European Commission

ANNEX C1: Twinning Fiche

Project title: Support to Cybersecurity in Ukraine

Beneficiary administration: Ministry of Digital Transformation (MDT) and State Service of Special Communication and Information Protection (SSSCIP)

Twinning Reference: UA 19 ENI JH 01 21

Publication notice reference: EuropeAid/173152/DD/ACT/UA

EU funded project

TWINNING TOOL

List of Abbreviations:

BC - Beneficiary Country

CEC - Central Election Commission

CIIs - Critical Information Infrastructures

CIIP - Critical Information Infrastructure Protection

CERT-UA - Cyber Emergency Response Team of Ukraine

CFCU Central Finance and Contracting Unit

CMU – Cabinet of Ministers of Ukraine

CoE – Council of Europe

DDoS - Distributed-Denial-of-Service

ENI - European Neighbourhood Instrument

ENISA - European Cyber-security Agency

IcSP- EU Instrument contributing to Stability and Peace

ICT - Information and Communication Technology

I-DESI - International Digital Economy and Society Index

IT - Information Technology

ITU – International Telecommunications Union

KSZI - Complex information protection systems ("Kompleksni Systemy Zakhystu Zviazku")

LTE - Long Term Expert

NCSI - National Cyber Security Index

NIS Directive - EU Network and Information Security Directive

MDT, MDTU - Ministry of Digital Transformation

MTE - Mid Term Expert

MS, MS(s) – Member State, Member State(s)

NCCIR - National Commission for the State Regulation of Communications and Informatization[1]

NSDC - National Security and Defence Council

OECD – Organisation for Economic Cooperation and Development

PAO - Twinning Programme Administration Office

PL - Project Leader

PSC - Project Steering Committee

RTA - Resident Twinning Advisor

SIGMA - Support for Improvement in Governance and Management,

SSSCIP - State Service for Special Communications and Information Protection

STE - Short Term Experts

[1] As per website: https://nkrzi.gov.ua/index.php?r=site/index&pg=2&language=en).

1. Basic Information

1.1 Programme: Commission Implementing Decision C(2019) 3711 of 14.5.2019 on the Annual Action Programme part 1 in favour of Ukraine for year 2019

Technical Cooperation Facility 2019 (2019 / 041-718)

The action will be implemented in direct management.

***For UK applicants:** Please be aware that following the entry into force of the EU-UK Withdrawal Agreement[2] on 1 February 2020 and in particular Articles 127(6), 137 and 138, the references to natural or legal persons residing or established in a Member State of the European Union and to goods originating from an eligible country, as defined under Regulation (EU) No 236/2014[3] and Annex IV of the ACP-EU Partnership Agreement[4], are to be understood as including natural or legal persons residing or established in, and to goods originating from, the United Kingdom[5]. Those persons and goods are therefore eligible under this call.*

1.2 Twinning Sector: Justice and Home Affairs (JH)

1.3 EU funded budget: EUR 1,500,000

1.4 Sustainable Development Goals (SDGs): Goal 16 - "Peace and Justice and Strong Institutions"

2. Objectives

2.1 Overall Objective(s):

To increase the cyber security capacities of Ukraine by assisting the SSSCIP and MDT in aligning their operations with the EU and international standards.

2.2 Specific objectives:

- Ukrainian public authorities are better prepared to manage cyber security at strategic, operational and tactical levels.
- The cyber security legal framework, governance, guidelines and procedures in line with the EU legislation and good practices are developed.

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

[2] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community

[3] Regulation (EU) No 236/2014 of the European Parliament and of the Council of 11 March 2014 laying down common rules and procedures for the implementation of the Union's instruments for financing external action.

[4] Annex IV to the ACP-EU Partnership Agreement, as revised by Decision 1/2014 of the ACP-EU Council of Ministers (OJ L196/40, 3.7.2014)

[5] Including the Overseas Countries and Territories having special relations with the United Kingdom, as laid down in Part Four and Annex II of the TFEU.

This project is relevant for the Association Agreement under different headings: by its horizontal nature, Cybersecurity connects to Art.14, “Rule of Law and Respect for Human Rights and Fundamental Freedoms” of Title III (Justice, Freedom and Security) and to Art. 391, of Title V (Economic and Sector Cooperation), which refers to cooperation on Information Security.

Ukraine has adopted its new Cybersecurity Strategy on the basis of the Decision of the National Security and Defense Council of May 14, 2021 "On the Cyber Security Strategy of Ukraine". The new Strategy was approved by the Decree of the President of Ukraine dated August 26, 2021 № 447/2021.

The updated Cybersecurity Strategy of Ukraine was developed taking into account the practice of its implementation in the previous period (2016 - 2020), corresponds to the innovations of the Cyber Security Strategy for the Digital Decade and the EU Cyber Security Law, current challenges and trends in cyberspace threats.

The priorities and strategic goals of the new Strategy are the introduction of effective cyber defense, counteraction to intelligence and subversive activities in cyberspace and ensuring the security of digital services.

Moreover, based on a commitment taken at the 22nd EU-Ukraine Summit of 6 October 2020, an EU-Ukraine Cyber-Dialogue, was launched in June 2021.

In terms of policy, the EU adopted its Cybersecurity Strategy for the Digital Decade in December 2020. This also entails an external dimension, including the EU cybersecurity diplomacy toolbox, as well as the objective of ensuring EU’s role as standard setter in international governance of the cybersecurity domain.

The EU Network and Information Security Directive (hereinafter referred to as the ‘NIS Directive’) remains the benchmark regulation that Ukraine needs to approximate its legislation to, in terms of *acquis.*. In December 2020, the Commission adopted a proposal for a reviewed NIS framework (the so-called ‘NIS2 proposal’), building on the fundamentals of the NIS Directive, and which is now undergoing adoption procedure with co-legislators (European Parliament and Council).

3. Description

3.1 Background and justification:

Ukraine has been increasingly the target of cyberattacks in recent years, and especially following the Euromaidan Revolution. Cyberattacks have sought to undermine key infrastructures, like energy and banking services and inflict both physical and reputational damage on Ukraine. Attacks have also included the electoral process in the country.

On 21 May 2014, during the run up to the Presidential Elections a group of hackers knows as CyberBerkut compromised the Central Election Commission (CEC), disabling core CEC network nodes and numerous components of the election system. On 25 May – election day – 12 minutes before the polls closed, the attackers posted on the CEC website a picture of Ukrainian Right Sector leader Dmitry Yarosh, incorrectly claiming that he had won the election. This image was immediately picked up by some media, notably by Russian TV channels, feeding into social media propaganda and disinformation about the political situation in Ukraine.

In October 2014, on Saturday 25, on the eve of the Parliamentary elections, another cyberattack (via Distributed-Denial-of-Service) was aimed at the Central Electoral Commission, which reported a slowing down of its servers without further damages.

On 23 December 2015, a cyberattack targeted Ukraine power grids. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers; 30 substations were switched off, and about 230 thousand people were left without electricity for a period from 1 to 6 hours

On 27 June 2017, a major cyberattack – "Petya" from the name of the used ransomware - hit several state companies, critical infrastructures, and many banks in Kyiv, and quickly propagated to the rest of the country and to other countries. The attack was conducted through the use of a ransomware, a type of malicious software that blocks access to the victim's data or threatens to publish or delete it until a ransom is paid. The Petya ransomware appeared to be an upgraded of version of WannaCry, a virus previously used in another cyberattack that occurred in May 2017 and which affected some 200.000 devices.

The radiation monitoring system of the Chernobyl Nuclear Power Station was also hit, but monitoring activities continued through non-digital means. According to the National Bank of Ukraine, some 30 banks, including major ones such as Privatbank, Oschadbank, Ukrsotsbank, Ukrgasbank, OTP Bank, were targeted by the attack. According to the National Security and Defence Council (NSDC), state institutions that implemented the recommendations of the National Coordinating Center for Cyber Security were not infected by Petya.

The ongoing conflict in the East of the country, substantially fostered by Russia, is a multiplier of risks of cyberattacks, both at the tactical and strategic level: cyberattacks may happen locally, used as a means to inflict damage on Ukrainian infrastructures close to the contact line, and where successful they might create spill-over effects that would affect large populations (as in the sabotage of chemical plants). There is also a possibility that cyberattacks may be used in a strategic way, on a wider scale, especially in the case of a still possible escalation of the conflict in the East: in this scenario cyberattacks may play a much larger role and aim to destabilize the Ukrainian state as part of the hybrid war carried out by Russia.

Ukraine has prioritised digital transformation and aspires to harmonize its legal framework in this area with the EU. Cybersecurity is a vital domain as it ensures trust between partners. Ukrainian government has expressed interest to enhance the co-operation with the EU in order to increase cyber resilience of its critical civilian infrastructure and to exchange best practices between relevant EU and Ukrainian cyber entities. The EU’s particular added value comes through the experience of its Member States in countering cyber threats and interacting with different public and private institutions within the EU cybersecurity eco-system. This project would help build Ukraine’s capacities for cybersecurity, in complementarity with the other EU actions in this sector (E-Governance, Cybercrime projects etc).

The Ministry of Digital Transformation was established in September 2019. The mandate of the ministry includes strategic development of new digital policy, electronic services for people and business, cyber security and implementation of telecommunication legislation.

The SSSCIP – under the Ministry - according to Ukraine’s “Law on the Basic Principles of Cyber Security” adopted in 2017 , has the mandate to (1) ensure the design and implementation of the state cybersecurity policy; (2) protection of critical information infrastructure facilities; (3) coordination of the activities of other cyber security stakeholders; (4) undertaking organisational and technical measures on detection and response to cyber incidents and attacks as well as address of their consequences; (5) provision of information on cyber threats and recommendations on security measures.

Ukraine adopted a Law on the Fundamentals of Cybersecurity in Ukraine, which came into force in May 2018: with this law Ukraine has a legislative act that establishes a comprehensive governance system for ICT security. It defines key cybersecurity principles, objects of cybersecurity and defence, cybersecurity roles, responsibilities and tasks, principles for protections of Critical Information Infrastructures (CIIs) and guidance for international cooperation in the field of cybersecurity.

The Law on the Fundamentals of Cybersecurity in Ukraine vests major authorities for Critical Information Infrastructure Protection (CIIP) within the Cabinet of Ministers, which is mandated to make decisions on what to protect and how. However, Ukraine has not yet identified its critical infrastructure nor has adopted the criteria for the identification thereof, and many pieces of secondary legislation by the Cabinet of Ministers are at the various stages of drafting.

A Cyber Emergency Response Team (CERT-UA) has been established as part of SSSCIP and meets some of the requirements of the EU Network and Information Security Directives. It is capable of ensuring a high-level availability of its services, is tasked to monitor and respond to incidents at national level, provide dynamic risk and incident analysis and situational awareness, establish co-operation relationships with the private sector and has a possibility and participates in international co-operation frameworks. However, CERT-UA is not tasked with provision of early warnings, alerts, announcements and dissemination of information to relevant stakeholders and the level of co-operation with the private sector is low. Adding CIIs to its constituencies will constitute a significant additional load to CERT-UA, therefore additional human resources for incident monitoring, early warning, incident response and other services will be required. To be better prepared to play an active role in CIIP, CERT-UA needs to document and adopt incident and risk handling procedures based on the European Cyber-security Agency (ENISA) guidelines and recommendations and reference documents of the NIS (Network and Information Security) Co-operation Group.

3.2 Ongoing reforms:

The beneficiary agency is the State Security Service for Communication and Information Protection (SSSCIP). The mandate of the SSSCIP is defined in the Cabinet of Ministers of Ukraine regulations dated September 3, 2014 № 411 "On approval of the Regulations on the Administration of the State Service for Special Communications and Information Protection of Ukraine".

The main tasks of the State Service for Special Communications and Information Protection of Ukraine are:

- development and implementation of state policy in the areas of cryptographic and technical protection of information, cyber protection, telecommunications, use of radio frequency resource of Ukraine, special purpose postal service, government courier service, protection of state information resources and information, the requirement for protection of which is established by law, in information, telecommunication and information-telecommunication systems and on objects of information activity, as well as in the spheres of use of state information resources in terms of information protection, counteraction to technical intelligence, functioning, security and development of state government communication system, National system of confidential communication;

- participation in the development and implementation of state policy in the areas of electronic document management (in terms of information protection of state bodies and local governments), electronic identification (using electronic trust services), electronic trust services (in terms of setting security requirements and information protection during provision and use of electronic trust services, control over compliance with the requirements of the legislation in the field of electronic trust services);

- ensuring in the prescribed manner and within the competence of the activities of entities that directly carry out the fight against terrorism.

Program of regulatory work of SSSCIP is available online.

SSSCIP is currently undergoing a reform planned for 2020-2024 that is aimed to:

- Develop SSSCIP's approach to network and information system of key/critical entities protection with regard to modern risk-based approaches. One of the aims is the transition from current regulation of the integrated information security systems for electronic public services (including registers) into the information security management systems in compliance with international standards, and EU directives.
- Improve the capacities for formulation and implementation of public cybersecurity policies, increasing the security of public information resources and critical information infrastructure facilities and exercising greater public control in these areas. SSSCIP shall improve and develop an organizational and technical model of cybersecurity as part of the national cybersecurity system and reduce the likelihood of negative adversary influence on the public administration system.

3.3 Linked activities:

In 2018, with the financial support of the Konrad Adenauer Stiftung Office in Ukraine, Centre for Global Studies "Strategy XXI" carried out an assessment of the Ukraine – EU – NATO cooperation for in the cyber sphere including Ukrainian legislation in the field of cybersecurity.

In 2019, two EU funded projects (funded by IcSP and ENI) provided cybersecurity for the Presidential and Parliamentary elections, including crisis management and cyber-attack response training and simulation. In 2019, the EU funded project (implemented by Estonian Center for Eastern Partnership and CybExer Technologies OÜ) published a report entitled "POST-ELECTION ASSESSMENT OF THE CYBERSECURITY INFRASTRUCTURE AND INTERAGENCY COOPERATION IN UKRAINE WITH RELATED RECOMMENDATIONS".

The ongoing EU4DIGITAL CyberEast regional project aims to build cyber resilience in Eastern Partnership countries and is composed of two areas of work: cybercrime project "Action on Cybercrime for Cyber Resilience in the Eastern Partnership Region (CyberEast)", implemented by Council of Europe and cybersecurity project "EU4Digital: Cybersecurity East", implemented by GFA Consulting Group.

The EGOV4Ukraine project includes a decentralization component for building e-governance in the regions.

A Twinning with the Ukrainian Telecom Regulator has been launched on November 29 2019 to improve quality of service and market access in telecommunications in Ukraine and is relevant for the network standards and network security. The project involves a Consortium of Lithuanian and Latvian regulatory authorities in cooperation with the National Commission for the State Regulation of Communications and Informatization (NCCIR).

There are two ongoing EU funded projects that include some cyber actions, notably in the area of services: EU4Digital and EU4DigitalUA.

In 2020, USAID launched a 4-year project supporting Cybersecurity in Ukraine, the project will address 3 aspects: strengthen Ukraine's Cybersecurity enabling environment; develop Ukraine's cybersecurity workforce; build a resilient cybersecurity industry.

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

The **Network and Information Security (NIS) Directive**, ("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") is the relevant part of the EU acquis that Ukraine seeks to approximate to. A revision of the NIS Directive is forthcoming and the EU Commission has adopted a proposal for a revised Directive in December 2020.

3.5 Components and results per component

The project will have three components (component A will need to precede component B and C as these will build on the findings obtained by component A):

A. The regulatory legal framework, governance model, guidelines and procedures in the area of secure use of public data and resilient network and information systems analysed.

Subresults:

A.1 The current procedure for conducting state examination of complex information protection systems (also known as KSZI) reviewed; the regulatory legal framework of Ukraine reviewed, and the Ukrainian practice compared with the practices in selected (EU) countries.

A.2 The accreditation and/or certification procedures of the public sector information systems and IT systems of public enterprises managing critical services analyzed. The Ukrainian practice compared with practices in selected (EU) countries for implementation of minimum security measures for information systems (IT baseline security system). The analysis would also provide an overview of methodological approaches, country benchmarks and good EU practices in relation to the compliance with the risk based security requirements and reporting obligations- set out in the NIS Directive, including aspect relating to the capabilities and know-how for security incident response This analysis should also include an overview of good practices relating to supply chain security and use of policy tools such as coordinated vulnerability disclosure and provide corresponding recommendations tailor-made for the Ukrainian legal framework in this regard.

A.3 The current information security examination and authorization system (KSZI) analyzed with a view on how they addresses the needs of constantly changing IT environments and how they provide recommendations for more efficient approaches for the system owners i.e public authorities and critical service providers on these issues. An overview of good practices for adopting IT baseline security system in specific sectors in selected (EU) countries provided and on that basis potential changes to the current legal framework proposed.

B. An updated regulatory framework and IT security governance model prepared, the secure use of public sector data and resilient network and information systems ensured and the implementation strategy developed.

Subresults:

B.1 Draft/review of the updated regulatory framework and governance model ensuring the secure use of public sector data and resilient network and information systems based on the analysis conducted under Component A regarding the best practices for adopting IT baseline security system.

B.2 Pilots with the updated IT security framework in a number of public authorities or critical service providers (tentative number of three pilots). Pilot shall aim to put in practice the new components of the updated framework and helps to understand the needs of both counterparts – SSSCIP as the future examinator and the selected public authority as the implementer of updated cyber security requirements.

B.3 Based on the pilot experiences the drafts of necessary guidelines, sample documentation and recommendations on the basic tools for monitoring the security controls shall be provided. The guidelines shall help public authorities to assess their risks and to establish reasonable security objectives for every information system they own. As a result, the public authorities and critical service providers shall have necessary tools to implement IT security system i.e. establish, implement, operate, monitor and continuously maintain and improve an appropriate level of security of their network and information systems.

B.4 Training of trainers on conducting the updated regulatory framework and IT security governance model. Study the best practice in selected EU countries in preparing and/or accrediting IT auditors conducting the examination and authorisation procedures, organise workshops and other necessary formats to transfer knowledge to Ukraine.

C. Operational cyber security competencies enhanced and international cooperation of SSSCIP deepened.

C.1 Internal functions and organisation of SSSCIP reviewed with a purpose of formulating proposals for its improvement, taking into account cybersecurity reform in Ukraine and an updated regulatory framework and governance model developed under the Component B.

C.2 Support SSSCIP to strengthen their internal capacities for increasing transparency and publishing annual cyber security reports, as well as for the improvement and effective monitoring of information security of public authorities.

C.3 Support SSSCIP to increase cooperation between the Ukrainian and EU as well as selected EU Member States cyber security agencies and their networks, and possibly extending to ENISA and Europol.

C.4 Preparation of a consolidated report of all the necessary legal and institutional changes for the revision of the SSSCIP's tasks when conducting state examination of complex information protection systems in information, telecommunication and information-telecommunication systems and means of technical protection of information protection of information (the report will be handed over to MDT and serve as a basis for follow-up reform actions after the Twinning).

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

The EU MS Twinning partner(s) will provide a **Project Leader (PL)** and a **Resident Twinning Advisor (RTA).** The RTA is expected to be supported by **Component Leaders** who might be engaged as Mid Term Expert (MTE) or Long Term Expert (LTE). It is also required to secure a pool of **Short Term Experts (STE),** who will be called upon whenever necessary to contribute to the achievement of the mandatory results.

Short Term Experts will work together with the staff of the beneficiary institution under the overall direction of the beneficiary institution and the Project Implementation team. Besides providing the EU MS Twinning partner with adequate staff and other resources to operate effectively, the senior management of the beneficiary institution is expected to be involved in the development and implementation of policies and institutional change required to deliver the project results.

The Member State Project Leader (PL) is expected to be an official or assimilated agent with a sufficient rank to ensure an operational dialogue at political level. This should guarantee the capacity to lead the implementation of the project and the ability to mobilise the necessary expertise in support of its efficient implementation.

Involvement of the Member State PL(s) is expected during the preparation of the Member State proposal and attendance of the PL to the selection meeting is obligatory as well as the participation in quarterly meetings of the Project Steering Committee. Participation in some communication and visibility activities is expected.

The Member State PL is supported by the RTA, who works on-site with the Beneficiary administration.

3.6.1 Profile and tasks of the PL:

Qualifications and skills:

- Proven contractual relation to a public administration or mandated body (see Twinning Manual 4.1.4.2) responsible for cybersecurity with necessary public administration experience and with a sufficient rank to ensure an operational dialogue at political level;
- University degree in one of the following fields: law, public administration, computer/system/telecommunication engineering, computer science, economics or equivalent professional experience of 8 years in the sector of cybersecurity.
- .
- At least 3 years of specific experience in the area of public sector cybersecurity.
- Previous experience in project management will be considered as asset.
- Previous experience in international co-operation will be considered as asset.
- Fluent written and spoken English.

Experience as a team leader or project leader in minimum 1 but preferably 2 technical assistance or twinning projects would be considered as an asset.

<u>Tasks:</u>

- Conceive, supervise and coordinate the overall Twinning project.
- To provide strategic advice on high level regarding reforms supported by the Twinning.
- Coordinate and monitor the overall implementation of the project including coordination and direction of the MS TW partner.
- Co-ordinate MS experts' work and availability.
- Communicate with the beneficiary and EU Delegation.
- Ensure the backstopping functions and financial management.
- Guarantee from the MS administration side, the successful implementation of the project.
- Participate in quarterly meetings of the Project Steering Committee with the Beneficiary Country (BC) PL.
- Participate in preparation of the initial and subsequent work plans.
- Participate in preparation of both interim and final reports.

3.6.2 Profile and tasks of the RTA:

The relevant institution of MS will appoint a long-term Resident Twinning Advisor (RTA*)*.

<u>Qualifications and skills of the Resident Twinning Adviser</u>

- Proven contractual relation to a public administration or mandated body, in charge of cybersecurity sector.
- University degree in one of the following fields: law, public administration, computer/system/telecommunication engineering, computer science, economics or equivalent professional experience of 8 years in the cybersecurity sector.
- At least 3 years of general professional experience in public administration and project management in a public institutions context.
- Previous experience in training and mentoring in related areas will be considered as asset.
- Fluent written and spoken English.

Experience as a team leader or project leader in minimum 1 but preferably 2 technical assistance or twinning projects would be considered as an asset. Additional years of experience would be considered as an asset.

Tasks:

As to the general responsibility of the day-to-day implementation of the Twinning project in the Beneficiary Country, the Resident Twinning Adviser (RTA) tasks will include:

- Provide technical advice and assistance to the administration or other public sector bodies in the BC in the context of a predetermined work-plan;
- Coordination of all project activities and experts inputs in the BC;
- Ensuring day-to-day implementation of the Twinning project in the BC;
- Ensuring smooth correlation between the activities, deadlines and the envisaged results in the Work Plan;
- Preparation of the materials and documentation for regular monitoring and reporting;
- Preparation of side letters.
- Together with the Project Leader, to nominate, mobilize and supervise the Short-Term experts.

In addition to the above, an assistant and a full time translator-interpreter shall be appointed to assist the RTA. Allowance for this must be made within the project budget. Furthermore, the assistant and translator will facilitate the training activities. Where necessary (for example, during training activities, translation of project documents/reports and materials) the project will hire an additional translator with costs covered by the project.

3.6.3 Profile and tasks of Component Leaders*:*

Component Leaders will provide general guidance for the three Components of the project.

Qualifications and skills:

- University degree in one of the following fields: law, public administration, computer/system/telecommunication engineering, computer science, economics or equivalent professional experience of 8 years in cybersecurity.
- At least 3 years of experience in drafting of legislation or harmonization of external legislation with EU Network and Information acquis or cybersecurity governance reform in the public sector.
- Previous experience in training and mentoring in related areas will be considered as asset.
- Fluent written and spoken English.

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

STEs will provide specialised know-how for the individual tasks in the project.

- University degree in one of the following fields: law, public administration, computer/system/telecommunication engineering, computer science, economics or equivalent professional experience of 8 years in the sector of telecommunications / electronic communications.

- At least 3 years of experience in drafting of legislation or harmonization of external legislation with EU Network and Information acquis or cybersecurity governance reform in the public sector.
- Previous experience in training and mentoring in related areas will be considered as asset.
- Fluent written and spoken English.

4. Budget

The maximum budget available for this Grant is EUR 1.500.000

5. Implementation Arrangements

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

The Delegation of the European Union to Ukraine will manage the procurement, tendering, quality control, reporting and coordination with other donors, the financial and technical cooperation related to the actions described in this project fiche, taking remedial actions if and when needed.

The person in charge at the EU Delegation to Ukraine:

Mr Sergiy Ladnyy
Project Manager
EU Delegation to Ukraine
101, Volodymyrska street,
Kyiv, Ukraine, 01033
Tel.: +38 044 390 80 10
e-mail: Sergiy.LADNYY@eeas.europa.eu

The person in charge at the PAO in Ukraine:

Yuliia Yerchenko
Head of Unit of Twinning Programme Administration Office Activities Ensuring Twinning Coordination Division
Twinning Programme Administration Office (PAO)
15, Prorizna Street., Kyiv, 01601, Ukraine
Tel: +38 044 278 36 44
E-mail: yuliia.yerchenko@center.gov.ua

5.2 Institutional framework

The State Service of Special Communication and Information Protection, and within it the Cyber Emergency Response Team (add legal basis for the SSSCIP, constitutive act).

5.3 Counterparts in the Beneficiary administration:

The Project Leader (PL) and Regional Twinning Advisor (RTA) counterparts will be staff of the Beneficiary administration and will be actively involved in the management and coordination of the project.

5.3.1 Contact person:

Dmytro Makovskyi

First Deputy Chairman of the State Service of Special Communications and Information Protection of Ukraine,

Postal address: 03110, Kyiv, Ukraine, 03110, Solomianska 13 str.

E-mail: info@dsszzi.gov.ua

5.3.2 PL counterpart

Specify the name, official position and postal address of its institution, (no contact details of the person)

Yuliya Volkova

Head of the European Integration and International Cooperation Department of the State Service of Special Communications and Information Protection of Ukraine

5.3.3 RTA counterpart

Specify the name, official position and postal address of its institution, (no contact details of the person).

Yuliya Volkova

Head of the European Integration and International Cooperation Department of the State Service of Special Communications and Information Protection of Ukraine

6. Duration of the project

The project's implementation period is 21 months. The legal duration of the project is 24 months

7. Management and reporting

7.1 Language

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

7.2 Project Steering Committee

A project steering committee (PSC) shall oversee the implementation of the project. The main duties of the PSC include verification of the progress and achievements via-à-vis the mandatory results/outputs chain (from mandatory results/outputs per component to impact), ensuring good coordination among the actors, finalising the interim reports and discuss the updated work plan. Other details concerning the establishment and functioning of the PSC are described in the Twinning Manual.

7.3 Reporting

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

8. Sustainability

The twinning partners will undertake to provide the basic infrastructure necessary for the sustainability of their joint twinning achievements. The sustainability of the results is likely to be achieved if the twinning partners commit themselves to the following:

- absorbing efficiently the contents and understanding of the training materials by the Beneficiary personnel being measured and monitored after each training session that is provided by simple tests;
- making maximum use of the skills and abilities of the beneficiary country administration personnel previously trained by [other] Member States; apply "train the trainers approach" for sustainable capacity building of the beneficiary administration;
- allowing for confirmation of the effect of the twinning project for the beneficiary administration by organising a final seminar that presents achieved results of the twinning activities at the end of the twinning project;
- providing assurance that manuals and procedures developed within the twinning project will be used by the beneficiary beyond the primary contract period.

The success of the project will be based on achieving practical results and the sustainability of the results will be an important measure of success.

9. Crosscutting issues

All activities under this project will be designed and implemented in accordance with principles of good governance, human rights based approach, gender equality and environmental sustainability. Support to mainstreaming gender issues into the legislative processes under the activities for the implementation of Association Agreement will be provided. All activities will ensure the respect to key Principles of Public Administration, especially the commitment to inclusive and evidence-based policy and legislative development.

This action will be implemented following a rights-based approach, encompassing all human rights. The five working principles below will be applied at all stages of implementation: legality, universality and indivisibility of human rights; participation and access to the decision-making process; non-discrimination and equal access; accountability and access to the rule of law; transparency and access to information.

By promoting an institutional culture of openness, accountability and transparency, the project will positively impact on the credibility and integrity of concerned Government Departments and Agencies. The project will strive to act as an example of positive administrative reform.

10. Conditionality and sequencing

The underlying assumption for this project is the Ukrainian political will to create an efficient and reformed governance of cybersecurity in the country, which will aim for approximation and cooperation with the European Union.

Projects to be implemented through Twinning require the full commitment and participation of the senior management of the beneficiary institution. In addition, to provide the Twinning partner with adequate resources to operate effectively, the senior management must be fully involved in the development and implementation of the policies required to deliver the desirable results.

11. Indicators for performance measurement

Definition of project specific, realistic, verifiable targets and indicators complementing point 10. Please list the indicators by components, in line with the mandatory results/sub-results enumerated under 3.5 and the Annex C1a Simplified Logical framework.

	Project specific, realistic, verifiable targets and indicators
Overall	
Increasing cyber security capacities of Ukraine by assisting MDT and SSSCIP in aligning their operations with the EU and international standards.	Status of the cybersecurity capacity of Ukraine, baseline - 2021
Project specific	
• Ukrainian public authorities are better prepared to manage cyber security at strategic, operational and tactical levels. • The cyber security legal framework, governance, guidelines and procedures in line with the EU legislation and good practice are developed.	
Component A:	
Analysis of the regulatory legal framework, governance model, guidelines and procedures ensuring the secure use of public sector data and resilient network and information systems.	Target: “proposal for an improved/updated/in line with EU standards regulatory legal framework drafted and agreed among relevant actors” Indicator:_Status of the regulatory legal framework ensuring the secure use of public sector data and resilient network and information systems. Baseline: “limited/weak regulatory legal framework”
Sub-result A.1: The current procedure for conducting state examination of complex information protection systems (also known as KSZI) reviewed; the regulatory legal framework of Ukraine reviewed, and	Target A.1: A proposal to review the current procedure for conducting state examination of complex information protection systems in information, telecommunication and information-

the Ukrainian practice compared with the practices in selected (EU) countries.	telecommunication systems and means of technical protection of information protection of information (also known as KSZI) prepared by the project, submitted to SSSCIP, reviewed by SSSCIP and approved. Indicator A.1:_Status of the regulatory legal framework on the information security examination and authorization system (KSZI)
Sub-result A.2: The accreditation and/or certification procedures of the public sector information systems and IT systems of public enterprises managing critical services analyzed. The Ukrainian practice compared with practices in selected (EU) countries for implementation of minimum security measures for information systems (IT baseline security system).	A proposal to review the accreditation and/or certification procedures of the public sector information systems and IT systems of public enterprises managing critical services prepared by the project, submitted to SSSCIP and approved by SSSCIP. A review of the regulatory legal framework of Ukraine, and comparison of the Ukrainian practice with the practices in selected (EU) countries prepared by the project and adopted by SSSCIP.
Sub-result A.3: The current information security examination and authorization system (KSZI) analyzed with a view on how they addresses the needs of constantly changing IT environments and how they provide recommendations for more efficient approaches for the system owners i.e public authorities and critical service providers on these issues. An overview of good practices for adopting IT baseline security system in specific sectors in selected (EU) countries provided and on that basis potential changes to the current legal framework proposed.	A proposal to amend the current legal framework on the information security examination and authorization system (KSZI) prepared by the project, submitted to SSSCIP and approved/reviewed by SSSCIP.
Component B:	
Preparation of an updated regulatory framework and IT security governance model ensuring the secure use of public sector data and resilient network and information systems; development of the implementation strategy. Sub-result B.1: Draft of the updated regulatory framework and governance model ensuring the secure use of public sector data and resilient network and information systems is developed based on the analysis conducted under Component A on the best practices for adopting IT baseline security system.	Indicator B: Proposal for a regulation on the governance model for secure use of public sector data and resilient network and information systems, based on the analysis conducted under Component A about the best practices for adopting IT baseline security system prepared by the project, submitted to SSSCIP, reviewed and

Sub-result B.2: Pilots with the updated IT security framework in a number of public authorities or critical service providers (tentative number of three pilots) shall be carried out. Pilot shall aim to put in practice the new components of the updated framework and helps to understand the needs of both counterparts – SSSCIP as the future examinator and the selected public authority as the implementer of updated cyber security requirements. Sub-result B.3: Based on the pilot experiences the drafts of necessary guidelines, sample documentation and recommendations on the basic tools for monitoring the security controls shall be provided. The guidelines shall help public authorities to assess their risks and to establish reasonable security objectives for every information system they own. As a result, the public authorities and critical service providers shall have necessary tools to implement IT security system i.e. establish, implement, operate, monitor and continuously maintain and improve an appropriate level of security of their information network and information systems. Sub-result B.4: Training of trainers on the updated regulatory framework and IT security governance model conducted. The best practice studied in selected EU countries for preparing and/or accrediting IT auditors conducting the examination and authorisation procedures, workshops and other necessary formats to transfer knowledge to Ukraine organised.	submitted by SSSCIP to MDTU and CMU for adoption. Pilots with the updated IT security framework in public authorities or critical service provider. Indicator B.2: number of pilots carried out Indicator B.3: set of drafts guidelines, sample documentation and recommendations on the basic tools to implement IT security system and for monitoring the security controls prepared by the project, submitted to SSSCIP and adopted. Training of trainers carried out on conducting the new updated regulatory framework and IT security governance model. Indicator B.4: number of trainers trained.
Component C:	
Enhancement of the operational cyber security competencies and deepening of international cooperation of SSSCIP Sub-result C.1: Internal functions and organisation of SSSCIP reviewed with a purpose of formulating proposals for its improvement, taking into account cybersecurity reform in Ukraine and an updated regulatory framework and governance model developed under the Component B.	Proposal for a regulation on the governance model for secure use of public sector data and resilient network and information systems, based on the analysis conducted under Component A. Draft guidelines, sample documentation and recommendations on the basic tools for monitoring the security controls. Proposal for legislative changes necessary for the revision of the SSSCIP's tasks when conducting state examination of complex information protection systems in information, telecommunication and information-telecommunication systems and means

	of technical protection of information protection of information.

12. Facilities available

The following facilities will be made available for hosting the RTA and his/her assistants: office space, access to meeting rooms, hard and software, facilities available for training, seminars, conferences.

ANNEXES TO PROJECT FICHE

1. The Simplified Logical framework matrix as per Annex C1a (compulsory)
2. List of relevant Laws and Regulations (optional)
3. Reference to relevant Government Strategic plans and studies (may include Institution Development Plan, Business plans, Sector studies etc.) (optional)
4. Existing donor coordination framework (if existing)
5. Sector assessment reports of any kind including publically available reports from other International organisations (SIGMA, IMF, etc.)
6. Project/sector relevant publically available Conclusions/agreements between EU and the Beneficiary resulting from the political dialogue

Annex C1a : Simplified Logical Framework (to be reviewed)

	Description	Indicators (with relevant baseline and target data)	Sources of verification	Risks	Assumptions (external to project)
Overall Objective	*Increasing cyber security capacities of Ukraine by assisting the SSSCIP in aligning its operations with the EU and international standards.*	*Status of the cybersecurity capacity of Ukraine, baseline - 2021*	International cybersecurity rankings of Ukraine, such as ITU's Global Cybersecurity Index, The International Digital Economy and Society Index(I-DESI), the National Cyber Security Index (NCSI) measured by the Estonian e-governance Academy, ENISA assessments. Conclusions of the EU-Ukraine cybersecurity dialogue.	Underestimation of importance of cybersecurity in the context of overall political situation. Growing global cybersecurity threats may exceed the capacity of Ukraine to deal with them.	The Ukrainian political will to create an efficient and reformed governance of cybersecurity in the country, which will aim for approximation and cooperation with the European Union. The EU and Ukraine remain committed to continue cybersecurity dialogue.

Specific (Project) Objective(s)	1. *Ukrainian public authorities better prepared to manage cyber security at strategic, operational and tactical levels.* 2. *The cyber security legal framework, governance, guidelines and procedures in line with the EU Regulations and best practice developed.*	- *Status of the regulatory legal framework ensuring the secure use of public sector data and resilient network and information systems. Baseline: “limited/weak regulatory legal framework”* - *Strengthening the strategic and operational capacity of the SSSCIP;* - *Delivery of know-how and best EU practices.*	- Project reports with relevant analysis and recommendations; - Drafts of primary/secondary legislation, rules and procedures. Quality measurement system - Training or workshops materials. - No of staff trained.	- Changes in beneficiary government (SSSCIP) priorities. - Low pace of the adoption of the proposed improvements to the cyber security legal framework, governance, guidelines and procedures.	Institutional capacity of SSSCIP is sufficient to accept Twinning assistance. SSSCIP remain committed to the project. Parliament, CMU, MDTU and SSSCIP adopt respectively the proposed improvements to the cyber security legal framework, governance, guidelines and procedures.

Mandatory results/outputs by components: **Component A result/output:** **The regulatory legal framework, governance model, guidelines and procedures in the area of the secure use of public sector data and information systems analysed.**	***Component A mandatory subresults:*** *A.1 Review of the current procedure for conducting state examination of complex information protection systems in information, telecommunication and information-telecommunication systems and means of technical protection of information protection of information (also known as KSZI).* *A.2 Review of the regulatory legal framework of Ukraine, and comparison of the Ukrainian practice with the practices in selected (EU) countries.* *A.3 Analysis of the accreditation and/or certification procedures of the public sector information systems and IT systems of public enterprises managing critical services. Comparison of the Ukrainian practice with the practices in selected (EU) countries when enforcing standards developed for implementation of minimum security measures for information systems (IT baseline security system). The analysis would also provide overview of methodological approaches, country benchmarks and best EU practices on NIS directive requirements about the security*	- Status of the regulatory legal framework on the information security examination and authorization system (KSZI) - A proposal to amend the current legal framework on the information security examination and authorization system (KSZI) prepared by the project, submitted to SSSCIP and approved/reviewed by SSSCIP. - Review of the regulatory legal framework of Ukraine, and comparison of the Ukrainian practice with the practices in selected (EU) countries prepared by the project, submitted to SSSCIP and approved/reviewed by SSSCIP. - Analysis of the accreditation and/or certification procedures of the public sector information systems	- Project reports with relevant analysis and recommendations. - SSSCIP, MDTU and CMU websites.	Insufficient dedication, motivation, resources of SSSCIP to implement the project.	Insufficient cooperation between SSSCIP and other stakeholders.

	incident response and on the implementation of technical and operational security measures based on risk.	and IT systems of public enterprises managing critical services prepared, submitted to SSSCIP and approved/reviewed by SSSCIP.			

Component B result/output: An updated regulatory framework and IT security governance model prepared; the secure use of public sector data and resilient network and information systems ensured and the implementation strategy developed.	*Component B mandatory Results:* *B1. Draft/review of the updated regulatory framework and governance model ensuring the secure use of public sector data and information systems that is developed based on the analysis conducted under Component 1 about the best practices for adopting IT baseline security system.* *B2. Pilots with the updated IT security framework in public authorities or critical service providers. Pilots shall aim to put in practice the new components of the updated framework and helps to understand the needs of both counterparts – SSSCIP as the future examinator and the selected public authority as the implementer of updated cyber security requirements.* *B3. Based on the pilot experience the drafts of necessary guidelines, sample documentation and recommendations on the basic tools for monitoring the security controls shall be provided. The guidelines shall help public authorities to assess their risks and to establish reasonable security objectives for every information system they own. As a result, the public authorities and critical service*	- Proposal for a regulation on the governance model for secure use of public sector data and resilient network and information systems, based on the analysis conducted under Component A about the best practices for adopting IT baseline security system prepared by the project, submitted to SSSCIP, reviewed and submitted by SSSCIP to MDTU and CMU for adoption. - Number of pilots carried out. - Set of drafts guidelines, sample documentation and recommendations on the basic tools to implement IT security system and for monitoring the security controls prepared by the project, submitted to SSSCIP and adopted. - Number of trainers trained on conducting the new the updated	- Project reports with relevant analysis and recommendations; - Drafts of primary/secondary legislation, rules and procedures; - SSSCIP, MDTU and CMU websites - Quality measurement system - Training or workshops materials.	- Insufficient dedication, motivation, resources of SSSCIP to implement the project. -	Insufficient cooperation between SSSCIP and other stakeholders.

	providers shall have necessary tools to implement IT security system ie establish, implement, operate, monitor and continuously maintain and improve an appropriate level of security of their information systems. *B4. Training of trainers on conducting the new the updated regulatory framework and IT security governance model. Study the best practice in selected EU countries in preparing and/or accrediting IT auditors conducting the examination and authorisation procedures, organise workshops and other necessary formats to transfer knowledge to Ukraine.*	regulatory framework and IT security governance model.			

Component C result/output. Operational cyber security competencies enhanced and international cooperation of SSSCIP deepened	*Component C mandatory results:* *C1. Support SSSCIP to increase international cooperation between the Ukrainian and EU, as well as selected EU Member States cyber security agencies and their networks.* *C2. Support SSSCIP to strengthen their internal capacities for increasing transparency and publishing annual cyber security reports, as well as for the improvement and effective monitoring of information security of public authorities.* *C3. A review of the internal functions and organisation of SSSCIP in view of formulating proposals for its improvement, while taking into account cybersecurity reform in Ukraine and an updated regulatory framework and governance model developed under the Component B.* *C4. Preparation of the report of all the necessary legal and institutional changes for the revision of the SSSCIP's tasks when conducting state examination of complex information protection systems in information, telecommunication and information-telecommunication systems and means of technical*	- Efficiency of operations improved; - SSSCIP and their Ukrainian partners increased international cooperation with the EU, as well as selected EU Member States cyber security agencies and their networks - Review of the internal functions and organisation of SSSCIP prepared - Staff trained	- Project reports with relevant analysis and recommendations; - Drafts of primary/secondary legislation, rules and procedures; - Number of staff trained - Quality measurement system - Self-assessment surveys of staff	Insufficient dedication, motivation, resources of SSSCIP to implement the project.	Insufficient cooperation between SSSCIP and other stakeholders.

	protection of information protection of information.				

Annex 2. List of relevant Laws and Regulations (optional)

1. Decree of the President of Ukraine dated August 26, 2021 № 447/2021 On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cyber Security Strategy of Ukraine" (https://www.president.gov.ua/documents/4472021-40013)
2. New draft Strategy of Cybersecurity of Ukraine 2021-2025 (https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf , being translated into EN)
3. CABINET OF MINISTERS OF UKRAINE RESOLUTION dated September 3, 2014 № 411 "On approval of the Regulations on the Administration of the State Service for Special Communications and Information Protection of Ukraine" (https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF/conv#Text, no official translation available, https://translate.google.com/translate?sl=uk&tl=en&u=https://zakon.rada.gov.ua/laws/show/411-2014-%25D0%25BF/conv%23Text)
4. Program of regulatory work of SSSCIP is available online: https://cip.gov.ua/ua/news/zmini-9
5. The concept of reforming the SSSCIP by 2024 https://cip.gov.ua/ua/news/derzhspeczv-yazku-optimizuye-svoyu-strukturu-pozbudetsya-nevlastivikh-yii-funkcii-ta-posilit-kiberzakhist-ob-yektiv-kritichnoyi-infrastrukturi Law on the Fundamentals of Cybersecurity in Ukraine https://zakon.rada.gov.ua/laws/show/2163-19#Text

Annex 3. Reference to relevant Government Strategic plans and studies (may include Institution Development Plan, Business plans, Sector studies etc.) (optional)

The MDTU presented their draft "Mid-Term Action Plan of the Government of Ukraine for the years 2021-2023 within the competence of MDTU" to donors in February 2021. Its international cooperation activity has a Subproject 7 "National Cyber Resilience System".

The update of the draft plan can be requested from the MDTU or downloaded from here:
https://docs.google.com/spreadsheets/d/1RrvrARxGn0zLbgcPU5NXYgmd26jPHBz5-mtQHsfguWg/edit#gid=1350816258

Annex 4. Existing donor coordination framework (if existing)

Ministry of Digital Transformation of Ukraine (MDTU) has established a Sub-group on Digital Infrastructure, Digital Economy, Development of IT Business, Cybersecurity, as a part of overall government led donor coordination Sector Working Group on Digital Transformation.

The MDTU has elaborated together with donors the joint working plan; it includes the Subproject 7 “National Cyber Resilience System”:

https://docs.google.com/spreadsheets/d/1RrvrARxGn0zLbgcPU5NXYgmd26jPHBz5-mtQHsfguWg/edit#gid=1350816258

Annex 5. Sector assessment reports of any kind including publically available reports from other International organisations (SIGMA, IMF, etc.)

1. In 2018, with the financial support of the Konrad Adenauer Stiftung Office in Ukraine, the Centre for Global Studies “Strategy XXI”carried out an assessment of the Ukrainian legislation in the field of cybersecurity with reference to its harmonization with the EU Network and Information Security.

http://www.encouncil.org/wp-content/uploads/2019/10/ENG-Ukraine-EU-NATO-cooperation-to-counter-hybrid-threats-in-cyber-sphere.pdf

2. In 2019, two EU funded projects (funded by IcSP and ENI) provided cybersecurity for the Presidential and Parliamentary elections, including crisis management and cyber-attack response training and simulation.

https://icspmap.eu/pdf/?format=single&contract_number=405088

3. In 2019, the EU funded project (implemented by Estonian Center for Eastern Partnership and CybExer Technologies OÜ) published a report entitled “POST-ELECTION ASSESSMENT OF THE CYBERSECURITY INFRASTRUCTURE AND INTERAGENCY COOPERATION IN UKRAINE WITH RELATED RECOMMENDATIONS”.

https://eceap.eu/wp-content/uploads/2019/11/Post-Election-Assessment-RecommendationsFINAL.pdf

4. “Cybercrime and cybersecurity strategies in the Eastern Partnership region” updated report 2018:

https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c

5. International Telecommunications Union (ITU) Global Cybersecurity Index

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

6. The International Digital Economy and Society Index (I-DESI)

https://digital-strategy.ec.europa.eu/en/policies/desi

7. The National Cyber Security Index (NCSI) measured by the Estonian e-governance Academy https://ncsi.ega.ee/country/ua/

Annex 6. Project/sector relevant publically available Conclusions/agreements between EU and the Beneficiary resulting from the political dialogue

The EU-Ukraine first cybersecurity dialogue meeting took place on June 3, 2021.

https://eeas.europa.eu/headquarters/headquarters-homepage/99530/cyberspace-eu-and-ukraine-launch-dialogue-cyber-security_en