EN

THIS ACTION IS FUNDED BY THE EUROPEAN UNION

ANNEX 3 ADDING ANNEX 18

to the Commission Implementing Decision amending "Implementing Decision C(2021) 9716 final adopting a financing of the multi-country multiannual action plan in favour of the Western Balkans and Turkey for 2021-2022"

Action Document for "EU Support to Cybersecurity Capacity Building in the Western Balkans - 2022"

MULTIANNUAL ACTION PLAN

This document constitutes the multiannual work programme in the sense of Article 110(2) of the Financial Regulation, and annual and multiannual action plans and measures in the sense of Article 9 of IPA III Regulation and Article 23 of NDICI - Global Europe Regulation.

1. SYNOPSIS

1.1. Action Summary Table

Title	**EU Support to Cybersecurity Capacity Building in the Western Balkans – 2022** "Multi-country multiannual action plan in favour of the Western Balkans and Turkey for 2021-2022"
OPSYS	OPSYS Action: ACT-61445 ABAC commitment level 1: JAD.973007 (allocation 2022)
Basic Act	Financed under the Instrument for Pre-accession Assistance (IPA III)
Team Europe Initiative	No
Zone benefiting from the action	Western Balkans (Republic of Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, Republic of North Macedonia, and Republic of Serbia)
Programming document	IPA III Programming Framework
PRIORITY AREAS AND SECTOR INFORMATION	
Window and thematic priority	Window 1 – Rule of Law, Fundamental Rights and Democracy Thematic priority: 3 - Fight against organised crime / security

Sustainable Development Goals (SDGs)	Main SDG: 16: Peace, Justice and Strong Institutions			
DAC code(s)	15210 - Security system management and reform – 100%			
Main Delivery Channel @	Third Country Government (Delegated co-operation) - 13000			
Markers (from DAC form)	**General policy objective** @	**Not targeted**	**Significant objective**	**Principal objective**
	Participation development/good governance	☐	☐	☒
	Aid to environment	☒	☐	☐
	Gender equality and women's and girl's empowerment	☒	☐	☐
	Trade development	☒	☐	☐
	Reproductive, maternal, new-born and child health	☒	☐	☐
	Disaster Risk Reduction	☒	☐	☐
	Inclusion of persons with Disabilities	☒	☐	☐
	Nutrition	☒	☐	☐
	RIO Convention markers @	**Not targeted**	**Significant objective**	**Principal objective**
	Biological diversity	☒	☐	☐
	Combat desertification	☒	☐	☐
	Climate change mitigation	☒	☐	☐
	Climate change adaptation	☒	☐	☐
Internal markers	**Policy objectives**	**Not targeted**	**Significant objective**	**Principal objective**
	Connectivity	☒	☐	☐
	Digitalisation	☐	☒	☐
	Migration	☒	☐	☐
	Covid-19	☒	☐	☐
BUDGET INFORMATION				
Amounts concerned	Budget line: 15.020101.01 Total estimated cost: EUR 5 000 000 Total amount of EU budget contribution EUR 5 000 000			
MANAGEMENT AND IMPLEMENTATION				
Implementation modalities (type of	Project Modality			

financing and management mode)	**Indirect management** with the entity(ies) to be selected in accordance with the criteria set out in section 4.3.1
Relevant priorities and flagships from Economic and Investment Plan for the Western Balkans	Priorities: "Digital Transition", "Governance, Rule of Law, PAR" – not in financial terms
Final date for concluding contribution / delegation agreements, procurement and grant contracts	Allocation 2022 - At the latest by 31 December 2023
Indicative operational implementation period	72 months following the adoption of this amending Financing Decision

1.2. Summary of the Action

The EU is committed to support increased resilience of the Western Balkans to cyber threats as a strategic geopolitical investment including in view of the European perspective of the region. An investment in the region's cyber resilience and support to EU alignment is key to ensure the stability of IPA III beneficiaries and ensure trustworthy and reliable services and digital tools for citizens and businesses.

The global cyber threat landscape has further been aggravated by Russia's war of aggression against Ukraine, with direct impacts for the EU and its neighbours. The cyber threats arising from the war underline the need to boost sharing of information and expertise between the EU and the Western Balkans and across cybersecurity communities, including in view of hybrid threats.

The overall objective of this action is to enhance cyber resilience of the Western Balkans through regional cooperation and specific, beneficiary-targeted capacity building activities. Cybersecurity capacity building is identified as a priority in the IPA III Programming Framework Window 1 Thematic Priority 3. Direct institutional and operational gaps in cyber prevention, preparedness and response will be targeted. The action will facilitate EU engagement on cybersecurity with the region. The EU's approach to cybersecurity capacity building in the Western Balkans uses a right-based and whole-of-government approach to strengthen prevention, preparedness, and resilience to cyber threats with a strong focus on institution-building.

The action is developed in support of the Enlargement strategy[1] and complements foreseen EU crisis response support to Albania, Montenegro and North Macedonia as well as on-going support to cybercrime capacity. The action is designed in response to a cybersecurity capacity building needs exercise conducted in 2022 in the Western Balkans IPA III beneficiaries.

[1] An Economic and Investment Plan for the Western Balkans .COM (2020) 641 final. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52020DC0641

2. RATIONALE

2.1. Context

Russia's war of aggression against Ukraine dominates the EU's current security agenda. The war threatens not only Ukraine's sovereignty and territorial integrity but also the entire global stability and security. Both inside the EU and in its neighbourhood, the Russian aggression brings a range of risks to the security of citizens. Next to new uncertainties over supplies of energy and raw materials and the risk of critical information infrastructure (CII) being targeted in cyberattacks, other acute risk factors require attention in parallel. European safety and security are jeopardised by potential attacks or accidents resulting from chemical, biological, radiological or chemical agents in the war zone, and the vulnerabilities of millions of people who have fled the war can be quickly exploited by organised crime, through the trafficking of women and children, who are particularly at risk.

The digital transformation is a key driver for economic growth and societal change including in the Western Balkans. In the context of the growing dependency of economies and societies on digital technologies, the overall global cyber threat landscape continues to aggravate. Russia's war of aggression against Ukraine threatens not only Ukraine's sovereignty and territorial integrity but the entire global stability and security. Both inside the EU and in its neighbourhood, it brings risks to the security of citizens. The cyber threats arising from the war underline the need to cultivate a culture of sharing information and expertise between the EU, Member States, and across the cybersecurity communities.

Given the rapid evolution of the digital domain, providers and users of digitalised services are expected to face increased cyber threats which, due to their cross-cutting and high impact, require resilience at strategic and operational levels across policy areas, including home affairs, security and defence, foreign policy, industrial and economic policy, research and technology development, and education.

With the realisation that digital society and digital services cannot safely exist without a solid cybersecurity framework, cybersecurity and resilience must become a focus of both domestic reforms and EU engagement in the Western Balkans. There is need for an increased EU-Western Balkans cooperation on cybersecurity to improve the region's preparedness and resilience to cyber threats. The IPA III Programming Framework recognises the need for enhanced cyber resilience and cybersecurity of the Western Balkans region in compliance with EU *acquis* and best practice.

Support to digitalisation is also underpinning the European Commission's policy priority "Europe Fit for the Digital Age", adapted for the external action. The digital transformation goes hand in hand with the green transformation, which collectively can drive economic growth in the Western Balkans. This is recognised in the Economic and Investment Plan for the Western Balkans[2] which facilitates increased investment in the region including in support of the digital transition and the Green Agenda for the Western Balkans.[3] Investments in energy, transport, water and environment infrastructure need to be accompanied by cybersecurity measures and a comprehensive plan to mitigate and adapt to climate change through a shift to a low-carbon and climate resilient development path.

2 COM (2020) 641 final

3 Guidelines for the Implementation of the Green Agenda for the Western Balkans. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020SC0223. SWD(2020)223 final, 6.10.2020

The EU Network and Information Security (NIS) Directive[4] and its revision (the so-called NIS 2.0)[5] set forth requirements for cybersecurity strategies. While Western Balkans IPA III beneficiaries generally acknowledge the importance of cybersecurity, four have cybersecurity strategies[6] in place, with the majority adopted within 2020-2022. In Albania, North Macedonia and Montenegro, the cybersecurity strategies and developments have been influenced by their EU integration path and the cooperation with NATO. Serbia's reform processes and related international dynamics have been closely connected to its EU candidate status. At the same time, Serbia has maintained its neutrality in foreign policy. Its cybersecurity commitments post April-2022 elections are yet to emerge, although its recent signature of the Declaration for the Future of the Internet,[7] aligning with the EU, signifies continued commitment to shared values. Bosnia and Herzegovina and Kosovo have yet to adopt comprehensive cybersecurity strategies, although in the case of the former, a document was drawn up in Bosnia and Herzegovina in 2019 under the auspices of the OSCE Mission in Bosnia and Herzegovina which should provide guidelines for the harmonization of existing and creation of new strategies for cybersecurity. A recent EU-funded needs assessment exercise on Western Balkans' cyber resilience has outlined the need for increased investment in EU-aligned cybersecurity capacity building for the region.

This action builds on the core objective of the European Union's engagement with the Western Balkans – to prepare the targeted IPA III beneficiaries to meet all the requirements of EU membership. Cyber resilience and cybersecurity are reflected in the Chapters 10 and 24 of the EU *acquis* and thus form an integral part of the accession process. The EU's Cybersecurity Strategy for the Digital Decade[8] and the EU Cyber Capacity Building Board that is currently being established identify the Western Balkans region as a priority for its future cyber capacity building activities. The EU is well-placed to provide cybersecurity capacity-building to the region, drawing upon the expertise of Member States and accompanying the assistance with policy engagement linked to the enlargement context and *acquis* alignment.

Effective coordination among donors as well as among other capacity building actors and implementers will remain one of the key success factors for a successful EU intervention's investment in cybersecurity capacity building in the Western Balkans. As such, the action will build upon rapid cybersecurity assistance provided by the European Commission to Albania, Montenegro and North Macedonia on cybersecurity governance structures and operational capacities for cyber incidents management and will complement cybercrime capacity building funded under the Instrument for Pre-Accession Assistance (IPA II). It will also work in close complementary with upcoming IPA III support in the area of critical infrastructure protection and cooperate with activities undertaken under the Flagship on Digital Infrastructure of the Economic and Investment Plan for the Western Balkans[1]. The action will actively participate in donor coordination fora in each respective beneficiary as well as in exchanges organised by EU CyberNet.

---

[4] 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. *OJ L 194, 19.7.2016, p. 1–30.* http://data.europa.eu/eli/dir/2016/1148/oj

[5] Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, repealing Directive (EU) 2016/1148
COM/2020/823 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

[6] A *national cybersecurity strategy* is widely understood as a high-level, comprehensive expression of the vision, high-level objectives, principles and priorities that guide a country in improving its security and resilience to cyber risks (https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf).

[7] Serbia supports Declaration for Future of Internet at meeting organised by United States
Belgrade, 28 April 2022. https://www.srbija.gov.rs/vest/en/188272/serbia-supports-declaration-for-future-of-internet-at-meeting-organised-by-united-states.php

[8] The EU's Cybersecurity Strategy for the Digital Decade. JOIN(2020) 18 final. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

2.2. Problem Analysis

The action targets concrete gaps at executive and operational levels in the cyber preparedness and response of the Western Balkans. The action will support beneficiary implementation of strategies underpinning their European path.

AREA OF SUPPORT #1: Cybersecurity governance and legal framework

A recently finalised EU-funded assessment on Western Balkans' cyber resilience has concluded that the targeted IPA III beneficiaries have various maturity levels as regards the cybersecurity governance framework. This is a core area for EU support in view of its importance including for operational capacity and in view of the European perspective of the region which requires alignment to EU *acquis*. There is generally a need to ensure clearly defined institutional frameworks, capacity and clear mandates as well as functional coordination mechanisms for cybersecurity governance. Legislative work is needed to harmonize the existing laws with the EU *acquis* – specifically, with the EU Network and Information Security (NIS) Directive[9] and its revision (the so-called NIS 2.0)[10] – and to establish an adequate legal basis for CII cybersecurity together with enforcement mechanisms in order to ensure that cybersecurity measures are implemented and that significant incidents are reported. Part of the challenge appears in overlapping responsibilities and gaps in implementation as well as in the lack of enforcement mechanisms, procedures and guidelines to ensure that the legislation and strategy are in place and get implemented. While the region presents some successful examples of public-private cooperation in cybersecurity, overall, there is a lack of a model on how to secure such cooperation. The Western Balkans also demonstrate a need for an inclusive process in forming foreign policy and international cooperation in line with relevant EU cyber diplomacy policies, as well as a need to connect to regional and international cooperation and information sharing formats. Strong and clear governance frameworks are the core of solid operational response as they ensure clear and efficient decision making across the institutional levels. Regional and international cooperation will further support the incident prevention and management processes by information and knowledge sharing.

AREA OF SUPPORT #2: Cyber risk and crisis management mechanisms

Although some of the targeted IPA III beneficiaries stand out as more advanced as regards cyber threat and risk assessment capacity, there is room for improvement in practice with regard to both CII operators and the public sector risk and crisis management structures. Strong and cooperating risk management institutions in line with EU standards are a prerequisite for the successful management of cyber incidents and cyber-induced crises. Domestic-level cybersecurity risk management frameworks lack capacities and processes necessary for instituting a systematic practice of cyber threat and risk assessments, as well as processes for incident reporting and information sharing for situational awareness. IPA III beneficiaries' overall domestic crisis management frameworks commonly lack consideration for cyber risks and key cybersecurity stakeholders are not trained in cyber-specific crisis management. Out of six Western Balkans IPA III beneficiaries, four have legally mandated cyber risk assessments for government organisations, the remaining two have a few sectoral or organisational practices but without a systematic, cross-government approach. Oversight roles for the implementation of risk management practice are in place in two IPA partners.

The following are the main stakeholders under the areas of support #1 and #2:

[9] 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.
OJ L 194, 19.7.2016, p. 1–30. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[10] Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, repealing Directive (EU) 2016/1148
COM/2020/823 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

Albania: National Authority for Electronic Certification and Cybersecurity (AKCESK) ▪ National Agency for Information Society (AKSHI) ▪ Electronic and Postal Communications Authority (AKEP) ▪ Ministry of Defence (MOD) ▪ Ministry of Interior (MoI)

Bosnia and Herzegovina: Ministry of Security of Bosnia and Herzegovina ▪ Ministry of Communications and Transport of Bosnia and Herzegovina ▪ Ministry of Defence of Bosnia and Herzegovina ▪ Federal Ministry of Transport and Communications (Federation of Bosnia and Herzegovina) ▪ Brcko District Government/Police ▪ Ministry of Interior Affairs of Federation of BiH ▪ Ministry for Scientific-Technological Development, Higher Education and Information Society of Republika Srpska ▪ Ministry of Interior Affairs of Republika Srpska ▪ CERT[11] RS (Republika Srpska); ▪ Academic CERT ▪ mil-CERT ▪ Neretva Group for Cyber Security - informal group of experts from various institutions ▪ Ministry of Foreign Affairs of Bosnia and Herzegovina ▪ Association for Digital Transformation

Kosovo: Ministry of Internal Affairs ▪ Office of the Prime Minister ▪ Ministry of Economy ▪ Secretariat of the Kosovo Security Council ▪ Ministry of Defence ▪ Kosovo's National Cyber Security Unit (KOS-CERT) ▪ Agency for Information Society (ASHI) ▪ Ministry of Finance, Labour and Transfers

Montenegro: Prime Minister's Office ▪ Ministry of Public Administration ▪ Ministry of Interior ▪ Ministry of Defence ▪ National Security Agency ▪ Directorate for Protection of Confidential Data (CIRT-ME)

North Macedonia: Prime Minister's Office ▪ Ministry of Information Society and Administration (MISA) ▪ Agency for Electronic Communications - hosting the national CIRT ▪ Ministry of Interior ▪ Ministry of Defence - in charge of cyber defence MKD-CIRT ▪ National Center for Computer Incident Response at the Agency for Electronic Communications

Serbia: Office for Information Technologies and e-Government ▪ Ministry of Trade, Tourism and Telecommunications ▪ SRB CERT (hosted by the Regulatory Agency for Electronic Communications and Postal Services (RATEL) ▪ Other computer security incident response teams (CSIRTs) (Government Office for Information Technologies and eGovernment; CERT MUP) ▪ Government Body for Coordination of Information Security Affairs (composed of representatives from various ministries) ▪ Ministry of Foreign Affairs ▪ National Security Council Internet Registry (RNIDS) ▪ Cybersecurity Network Foundation ▪ SHARE Foundation

AREA OF SUPPORT # 3 Operational capacities for cyber incidents management

The capacities of the national CSIRTs/CERTs[12] of several of the targeted IPA III beneficiaries appear severely limited in terms of both personnel and equipment. There is a need for improved tools and capabilities for threat monitoring and scanning, vulnerability handling, malware analysis, and early warning, as well as strengthening domestic and regional cooperation and information sharing. Both operational and initiating CSIRT teams also require support to further developing their professional skills through the improved availability of professional training and access to cybersecurity exercises. Importantly, the lack of documented processes and procedures for incident detection and resolution, external networking/peer-to-peer processes, and incident escalation need to be remedied.

[11] CERT stands for Computer Emergency Response Team, an institution with specific responsibilities in cyber protection. For reasons of tradition and practicality, the terms 'CSIRT' (Computer Security Incident Response Team) and 'CERT' are used interchangeably in this action document.

[12] As a term of art, 'national CSIRT' denotes a CSIRT (Computer Security Incident Response Team) that is designated by a country or economy to have specific responsibilities in cyber protection for the country or economy (Carnegie Mellon University). The term 'national CSIRT' is hence used throughout this report without prejudice to the political status or recognition of specific territories or economies.

The following are the main stakeholders under the area of support #3:

	Albania	**Bosnia and Herzegovina**	**Kosovo**	**North Macedonia**	**Montenegro**	**Serbia**
National CSIRT/CERT	National CIRT of Albania embedded in AKCESK	None	Kosovo National Cyber Security Unit (KOS-CERT)	MKD-CIRT	CIRT.ME embedded in the Directorate for the Protection of Classified Information	SRB-CERT
Other CSIRTs	Government CSIRT under AKSHI[13]	CERT RS (Republika Srpska); MilCERT (Ministry of Defence) Academic CERT under Sarajevo University CERT for the institutions of Bosnia and Herzegovina	CERT-KSF-RKS (CSIRT of the Security Forces)	Academic CERT (at University of Skopje - FINKI)	None	GOV CERT; CERT MUP; MoD CERT; a number of non-governmental and private CSIRTs/CERTs, e.g. financial CERT, SHARE CERT
(Single) Point of Contact for cybersecurity	AKCESK	None	KOS-CERT	MKD-CIRT (some regulated sector-specific incident reporting and information exchange; voluntary for remainder)	CIRT.ME	None

3. DESCRIPTION OF THE ACTION

3.1. Intervention logic

The overall objective (impact) of the action is to enhance the cyber resilience of the Western Balkans in compliance with EU *acquis* and best practices. This action impact is aligned with the IPA III Programming Framework which outlines that *"emerging security issues at global level also need to be addressed, in particular in the area of cybersecurity and building State and societal resilience against hybrid threats. Particular attention will be paid to providing increased support to capacity-building in the area of* ***cybersecurity*** *and fight against cybercrime."*[14]

The specific objective (Outcome) of the action is improved cybersecurity prevention, preparedness and response of relevant public and private stakeholders in the Western Balkans IPA III beneficiaries.

The following main outputs will be delivered by this action, contributing to the Outcome when assumptions hold true:

[13] National Cybersecurity Strategy and Action Plan 2020–2025 outline the objective of establishing CSIRTs in all industry sectors (including CI and CII).

[14] IPA III Programming Framework, p.16. https://ec.europa.eu/neighbourhood-enlargement/system/files/2022-01/C_2021_8914_F1_ANNEX_EN_V5_P1_1462290.PDF

Output 1: Strengthened organisational skills and mandates of public institutions on cybersecurity.

Output 2: Increased knowledge of public institutions on EU *acquis* related to cybersecurity and on cyber norms and international law.

Output 3: Improved capacities and mechanisms for cooperation of public institutions, civil society and private sector.

Output 4: Established and strengthened cyber risk and crisis management mechanisms of the Western Balkan IPA III beneficiaries.

Output 5: Increased operational capacities of Computer Security Incident Response Teams (CSIRTs) in cyber incidents management of the Western Balkan IPA III beneficiaries.

Given the high policy and political relevance of the outputs, the action will at all stages dovetail and support the overall policy engagement of the EU with the IPA III Western Balkans and allow for stepping up engagement.

3.2. Indicative Activities

The action will indicatively include the following main activities:

Under Output 1: Strengthened organisational skills and mandates of public institutions on cybersecurity.

1.1. Implementation of trainings and workshops to exchange best practices and raise organisational skills.

Under Output 2: Increased knowledge of public institutions on EU *acquis* related to cybersecurity and on cyber norms and international law.

2.1. Provision of advice on how to adjust the normative-legislative framework on cybersecurity.

2.2. Implementation of trainings and workshops on the application of frameworks of international cyber diplomacy.

Under Output 3: Improved capacities and mechanisms for cooperation of public institutions, civil society and private sector

3.1. Facilitation of meetings and provision of advice to set up cooperation mechanisms.

3.2. Implementation of workshops and trainings for civil society organisations and private sector to raise capacities on communication and awareness raising activities.

Under Output 4: Established and strengthened cyber risk and crisis management mechanisms of the Western Balkan IPA III beneficiaries.

4.1. Implementation of workshops, training sessions to share models on risk management mechanisms, threat intelligence and information sharing platforms and to develop organisational-level risk assessment models.

4.2. Provision of legal and technical advice to target groups.

4.3. Implementation of technical cybersecurity exercises to test and practice acquired knowledge and skills.

Under Output 5: Increased operational capacities of Computer Security Incident Response Teams (CSIRTs) in cyber incidents management of the Western Balkan IPA III beneficiaries.

5.1. Trainings on incident management processes and specific topics linked to cybersecurity; trainings on the use equipment and tools.

5.2. Provision of certification trainings for self-assessment and assessment of the process for joining relevant international bodies.

5.3. Provision of equipment and tools to CSIRTs.

5.4. Implementation of joint cybersecurity exercises and community building formats.

5.5. Assistance of participation of target groups in international conferences and networks events.

Across all outputs, regional and specific beneficiary-tailored activities will be carried out. The action will also support the EU's political engagement with the beneficiaries on cybersecurity, including by organising policy fora and exchange opportunities.

3.3. Mainstreaming

Environmental Protection, Climate Change and Biodiversity
The European Green Deal[15] aims to make Europe the first climate-neutral continent by 2050, and this cannot happen without its twin objective: the digital transition. A smarter and greener use of digital technologies are a key part in making sure Europe reaches that ambitious goal. Digital technology can help cut global emissions by 15% and outweigh the emissions caused by the sector.[16] The EU needs to apply these technologies systematically and make sure they power solutions carefully designed according to circular, regenerative principles. A digital and cyber resilient society will bring innovative business models, new services and better resource management and will contribute to achieving the climate goals. Throughout the implementation of this action, caution will be taken to reduce any associated environmental impact where possible.

Gender equality and empowerment of women and girls
The action will ensure the equal participation of women and integrate gender perspectives into its activities as a cross-cutting priority and will strive to promote gender equality and equal opportunities. Gender equality incentives will be incorporated particularly in capacity building activities. The action will strive to encourage women to build their up their cyber skills and encourage governments to motivate girls and women to study ICT and cybersecurity. Furthermore, the action will work with partners to ensure a balanced representation of women and men among action beneficiaries to the greatest extent possible (e.g. the action will not propose or accept single-gender workshops, panels, etc.).

As per OECD Gender DAC codes identified in section 1.1, this action is labelled as G0.

Human Rights
All activities under this action will be designed and implemented in accordance with the principles of good governance and human rights, gender equality, the inclusion of socially or economically deprived groups and environmental sustainability, wherever these issues are of particular relevance to the institutions and beneficiaries to be assisted. Cybersecurity, also in relation to capacity building, involve a wide range of stakeholders including from security and law enforcement agencies. Therefore, particular focus should be placed in the incorporation of safeguards in the proposed action in relation to human rights, data protection and good governance, in line with the EU Cybersecurity Strategy for the Digital Decade,[17] the EU Strategic Framework and Action Plan on Human Rights and Democracy.

As per OECD Disability DAC codes identified in section 1.1, this action is labelled as D0.

Democracy
The European Union has repeatedly confirmed the importance of having all stakeholders involved in internet governance and its commitment to strengthening the multi-stakeholder model, which is supported by like-

[15] COM(2019) 640 final, 11.12.2019
[16] https://www.weforum.org/agenda/2019/01/why-digitalization-is-the-key-to-exponential-climate-action/ (2019)
[17] JOIN(2020) 18 final

minded partners.[18] This stands in contrast to having only the government at the centre of cyber-related decision-making. The civil society will have a role to play particularly in the activities linked to the field of governance and awareness raising. The overall approach of the action will be in line with the three pillars of the European Democracy Action Plan.[19]

3.4. Risks and Lessons Learned

Category	Risks	Likelihood (High/ Medium/ Low)	Impact (High/ Medium/ Low)	Mitigating measures
People and the organisation	Risk 1 Limited interest, trust, and/or stakeholders' buy-in into the foreseen action	**L**	**M**	Lack of interest, trust and/or buy-in will be addressed through the demonstration of concrete results that can be derived from the cooperation. While specific activities will be planned and consulted with the Western Balkans, including at the technical and strategic level, specific work plans can be adjusted should there be limited interest. Awareness-raising and regional capacity-building activities are also expected to contribute to strengthened networking and trust-building, creating favourable conditions at the technical/operational level to counterbalance possible negative developments at the political level. Regular dialogue and coordination with DG NEAR, DG CNECT, EEAS, FPI and EU Delegations/EU Office is foreseen to ensure beneficiary buy-in.
Planning, processes and systems	Risk 2 Political instability/tensions, and/or complex institutional set-ups may disrupt or delay activities	**M**	**H**	The action will adopt a flexible approach in planning and implementation of its activities. A strong link between the action delivery and the policy engagement between the EU and the region is seen as a mitigation strategy.
Planning, processes and systems	Risk 3 Limited absorption capacity in Western Balkans and lack of donor coordination	**M**	**M**	Implementing partner will be responsible to ensure coordination with the EU Commission, as well as with other donors in the region with a view to better streamline the various activities. Coordination of other

[18] Operational Guidance for the EU's international cooperation on cyber capacity building, p. 61. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf p. 43-44.
[19] COM(2020) 790 final

				actors and implementers is expected to be supported by EU CyberNet.
Regional political aspects	Risk 4 Little interest in regional cooperation for political reasons	**M**	**M**	Outlining the benefits for regional cooperation by supporting and encouraging participation in regional cooperation activities. Promoting the need for "regional-actions" on cybersecurity issues. Holding regional project team meetings.
External environment	Risk 5 Growing global cybersecurity threats may exceed the capacity of the Western Balkans region to deal with them	**L**	**M**	Continued support to the Western Balkans on cybersecurity and stepping up dialogue with and training of skillsets of the main stakeholders among respective IPA beneficiaries as specified in 2.2.

Lessons Learned:

The proposed action builds upon lessons learned from previous and on-going IPA multi-country programmes. The main lessons learned which are reflected in the design of the action or its specific pillars include:

- In view of the direct policy relevance of the action, implementation will require high institutional commitment from the beneficiaries. This will require that the action is accompanied by policy dialogue and engagement from the European Commission towards the region. Accordingly, close monitoring and evaluation of implementation and engagement of the relevant European Commission line DGs (NEAR, CNECT) across all activities is necessary throughout the action;
- Previous actions have shown the need to adopt a flexible approach to project implementation particularly also in the COVID-19 context. While activity plans are to be agreed at the level of Steering Committees, adaptations should be possible throughout the programme;
- Need for continuous coordination to ensure complementarity with bilateral support programmes, particularly those funded under the IPA instrument;
- Staff rotation in beneficiary institutions and agencies can provide drawbacks in achieving progress or attaining significant consolidation of results. Therefore, detailed planning of available human resources, proper documentation of all training activities and knowledge transfer should be applied;
- The role of beneficiaries in planning the activities has to be strong in order to facilitate greater ownership and to enhance the effectiveness and sustainability of the actions. A demand-driven approach on the basis of a comprehensive needs assessment is therefore necessary.

3.5. Indicative Logical Framework Matrix

Results	Results chain: Main expected results	Indicators	Baselines	Target	Sources of data	Assumptions
Impact	To enhance the cyber resilience of the Western Balkans in compliance with EU *acquis* and best practices	A) Degree of readiness of Western Balkans on EU *acquis* alignment on cybersecurity B) Global Cybersecurity Index (GCI) Score C) Political Stability and Absence of Violence/Terrorism	A) Some level of preparation/moderately prepared (2021) B) Albania: 64.32; Bosnia and Herzegovina: 29.44; Kosovo: - ; Montenegro: 53.23; North Macedonia: 89.92; Serbia: 89.8 (2020) C) Albania: 49.53; Bosnia and Herzegovina: 27.38; Kosovo: 36.79; Montenegro:47.17; North Macedonia: 50.47; Serbia: 43.87 (2020)	A) Increased level of preparedness (2026) B) Improvement of score on cybersecurity (2026) C) Increased percentile rank on political stability and absence of violence/terrorism (2026)	A) European Commission annual reports per beneficiary B) Global Cybersecurity Index (GCI) managed by the International Telecommunication Union (GCI) C) World Bank Worldwide Governance indicators *Percentile rank 0-100; 0 corresponds to lowest rank and 100 corresponds to highest rank*	*Not applicable*

Outcome	Improved cybersecurity prevention, preparedness and response of relevant public and private stakeholders in the Western Balkans IPA III beneficiaries	Level of preparedness to prevent cyber threats and manage cyber incidents	Albania: 68; Bosnia and Herzegovina: 103; Kosovo: -; Montenegro: 91; North Macedonia: 52; Serbia: 18 (2021)	Improved ranking (2026)	National Cybersecurity Index (NCSI)	The political and security situation allows the system to function freely. Cyber risk and crisis management approaches remain sufficient and up-to-date with changing threat landscape. Continuous commitment, steered and coordinated at the highest level of the beneficiaries, to address cybersecurity threats in line with the EU. Beneficiaries recover from eventual cyber incidents.

Output 1	Strengthened organisational skills and mandates of public institutions on cybersecurity	Number of secondary legislation drafts that benefit from the support of the EU intervention	0 (2023)	To be determined by the project (2026)	Project reports	Ministries timely prepare and submit legislative drafts to the Parliaments. Parliaments are sensitised and willing to revise and adopt new legislation following international best practices. Ministries and governmental bodies adopt secondary legislation. Ministries and governmental bodies have sufficient leverage, resources and political mandate to implement and enforce cybersecurity policy.
Output 2	Increased knowledge of public institutions on EU *acquis* related to cyber security and on cyber norms and international law	Number of decision-makers trained by the EU-funded intervention who increased their knowledge and/or skills on EU *acquis* and on cyber norms and international law (disaggregated by sex)	0 (2023)	To be determined by the project (2026)	Project reports	
Output 3	Improved capacities and mechanisms for cooperation of public institutions, civil society and private sector	Status of national cooperation mechanisms on cybersecurity	Low (2023)	Improved status (2026)	Project reports	
Output 4	Established and strengthened cyber risk and crisis management mechanisms of the Western Balkans IPA III beneficiaries	Number of cyber risk assessments conducted with support of the EU-funded intervention	0 (2023)	To be determined by the project (2026)	Project reports	Target group management is sensitised and willing to commit to implementing cyber risk management/ risk-based approach. Target group organisations commit to acquiring adequate

						staffing for cyber risk and crisis management tasks.
Output 5	Increased operational capacities of CSIRTs in cyber incidents management of the Western Balkans IPA III beneficiaries	A) Number of CSIRTs that have a training programme in place B) Number of cooperation arrangements among Western Balkans CSIRTs and among the Western Balkans and the EU CSIRTs in place	A) 0 (2023) B) 0 (2023)	A) 6 (2026) B) To be determined by the project (2026)	Project reports	Beneficiaries commit to acquiring adequate staffing to absorb training and service development. Beneficiaries are capable to absorb the equipment and tools to CSIRTs.

4. IMPLEMENTATION ARRANGEMENTS

4.1. Financing Agreement

In order to implement this action, it is not envisaged to conclude financing agreements with the targeted IPA III beneficiaries.

4.2. Indicative Implementation Period

The indicative operational implementation period of this action, during which the activities described in section 3 will be carried out and the corresponding contracts and agreements implemented, is 72 months from the date of adoption by the Commission of this amending Financing Decision.

Extensions of the implementation period may be agreed by the Commission's responsible authorising officer by amending this Financing Decision and the relevant contracts and agreements.

4.3. Methods of implementation

The Commission will ensure that the EU appropriate rules and procedures for providing financing to third parties are respected, including review procedures, where appropriate, and compliance of the action with EU restrictive measures[20].

4.3.1. Indirect Management with a Member State Organisation

This action may be implemented in indirect management with a Pillar Assessed Member State Organisation or potentially a consortium of them. This implementation entails the full implementation including through direct implementation of activities and conducting budget implementation tasks (procurement and grants award procedures as relevant) of this action entitled "**EU Support to Cybersecurity Capacity Building in the Western Balkans**" and the corresponding impact, outcome and outputs as above described under section 3. The envisaged entity will be selected using the following criteria: Member State organisation; specific cybersecurity technical expertise; expression of support from cybercompetent authority/ies in the EU; management capacity demonstrated through implementation of previous actions in the security sector; track record of engagement with the Western Balkans. In case of a consortium, each entity would need to fulfil the above-mentioned criteria.

4.4. Scope of geographical eligibility for procurement and grants

The geographical eligibility in terms of place of establishment for participating in procurement and grant award procedures and in terms of origin of supplies purchased as established in the basic act and set out in the relevant contractual documents shall apply, subject to the following provisions.

The Commission's authorising officer responsible may extend the geographical eligibility on the basis of urgency or of unavailability of services in the markets of the countries or territories concerned, or in other duly substantiated cases where application of the eligibility rules would make the realisation of this action impossible or exceedingly difficult (Article 28(10) NDICI-Global Europe Regulation).

[20] www.sanctionsmap.eu Please note that the sanctions map is an IT tool for identifying the sanctions regimes. The source of the sanctions stems from legal acts published in the Official Journal (OJ). In case of discrepancy between the published legal acts and the updates on the website it is the OJ version that prevails.

4.5. Indicative Budget

Indicative Budget components Budget line: 15.020101.01	**EU contribution (amount in EUR)** **2022**
Methods of implementation – cf. section 4.3	
Outcome 1, Outputs 1-3	
Indirect management with a Member State Organisation – cf. section 4.3.1	5 000 000
Evaluation – cf. section 5.2 **Audit** – cf. section 5.3	N.A.
Communication and visibility – cf. section 6	N.A.
Totals	5 000 000

4.6. Organisational Set-up and Responsibilities

The steering of the action will be done through a Steering Committee co-chaired by the European Commission's Directorate-General for Neighbourhood and Enlargement Negotiations and the implementing partner. Other European Commission services (such as Directorate-General for Communications Networks, Content and Technology), the European External Action Service and the EU Delegations and EU Office will be closely associated as relevant. Programme-specific contact points shall be nominated in each relevant IPA III beneficiary, in EU Delegations and EU Office to ensure coordinated internal and external communication.

Regular meetings of the Steering Committee will be held to ensure overall management support and strategic guidance to the action. The Steering Committee will meet at least annually and will be responsible for the monitoring the implementation of the action on the basis of activity reports presented by the implementing partner.

5. PERFORMANCE MEASUREMENT

5.1. Monitoring and Reporting

The day-to-day technical and financial monitoring of the implementation of this action will be a continuous process, and part of the implementing partner's responsibilities. To this aim, the implementing partner shall establish a permanent internal, technical and financial monitoring system for the action and elaborate regular progress reports (not less than annual) and final reports. Every report shall provide an accurate account of implementation of the action, difficulties encountered, changes introduced, as well as the degree of achievement of its results (Outputs and direct Outcomes) as measured by corresponding indicators, using as reference the logframe matrix. The Commission may undertake additional project monitoring visits both through its own staff and through independent consultants recruited directly by the Commission for independent monitoring reviews (or recruited by the responsible agent contracted by the Commission for implementing such reviews).

The implementing partner will continuously capture, record and track key statistical information on the implementation of activities. Particular emphasis will be placed on systematic collection of data required to track progress on indicators identified in the logical framework. A detailed contract logical framework will be part of the implementation agreement. The monitoring methods and sources will include the following as

relevant: action records showing details about events held and actions taken (including gender aggregated indicators); website and social media analysis showing viewership, reach, and engagement of target audiences; visibility and impact of social media campaigns; number of mainstream media stories published using material provided through the action; and feedback from participants through questionnaires designed for the action.

5.2. Evaluation

Having regard to the importance of the action, a mid-term evaluation will be carried out for this action or areas of support via an implementing partner.

It will be carried out for learning purposes, in particular with respect to assessing the commitment of IPA III Western Balkans beneficiaries to implement EU aligned cybersecurity capacity building.

The evaluation reports shall be shared with the targeted IPA III beneficiaries and other key stakeholders following the best practice of evaluation dissemination. The implementing partner and the Commission shall analyse the conclusions and recommendations of the evaluations and, where appropriate, in agreement with the targeted IPA III beneficiaries, jointly decide on the follow-up actions to be taken and any adjustments necessary, including, if indicated, the reorientation of the project.

5.3. Audit and Verifications

Without prejudice to the obligations applicable to contracts concluded for the implementation of this action, the Commission may, on the basis of a risk assessment, contract independent audit or verification assignments for one or several contracts or agreements.

6. COMMUNICATION AND VISIBILITY

Visibility of EU funding and communication about objectives and impact of Actions are a legal obligation for all Actions funded by the EU, as set out in the EU communication and visibility requirements in force.
In particular, the recipients of EU funding shall acknowledge the origin of the EU funding and ensure its proper visibility by:

- providing a statement highlighting the support received from the EU in a visible manner on all documents and communication material relating to the implementation of the funds, including on an official website and social media accounts, where these exist; and
- promoting the actions and their results by providing coherent, effective and proportionate targeted information to multiple audiences, including the media.

Visibility and communication measures shall be implemented, as relevant, by the national administrations (for instance, concerning the reforms linked to EU budget support), entrusted entities, contractors and grant beneficiaries. Appropriate contractual obligations shall be included, respectively, in financing agreements, delegation agreements, and procurement and grant contracts.
The measures shall be based on a specific Communication and Visibility Plan, established and implemented in line with the EU communication and visibility requirements in force. The plan shall include, inter alia, a communication narrative and master messages for the Action, customised for the various target audiences (stakeholders, civil society, general public, etc.)
Visibility and communication measures specific to this action shall be complementary to the broader communication activities implemented directly by the European Commission services and/or the EU Delegations and Offices. The European Commission and the EU Delegations and Offices should be fully informed of the planning and implementation of the specific visibility and communication activities, notably with respect to the communication narrative and master messages. It is the responsibility of the implementing partner to keep the EU Delegations/Office and the European Commission fully informed of the planning and implementation of the specific visibility and communication activities.

7. SUSTAINABILITY

The action has been designed to ensure the long-term sustainability of its results. By focusing on the strengthening of institutions and building capacity thereof, including through access to adequate policies, new equipment, IT tools, knowledge and skills used on an everyday basis, the resulting capacity increase is expected to be sustainable. Key activities in this regard include support to legislation, guidelines and development of training materials.

The sustainability of the equipment supplied through the action will be guaranteed through the existence of long-term maintenance contracts accompanying the purchasing and capacity-building within or in complement to the present action. Coupling capacity building with modernisation of equipment will improve the efficiency of the cybersecurity risk management systems as a whole and will ensure sustainable results.

Furthermore, where possible, the action will seek to streamline best practices in line with EU and international standards into the everyday technical operation of the different areas of the beneficiaries' risk management systems and CSIRTs. Any ICT development should respect the existing standards or needs for interoperability of IT systems. The necessary technical specifications shall be consulted with the relevant authorities and ensured before the launch of the tender.

Comprehensive policy dialogue will be maintained at all times between the Commission, EU Delegations and implementing partners to ensure strong political will to maintain equipment, infrastructure and training initiatives.