will be accessible to any interested public and private entities for enrollment.

- Status of cyber incident notification and information sharing platform.

Sub-Result 2.3.: Mandatory security requirements for critical information infrastructures and operators of essential services defined

Indicator(s) of performance:

- Status of set of recommendations on legal, organisational and technical mandatory measures for critical information infrastructures;
- Availability of the normative documents enlisting security rights/obligations for critical information infrastructures.

Sub-Result 2.4.: Procedures for review and audit of security requirements for critical information infrastructures and operators of essential services defined

Indicator(s) of performance:

- Status of set of recommendations on review and audit requirements;
- Availability of legal document on cybersecurity review and audit of critical information infrastructures by competent authority.

Component 3 – Operational cyber related capacities & capabilities of the national cybersecurity authorities and other stakeholders strengthened

Indicator(s) of performance:

- Institutional and human capacity of Georgian cyber authorities ensuring performance of their responsibilities under NIS Directive;
- Availability of professional capacities and technical capabilities among various stakeholders within cybersecurity ecosystem.

Sub-Result 3.1: Qualification requirements of cybersecurity professionals identified / skill pipeline developed

Indicator(s) of performance:

- Availability of gaps and needs analysis report;
- Availability of the capacity needs analysis document.

Sub-Result 3.2: Cybersecurity capacity building activities performed

Indicator(s) of performance:

- Availability of the training plan;
- Share of/number of trained and skilled cybersecurity specialists capable to perform new functions in accordance with NIS Directive;
- Share of information security specialists capable to conduct review and information security audits in accordance with NIS Directive;
- Share of critical information infrastructure representatives informed on new legal, operational and technical requirements based on NIS Directive.

Sub-Result 3.3: Strategy for building cyber awareness and education capacities within Georgia’s information society elaborated

Indicator(s) of performance:

- Availability of the survey on the cyber awareness of Georgian information society;
- Status of the cyber awareness and education strategy.

12. Facilities available

The Beneficiary commits itself to deliver the following facilities:

- Adequately equipped office space for the RTA and the RTA assistant(s) for the entire duration of their secondment;
- Supply of office room including access to computer, telephone, internet, printer, photocopier;
- Adequate conditions for the STEs to perform their work while on mission;
- Provide suitable venues for the training sessions and meetings that will be held under the Project;
- Security related issues will be assured according to the standards and practices applicable for all Georgian public institutions.

ANNEXES TO PROJECT FICHE

1. Simplified Logical Framework
2. DEA Organisational Chart
3. CSB Organisational Chart

Annex 1

Simplified Logical Framework

Project Title: **Strengthening Cybersecurity Capacities in Georgia**				Programme name and number: **“EU4 Security, Accountability and Fight against Crime in Georgia (SAFE)", ENI/2018/041-443, Direct Management**	
Beneficiary Institution: **LEPL Data Exchange Agency**				Total budget: **1, 300,000 €**	EU ENI financing (100%)
	Description	**Indicators (with relevant baseline and target data)**	**Sources of verification**	**Risks**	**Assumptions (external to project)**

Overall Objective	To strengthen Georgia’s preparedness and resilience towards cyber threats and attacks, by capacity building of Georgian stakeholders and creating enabling cybersecurity frameworks, in line with the EU’s approach, standards, and relevant legal and policy framework, notably but not limited to the	- Interoperability of Georgian cyber security systems with EU relevant systems.
		Baseline: 2019 - Limited interoperability of Georgian cyber security systems with EU relevant systems.
		Target: 2025 - Full interoperability of Georgian cyber security systems with EU relevant systems.
		- Georgia's international standing (rankings and indicators) in cybersecurity.
		Baseline: According to ITU Global Cybersecurity Index 2018 Georgia’s
			Monitoring/assessment reports by EU institutions/relevant experts;
			National Cybersecurity Strategy (2020-2022) implementation monitoring report;
			ITU Global CyberSecurity Index		

	NIS Directive.	global rank is #18 and regional rank is #9. Target: By 2022 improved by at least one position in each ranking.			
Specific (Project) Objective(s)	The specific objective of the project is to strengthen Georgia's cybersecurity legal and institutional frameworks to increase its security level of networks and information systems, as well as its level of prevention, preparedness, reaction and resilience to cyber incidents and threats. The benchmark for this will be the EU's relevant policy and legal framework, namely the NIS Directive and the EU's external cyber capacity building guidelines. The project will carefully follow the EU's approach to promoting a rules-based cybersecurity	- Availability of all enabling frameworks and technical tools necessary for handling cyber incidents in a timely and efficient manner. Baseline: 2019- Limited compliance with NIS Directive. Target: 2022 - Full compliance with NIS Directive.	Monitoring/assessment reports by EU institutions/relevant experts Report on implementation of AA & National Action Plan for Georgia's Integration in EU 2019-2021 DEA Reports	Change in political situation in Georgia; Difficulties related to the drafting and implementing of the upgraded legislation; Lack of commitment from respective actors; Delays in adopting new/or amended legislation.	Government commitment on fulfilment of AA requirements continued; Strong support and commitment from the management of the beneficiary; Strong support and commitment from twinning partner(s); Relevant staff of the beneficiary available and involved in the project; Timely decisions made by Government; Co-operation with relevant stakeholders;

	governance in full respect of Human Rights and Fundamental Freedoms. It will take into consideration a whole-of-government and whole-of-society approach for an inclusive and accountable policy and decision-making process, involving CSOs, civic actors and the private sector. All this will benefit the citizens, the whole information society and digital economy of Georgia.				
Mandatory results/outputs by components	**Mandatory result 1:** Georgian national Cyber security institutional governance model strengthened	- Status of legal amendments and regulatory documents redefining cybersecurity governance model; Baseline: 2019 – Amendments not elaborated Target: By the end of the project - Normative acts submitted for enactment to the Parliament of Georgia, GoG and/or adopted by respective ministries - Usage of the coordination mechanism	LEPL Legislative Herald of Georgia - www.matsne.gov.ge; Reports on stakeholder consultations; Project documentation: legal analysis reports, institutional analysis reports, recommendations,	Difficulties in finding a consensus among authorities on cybersecurity governance model (incl. redistribution of powers and coordination scheme) Delays during the project implementation; Lack of understanding among relevant	Strong commitment on cybersecurity at political level ensured Collaboration between all stakeholders Agreement and involvement of all stakeholders.

		among government actors; Baseline: 2019 – Ad hoc coordination and limited cooperation actions among government actors. No institutionalized structures for coordination created at the national level[21]. Target: By the end of the project – Annually at least 5 joint actions performed. - Usage of the formalized public-private communication/cooperation mechanism on all relevant spheres of cooperation. Baseline: 2019 – Public-private communication/cooperation on ad hoc basis. Target: By the end of the project – At least 5 joint actions implemented. - Status of NCSS and action plan of Georgia. Baseline: 2019 – draft of NCSS for 2020-2022 Target: By the end of the first half of the project – Final draft of the NCSS and action plan elaborated and agreed among relevant stakeholders.	workshop reports, STE mission reports etc. Project quarterly and final reports. Final draft of the NCSS and action plan; Information on dissemination of NCSS and action plan; Reports on stakeholder consultations	stakeholders.	

[21] 2019 Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre, assesses Georgian institutional framework with limited cooperation mechanisms.

	Mandatory result 2: Legal, operational and technical frameworks developed enabling the protection of critical information infrastructures (CIIP) and operators of essential services (OES) as per the NIS Directive	- Critical information infrastructures' operational and technical capabilities to handle cyber threats and incidents. Baseline: 2019 – Limited capabilities. Target: By the end of the project – Increased capabilities to handle responsibilities according to the NIS Directive.	LEPL Legislative Herald of Georgia - www.matsne.gov.ge; Project documentation: legal analysis reports, institutional analysis reports, recommendations etc. Project quarterly and final reports	Difficulties related to the implementation of the upgraded legislation; Delays in adopting new/or amended legislation; Lack of appropriate human resources; Lack of material-technical resources; Need for additional financial interventions.	Strong collaboration and involvement at all levels including media, governmental, educational, donor, non-governmental and private organisations ensured Proactive cooperation between Twinning partners ensured
	Mandatory result 3: Operational cyber related capacities & capabilities of the national cybersecurity authorities and other stakeholders strengthened	- Institutional and human capacity of Georgian cyber authorities ensuring performance of their responsibilities under NIS Directive; Baseline: 2019- Limited institutional and human capacity of Georgian cyber authorities[22]. Target: By the end of the project – Enhanced institutional and human capacity of Georgian cyber authorities ensuring performance of their responsibilities under NIS Directive. - Availability of professional capacities and technical capabilities among various stakeholders within cybersecurity ecosystem;	Project documentation: (list of participants from various meetings & trainings, training programmes, training materials, training reports) Draft of the cyber awareness and education strategy; Twinning Project assessment report.	Lack of appropriate human resources;	Strong collaboration and involvement at all levels including media, governmental, educational, donor, non-governmental and private organisations ensured; Relevant human resources available and involved in the project;

[22] According to 2019 Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre, framework for cybersecurity professional training in Georgia is in the formative stage.

		Baseline: 2019 - Limited professional capacities and technical capabilities among various stakeholders Target: By the end of the project – Increased professional capacities and technical capabilities among various stakeholders within cybersecurity ecosystem.			

Sub-results per component (optional and indicative)	1.1 National competent authority/authorities (including CSIRT) designated and fully functional to take the role, tasks and responsibilities required by NIS Directive	- Availability of set of recommendations on the enhancement of the institutional-organisational structures and authorities (including CSIRT) according to NIS Directive. Baseline: Limited cybersecurity governance at strategic, operational and technical levels/competencies and responsibilities of different Georgian institutions insufficiently defined[23]. Target: By the end of the first half of the project – Set of recommendations prepared and agreed among beneficiaries. - Status of amendments to Georgian information security law and secondary legislation. Baseline: N/A Target: By the end of the project - Amendments drafted, agreed among relevant stakeholders and submitted for enactment to the parliament of Georgia / for approval to GoG. - Status of amendments to CSIRT(s) regulatory acts. Baseline: N/A Target: By the end of the project - Amendments drafted, agreed among relevant stakeholders and submitted for enactment to the Parliament of Georgia / for approval to GoG.	Legal and institutional analysis reports; Compatibility report of the legal act with NIS Directive; CSIRT(s) analysis report; Report on stakeholders' consultation; Project quarterly and final reports.	Difficulties in common institutional design agreed by stakeholders.	Readiness of the government to make institutional reforms in cybersecurity.

[23] 2019 Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre assesses Georgia with limited and insufficient definitions of competences and responsibilities of key governmental actors.

	1.2: National cybersecurity coordination framework created	- Availability of set of recommendations on defining authorities for different cyber incidents scenarios. Baseline: 2019 Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre. Target: By the end of the first half of the project – Recommendations elaborated and agreed among different stakeholders. - Status of legal or policy document(s) on coordinating authority roles and coordination scheme. Baseline: N/A Target: By the end of the project - Legal amendments/policy document(s) drafted, agreed among relevant stakeholders and submitted for enactment to the Parliament of Georgia / for approval to GoG.	Report on stakeholder's consultation on coordination authority roles and coordination scheme; Project documentation: Workshop reports, list of workshop participants, STE mission reports, recommendations. Project quarterly and final reports.	Stakeholders couldn't agree on coordination authority roles and coordination scheme.	Commitment from relevant decision makers side; High involvement of the stakeholders ensured.
	1.3: Public-private cooperation platform established	- Availability of memorandum of understanding (MoU)[24] for cybersecurity cooperation and collaboration between relevant public and private organisations. Baseline: N/A Target: By the end of the first half of the project – MoU is prepared, agreed and enacted by relevant public and private entities.	DEA official website; Report on stakeholder consultation; Project documentation (Minutes of the meetings, list of participants, recommendations,	Stakeholders couldn't find possible spheres for cooperation between public and private organisations.	High involvement of the representatives of the public and private organisations ensured.

[24] Memorandum of Understanding (MoU) will be accessible to any interested public and private entities for enrollment.

		- Number of cooperation actions between public and private stakeholders. Baseline: Limited cooperation on ad hoc basis. Sporadic involvement of private sector in development of cybersecurity frameworks[25]. Target: By the second half of the project – at least 3 joint cooperation actions implemented.	STE mission reports etc.) Memorandum of Understanding.		
	1.4 The third Georgian NCSS reviewed in the context of the requirements of the NIS Directive	Status of the assessment document comparing the existing NCSS with NIS requirements. Baseline: N/A Target: By the end of the first half of the project - Assessment of the third Georgian NCSS is performed.	Project documentation (list of workshop participants, workshop reports, materials, recommendations etc.); Report on consultation with stakeholders; Assessment document and recommendations.	Insufficient commitment from respective authorities	High level of involvement of the key stakeholders in the process; All relevant information and documentation available.
	2.1: Critical information infrastructures and operators of essential services identified and notified	- Status of the draft policy document on critical information infrastructures' identification methodology; Baseline: 2019 – Identification criteria is briefly enlisted in the law. Target: By the end of the project – Draft policy document on critical information infrastructures' identification methodology and questionnaire is elaborated and agreed	Document on criteria and methodology for identification of critical information infrastructures; Draft list of critical information infrastructures; Report on stakeholders’	Reluctance of the critical information infrastructures to participate in the process.	High involvement of the stakeholders ensured; Close cooperation between Twinning project partners.

[25] 2019 Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre assesses the current public-private cooperation as poor and sporadic.

		among all key stakeholders. - Availability of the draft list of critical information infrastructures; Baseline: 2019 – The list of critical information infrastructures (which covers only government sector) exists; Target: By the end of the project – critical information infrastructures list prepared for adoption by GoG, which covers private critical organisations. - Share of critical information infrastructures participating in communication/collaboration mechanisms/platforms. Baseline: 2019 – 10% of critical information infrastructures participating in ad hoc communication/collaboration activities. Target: By the end of the project – 60% of critical information infrastructures participating in formalized communication/collaboration mechanisms/platforms.	consultation; Workshop report demonstrating the notification process of the critical information infrastructures about the legal amendments and their responsibilities; Number of critical information infrastructures participating in the workshop;		
	2.2 Incident notification requirements and procedures defined	- Availability of parameters and thresholds for incident classification Baseline: N/A (There is no institutionalized procedures and established thresholds in place for the classification of cyber incidents[26]). Target: By the end of the first half of the project – Incident classification	Manuals, guidelines, templates and other implementing tools published on the official website of DEA; Report on stakeholder consultations;	Critical information infrastructures not sharing the information in cyber incidents.	All relevant documentation and information available; Sufficient communication between the beneficiary and other stakeholders;

[26] According to the 2019 Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre, there is no formalised procedures for cyber incidents' classification.

		parameters and thresholds elaborated.
		- Availability of incident notification templates and procedures.
		Baseline: N/A
		Target: By the end of the first half of the project - Incident notification requirements, templates and procedures elaborated
		- Availability of manuals/guidelines on incidents classification and reporting.
		Baseline: N/A
		Target: By the end of the first half of the project - Manuals/guidelines on incidents classification and reporting elaborated.
		- Status of cyber incident notification and information sharing platform.
		Baseline: Informal practices for information sharing and incidents reporting without guidance and clear procedures
		Target: By the end of the project - Cyber incident notification and information sharing platform established.
			Project documentation (Minutes of the meetings, workshop reports, materials, list of participants, recommendations, STE mission reports etc.)
			Internal statistics;
			National Cyber Security Index;
					Commitment of the Twinning project partners.

	2.3 Mandatory security requirements for critical information infrastructures and	- Status of set of recommendations on legal, organisational and technical mandatory measures for critical information infrastructures.	Project documentation (Minutes of the meetings, workshop reports, materials, list of participants,	Lack of commitment from respective actors and/or decision makers	High involvement of critical information infrastructures ensured; Sufficient involvement of relevant human

	operators of essential services defined	Baseline: 2019 Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre. Target: By the end of the first half of the project - Set of recommendations prepared and agreed among stakeholders. - Availability of the normative documents enlisting security rights/obligations for critical information infrastructures. Baseline: 2019 – normative documents available, however compliance with NIS Directive is limited. Target: By the end of the project – Normative documents enlisting security rights/obligations for critical infrastructures are in full compliance with NIS Directive.	recommendations, STE mission reports etc.) Reports on stakeholder consultations; Legislative Herald of Georgia, LEPL www.matsne.gov.ge; Number of critical information infrastructures that comply with mandatory security requirements.		resources; Strong support and proactive cooperation of Twinning partners ensured.

	2.4 Procedures for review and audit of security requirements for critical information infrastructures and operators of essential services defined	- Status of set of recommendations on review and audit requirements; Baseline: N/A Target: By the end of the first half of the project - Set of recommendations prepared and agreed among stakeholders. - Availability of legal document on cybersecurity review and audit of critical information infrastructures by competent authority; Baseline: 2019 – Limited compliance with NIS Directive. Target: By the end of the project – Legal document on cybersecurity review and audit of critical information infrastructures by competent authority is in full compliance with NIS Directive.	Report on consultation with stakeholders; Reviews and audit reports conducted by competent authority; Set of recommendations; Legal documents; Project quarterly and final reports.	Lack of commitment from respective authorities	
	3.1 Qualification requirements for cybersecurity professionals identified / skill pipeline developed	- Availability of gaps and needs analysis report. Baseline: 2019- Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre. Target: By the end of the first half of the project - Gaps and needs are analysed. - Availability of the capacity	Training needs assessments; Analysis report and recommendations; Report on consultation with stakeholders;	Lack of involvement of different stakeholders;	High level of involvement of the key stakeholders in the process All relevant information and documentation available. Close cooperation between Twinning

		needs analysis document. Baseline: N/A Target: By the end of the first half of the project - Capacity needs are analysed.			project partners.
	3.2 Cybersecurity capacity building activities performed	- Availability of the training plan; Baseline: N/A Target: By the end of the first half of the project - Training Plan developed and agreed among all key stakeholders. - Share of/number of trained and skilled cybersecurity specialists capable to perform new functions in accordance with NIS Directive; Baseline: Limited availability of qualified specialists[27]. Target: By the end of the project - at least 70% of eligible cybersecurity specialists trained. - Share of information security specialists capable to conduct review and information security audits in accordance with NIS Directive. Baseline: 2019 - 350 CISS information security managers and 100 CISS auditors trained in information security management and audit; 100 CISS middle and top management employees	Report on consultation with stakeholders. Project documentation: (list of training participants. Training materials, training report etc.). Training plan covering different aspects (Number of specialists trained and skilled in order to perform authorities under NIS Directive. Number of critical information infrastructure representatives trained in order to be compliant with new legal, operational and technical requirements based on NIS Directive.)	Low level of participation of cyber professionals.	Sufficient number of staff involved in the implementation process; Collaboration between all stakeholders ensured; Strong support and proactive cooperation of Twinning partners ensured.

[27] 2019 Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre indicates that trained professionals in cybersecurity are below the levels required for an agile information security posture.

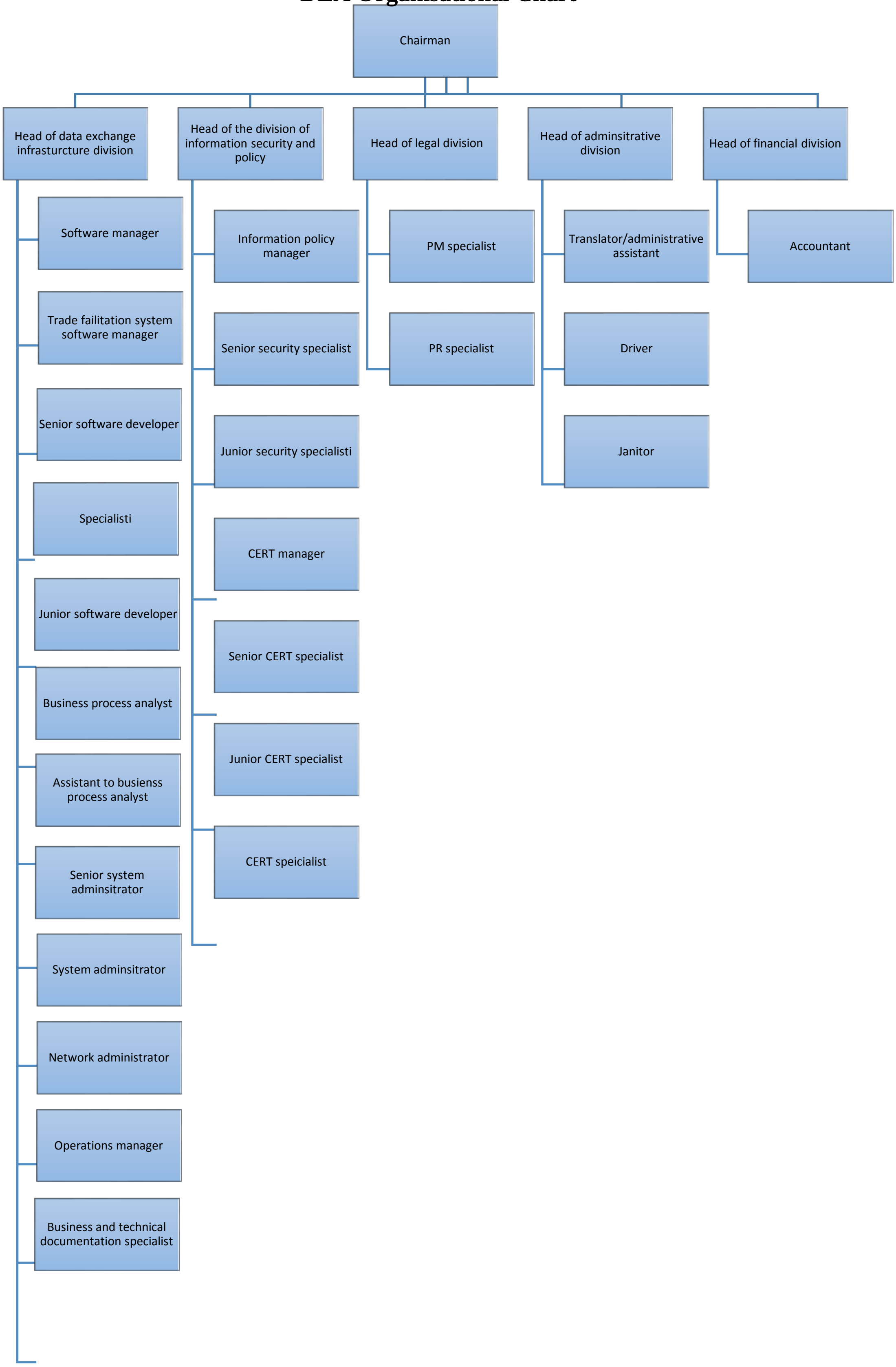
		trained in information security risk management; 50 CISS employees trained in basic incident handling. Target: By the end of the project at least 50% of designated information security specialists of critical information infrastructures are capable to conduct review and information security audits in accordance with NIS directive. - Share of critical information infrastructure representatives informed on new legal, operational and technical requirements based on NIS Directive. Baseline: 2019 - 350 CISS information security managers and 100 CISS auditors trained in information security management and audit; 100 CISS middle and top management employees trained in information security risk management; 50 CISS employees trained in basic incident handling. Target: By the end of the project - at least 70% of designated representatives of critical information infrastructure are informed on new legal, operational and technical requirements based on NIS Directive.			

	3.3 Strategy for building cyber awareness and education capacities within Georgia's information society elaborated	- Availability of the survey on the cyber awareness of Georgian information society. Baseline: 2019 - there is no National cybersecurity awareness rising program elaborated[28]. Target: By the end of the first half of the project – Survey on the cyber awareness is elaborated and shared among key stakeholders. - Status of the cyber awareness and education strategy. Baseline: 2019- there is no National cybersecurity awareness rising program elaborated. Target: By the end of the first half of the project - Strategy is drafted, agreed among relevant stakeholders and submitted for approval to GoG.	Project documentation: (workshop reports, List of workshop participants, workshop materials etc.); Survey(ies) report; Report on consultation with stakeholders; Strategy documents	Low level of participation of relevant target groups in Survey; Difficulty in reaching agreement among stakeholders of strategy directions. Delays during the project implementation process.	High involvement in survey on cyber awareness and education of the information society; Strong support and commitment to maintain project outcomes and recommendation ensured; Close cooperation of Twinning project partners.

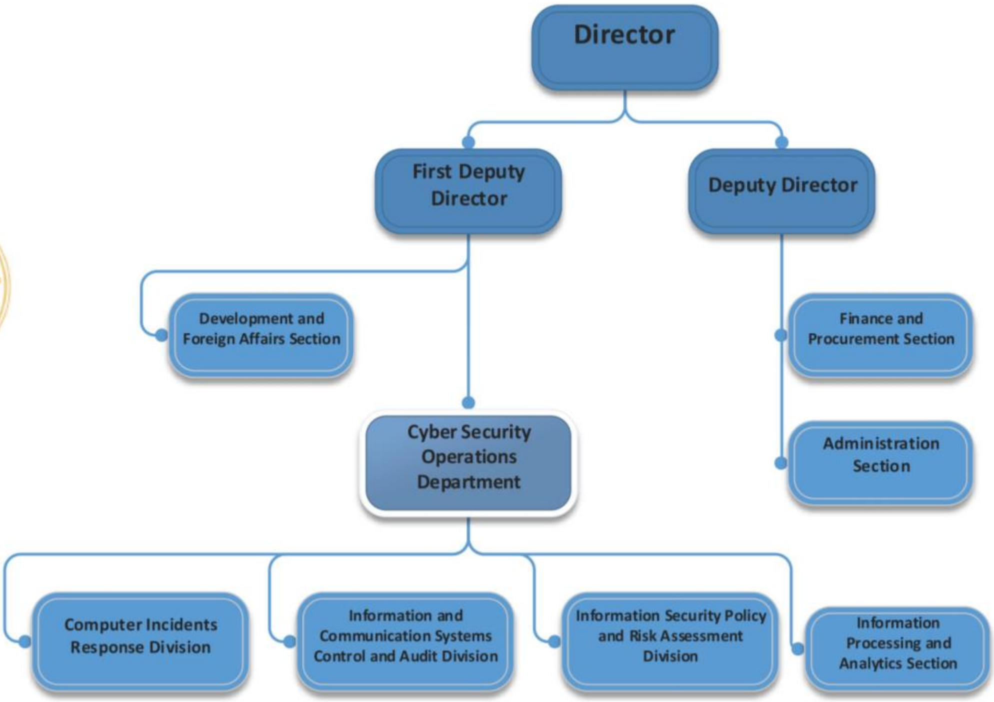
[28] According to 2019 Cybersecurity capacity review of Georgia by Global Cyber Security Capacity Centre, in Georgia there is no National cybersecurity awareness rising programme.

Annex 2

DEA Organisational Chart


Chairman
Head of data exchange infrasturcture division
Head of the division of information security and policy
Head of legal division
Head of adminsitrative division
Head of financial division
Software manager
Trade failitation system software manager
Senior software developer
Specialisti
Junior software developer
Business process analyst
Assistant to busienss process analyst
Senior system adminsitrator
System adminsitrator
Network administrator
Operations manager
Business and technical documentation specialist
Information policy manager
Senior security specialist
Junior security specialisti
CERT manager
Senior CERT specialist
Junior CERT specialist
CERT speicialist
PM specialist
PR specialist
Translator/administrative assistant
Driver
Janitor
Accountant

Annex 3 - CSB Organisational Chart



Director

First Deputy Director

Deputy Director

Development and Foreign Affairs Section

Finance and Procurement Section

Administration Section

Cyber Security Operations Department

Computer Incidents Response Division

Information and Communication Systems Control and Audit Division

Information Security Policy and Risk Assessment Division

Information Processing and Analytics Section