EUROPEAN
COMMISSION

Brussels, 9.10.2024
C(2024) 6891 final

ANNEX

ANNEX

to the

Commission Implementing Decision

on the financing of the Connecting Europe Facility – Digital sector and the adoption of the multiannual work programme for 2024-2027

ANNEX

Contents

1 Introduction

The Connecting Europe Facility (CEF) is a European Union funding programme to promote growth, jobs, inclusiveness and competitiveness through the efficient interconnection of transport, energy and digital networks within and across Member States. It fosters public and private investments for the development of high-performance, sustainable and resilient trans-European infrastructures of an increasingly interconnected European society.

The first CEF Digital Work Programme, adopted late 2021 in the midst of the COVID-19 pandemic, had a strong focus on territorial digital inclusion and the contribution to the achievement of the 2030 Digital Decade targets. While this objective is still at the heart of CEF Digital, the mutated policy context requires the adaptation of the new Work Programme's priorities, to address critical geopolitical and geoeconomic challenges and provide a reinforced ground to stimulate the competitiveness of the European digital ecosystem.

Following the informal Telecom Council meeting in Nevers on 9 March 2022, the development and protection of critical infrastructure such as telecommunications networks[1] and digital services has become a priority for the Union, resulting into a series of policy initiatives by the European Commission, including the Recommendation on "Secure and Resilient Submarine Cable Infrastructures" and the White Paper on "How to master Europe's digital infrastructure needs?"[2]. The threats to critical infrastructure, exacerbated by Russia's war of aggression against Ukraine, and the risk of critical dependencies in the digital sector are major concerns for the EU. Ensuring the physical and cybersecurity, as well as resilience of those critical infrastructures is a main priority in the current geopolitical landscape.

It is therefore imperative to step up investments in the digital strategic autonomy of the Union, *inter alia* through the deployment of sustainable and resilient high-performance infrastructure in an unprecedented manner.

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030[3] reaffirms the crucial role of digital connectivity and sets levels of ambition for 2030, namely a Gigabit network for all European households and 5G in all populated areas[4]. It also stresses the importance of connecting the Union with its international partners in line with the Global Gateway strategy[5].

CEF Digital is based on Regulation (EU) 2021/1153 of the European Parliament and of the Council (the "CEF Regulation")[6], which determines the general principles, legal base and procedures for providing EU financial support to trans-European networks in order to support projects of common interest (PCIs) in the fields of transport, energy and digital. The CEF Regulation also establishes the breakdown of resources available for 2021-2027 in transport, energy and digital. The first CEF Digital multiannual work programme, covering the calls for

---

1 Recommendation on the security and resilience of submarine cable infrastructures | Shaping Europe's digital future (europa.eu)

2 White Paper - How to master Europe's digital infrastructure needs? | Shaping Europe's digital future (europa.eu)

3 Decision - 2022/2481 - EN - EUR-Lex (europa.eu)

4 All end users at a fixed location are covered by a gigabit network up to the network termination point, and all populated areas are covered by next-generation wireless high-speed networks with performance at least equivalent to that of 5G, in accordance with the principle of technological neutrality

5 Global Gateway - European Commission (europa.eu)

6 Regulation - 2021/1153 - EN - EUR-Lex (europa.eu)

2021-23 was adopted with Implementing Decision C(2021)9463 of 16.12.2021, and amended with Implementing Decision C(2023)2533 of 19.4.2023.

In accordance with Article 20 of the CEF Regulation, the second multiannual work programme establishes the basis for the allocation of the Union financial support to PCIs for the digital sector of CEF for the period 2024-2027. It contains information about the actions planned over the covered period.

The work programme also outlines the general scope and objectives of the supported actions as defined in Article 3 of the CEF Regulation, the investment priorities (Article 8 and part V of the Annex – regarding point 3 of part V of the Annex only as non-exhaustive examples - of the CEF Regulation), the eligible actions (Article 9), the award criteria (Article 14), as well as the envisaged level of funding, which will take the form of grants and procurement (Article 6). It also covers accompanying measures to be awarded/contracted during the period 2024-2027.

For further information on the work programme and the related calls, please refer to the CEF Digital website at Connecting Europe Facility (europa.eu).

On the basis of the objectives laid down in the CEF Regulation, this multiannual work programme contains the actions to be financed and the budget breakdown for years 2024-2027 as follows:

(a) for grants (implemented under direct management), section 3, 5G infrastructures, 2024; section 4.1, EuroQCI, 2024; section 4.2 Global gateways, 2024, section 4.3 Operational digital platforms, 2025);

(b) for procurement (implemented under direct management) (section 5, support actions, 2024-27);

(c) for financial instruments (section 3, 5G infrastructures, 2025 and section 4.2, Global gateways, 2026;

(d) for contributions to blending facilities, (section 4.2, Global gateways, 2025-26)

The budget line is 02 03 03 01 and detailed indicative amounts allocated per topic, the legal bases, the implementing modes and planning are set out in sections 3 - 7.

2 Context, objectives and overall approach

2.1 Policy context and investment needs

The EU can fully reap the benefits of the digital transformation and strengthen its competitiveness worldwide if access to Gigabit networks is made available to all users, businesses and 'socio-economic drivers'[7] (SEDs), irrespective of their location or other economic factors affecting commercial deployment. Consistent deployment of high-performance infrastructure, including fibre and 5G infrastructures is needed to meet the increasing demand for the secure transfer and processing of massive amounts of geographically

[7] In particular, among others, schools, universities, hospitals, transport hubs and public administrations. See also, definition of socio-economic drivers in Art 2(s) and, more in detail, in Recital (37) of the CEF Regulation.

distributed data. By their nature, trans-European Gigabit and Terabit networks enable data to flow and people to collaborate wherever they are. They connect digital capacities such as cloud and high-performance computing as well as millions of objects and data able to transform and modernise vertical sectors such as health, education and training, tourism, manufacturing, transport and logistics. For users with disabilities to be able to benefit from the digital transformation it must be ensured that related developments are accessible[8] for and inclusive of persons with disabilities.

The increased online interaction between people and objects and the emergence of new applications scenarios driven by the advent of AI and Virtual Worlds, new ways of working, living, doing business and delivering public services require adequate capability from the underlying digital connectivity infrastructure, as well as a high level of protection, especially for sensitive data and critical infrastructures, from cyberattacks. Furthermore, sustainable and secure state-of-the-art backbone infrastructures are needed to interconnect digital capacities, such as cloud, data and high-performance computing, which are vital to support the EU's ambition to be digitally sovereign in an open and hyper-connected world.

According to a recent study conducted for the European Commission~~,~~[9] reaching current Digital Decade targets for Gigabit connectivity and 5G may require a total investment of up to EUR 148 billion, if fixed and mobile networks are deployed independently and standalone 5G~~–~~ offering European citizens and businesses the full capabilities that can be offered by 5G mobile networks - is deployed. A further EUR 26-79 billion of investments may be required under different scenarios to ensure full coverage of transport paths including roads, railways, and waterways, bringing the required total public and private investment needs, according to this study, for connectivity alone to over EUR 200 billion.

Beyond terrestrial connectivity, investments in satellite ground stations (teleport) backhaul infrastructures may be required in order to provide complementary solutions for backhaul-to-device connectivity in remote areas not covered by terrestrial technologies or to ensure service continuity in case of crisis or disaster relief. Moreover, in the future, satellite communication systems will offer electronic communications services, like the 5G standard, to enable a seamless handover between terrestrial and satellite services.

The successful completion of network virtualisation and software and cloud-based solutions to provide Network-as-a-service (NaaS) would require additional significant investment capacities. There is an estimated cloud investment gap in the EU of EUR 80 billion until 2027[10]. A slow transition of telecommunication providers in the EU towards developing and integrating cloud-based solutions for electronic communications services and beyond would pose risks of further dependencies in the digital services sector.

In the context of the implementation of the Recovery and Resilience Facility ("RRF"), some Member States have committed very significant amounts of public resources for the deployment

---

8 See the European Accessibility Act Directive 2019/882

9 Investment and funding needs for the Digital Decade connectivity targets | Shaping Europe's digital future (europa.eu)

10 European Alliance for Industrial Data, Edge and Cloud: "European industrial technology roadmap for the next-generation cloud-edge", extrapolating until 2030 the investment gap identified in the Commission Staff Working Document (27.5.2020): Identifying Europe's recovery needs, SWD(2020) 98 final/2, Brussels, pp. 17-18;
Synergy Resarch Group, e.g. based on Q1/2023 data, Investments related to general cloud capacities tailored to the business model of each cloud provider and not significantly overlapping with the general EU connectivity investment needs.

of Gigabit and 5G networks. However, these programmes are mainly focusing on the deployment of infrastructure within Member States and only marginally in cross-border infrastructure, linking Member States between themselves or with third countries.

In February 2024, the Commission published the White Paper "How to master Europe's digital infrastructure needs?"[11], in which it presents the challenges and opportunities Europe currently faces in the rollout of future connectivity networks, suggesting potential scenarios for action to strengthen the EU's capacities and economic security in all critical parts of the connectivity-computing continuum. In the White Paper, the Commission notably highlighted the difficulty of the European electronic communications sector to attract investment and the need for infrastructure programmes, such as CEF Digital to maximise the leveraging of private resources including through blending operations.

The White Paper includes a section dedicated to existing and new submarine cable infrastructures, including aspects of security, resilience, and funding. More specifically on funding, it suggests that a future amendment of the Annex Part V of the CEF Regulation could be considered in order to establish a list of strategic Cable Projects of European Interest (CPEIs) that would address identified risks, vulnerabilities and dependencies. CPEIs could be conceived to comply with the most advanced technological standards, such as sensor capabilities for their own monitoring and to support EU policies in the field of security, sustainability, or civil protection. The White Paper stresses that it will be important to ensure appropriate funding of CPEIs and pool together EU and national funding instruments, and explore the feasibility and potential leverage effect of financial instruments to ensure synergies and sufficient financing of CPEIs.

CEF Digital is expected to be one of the main instruments financing CPEIs to reinforce the connectivtity links between Member States, stimulate the EU's supply chain and support the EU-wide digital ecosystem. The CEF contribution to the digital transformation can be even further increased by Member States preparing eligible projects through a coherent combination of CEF and RRF investments or the design of complementary interventions under European Agricultural Fund for Rural Development ("EAFRD") and European Regional Development Fund ("ERDF") or national programmes.

As explained in the previous section, security of digital infrastructures, including backbone, backhaul and access networks, is a priority for the Union. In the first Report on the state of the Digital Decade 2023[12], the Commission recommended that Member States "boost their efforts, including through necessary investments, to ensure that European digital infrastructures are secure and resilient, especially backbone infrastructure and submarine cables." The 2024's report highlighted the progress made at EU level in deploying security backbone connectivity between Member States and with third countries, including through CEF Digital investments in submarine cables[13].

Lastly, the White Paper is accompanied by a Recommendation on Secure and Resilient Submarine Cable Infrastructures[14], which presents a set of actions at national and EU level aimed at improving submarine cable security and resilience, through a better coordination across the EU, both in terms of governance and funding. The Recommendation envisages the

---

11 Idem footnote 6

12 2023 Report on the state of the Digital Decade | Shaping Europe's digital future

13 Report on the state of the Digital Decade 2024

14 Recommendation on the security and resilience of submarine cable infrastructures | Shaping Europe's digital future (europa.eu)

creation of an Expert Group composed of Member States authorities that will advise the Commission about the CPEIs to be prioritised for funding in order to strengthen the resilience and security of the EU backbone.

2.2 Work programme objectives

Pursuant to the CEF Regulation, CEF Digital's overall goal is to contribute to the development of *PCIs* relating to the deployment of safe, secure, sustainable and very high capacity digital networks, including 5G systems, to the increased capacity and resilience of digital backbone networks in all EU territories, in particular the Outermost Regions, as well as to the digitalisation of transport and energy networks. Specific objectives that projects funded under CEF Digital are expected to address are set in the following sections.

Leverage private investment in market failure areas

To achieve the Digital Decade 2030 EU connectivity objectives, EU funding has to be used to leverage other public, but also private investment where possible, in areas with market failure. This work programme will therefore fund projects with different co-financing rates and encourage the necessary mix of public grants and private finance, while targeting areas where the market players alone would not deliver Gigabit infrastructures and services to address end-users' needs.

The underlying goal is to bring together public support and private investment in the most efficient manner possible, for instance by stimulating private operators' investments aiming to deploy networks as comprehensively as possible in terms of geographical reach, diversity of targeted entities, quality of connectivity, etc.

In this regard, and in order to maximise the leverage effect on private investment, the Commission will also implement the programme in close cooperation with public financial institutions, notably through the support of eligible operations through relevant InvestEU financial products.

Cross-fertilise investments and ensure complementarity of funding programmes

Digital connectivity infrastructures can be supported at European, national, regional and local levels when they fail to attract sufficient commercial funding. This work programme will cross-fertilise these investments and act as a catalyst for the EU-wide digital connectivity ecosystem. By encouraging the combination of different funding sources and taking into account the existence of complementary projects (e.g. national segments in market failure areas complementing cross-border projects or backhaul supporting access networks), the work programme aims at reducing fragmentation in investments while ensuring the coherence, interoperability and harmonisation of digital connectivity infrastructures and their efficient integration with other strategic infrastructures in the fields of transport and energy[15].

Both the Recovery and Resilience Facility (RRF) and the Cohesion policy funds can be used to support long-term reform and investments in digital and green technologies. Technologies such as fibre and 5G are expected to make a significant contribution to the European Green Deal[16] as they have the potential to both improve the sustainability footprint of the connectivity sector

---

15 Article 10 of CEF Regulation

16 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1576150542719&uri=COM%3A2019%3A640%3AFIN

itself and enable significant energy efficiency gains and carbon emissions reduction in the electronic communication sector as well as in other key economic sectors such as transport and energy. They will also be able to sustainably scale up to meet the ever-growing data and bandwidth demands in both fixed and mobile communications.

While CEF funding does not constitute State aid the use of other public resources to provide the necessary co-financing for a project may involve State aid and may require a notification to the Commission to assess its compatibility under State aid rules[17]. However, there are several possible scenarios in which the use of other public resources to co-finance certain types of projects would not constitute State aid[18] or may not require its notification.[19] More details on State aid and the Commission's considerations are provided in section 10.

It is expected that Member States will use actions funded under this work programme in coordination with similar projects funded under their own budget or other EU funding instruments such as the RRF, ERDF, EAFRD, etc. In this respect, several approaches can be envisaged provided that the provisions of the relevant Regulation are respected. In most cases close coordination between all public actors is needed, in particular to ensure the absence of double funding: for instance, it is not possible to use RRF funding to co-fund a CEF project, although it can be used to fund separate but complementary activities[20].

In line with the Digital Decade Policy Programme[21], the present work programme will support the implementation of Multi-Country Projects in selected areas, involving several Member States, pooling resources from the Union, Member States, and where possible private sources. Such projects require a coordinated approach, in close cooperation between the Commission and the concerned Member States. CEF Digital may contribute to Multi-Country Projects by preparing the ground (e.g. through feasibility studies), developing and sharing information on technical solutions, legal and financial aspects.

The Commission will also explore the possibility to establish a CEF Digital Connectivity Blending Facility (based on Art. 17 of CEF Regulation). The Commission services will work closely with potential Implementing Partner institutions at EU level (European Investment Bank "EIB") and in Member States, including National Promotional Banks and Institutions (NPBIs) and private banks, to efficiently combine grants from CEF Digital with repayable forms of financing not supported by the Union budget (such as equity and loans) from the Blending Facility partners, to support infrastructure deployment projects in Member States.

Building pan-European cross-border infrastructures

---

17 See Section 10.

18 See the Commission Notice on the notion of State aid as referred to in Article 107(1) of the Treaty on the Functioning of the European Union

19 See Commission Regulation (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty (as amended).

20 Several approaches can be envisaged in cases the other programmes' legal bases do not allow combining funds from different sources. One possibility is to split the deployment of a large infrastructure into two or more sections deployed by independent projects, each funded by different programme. Another possibility is to use the Seal of Excellence (SoE) quality label under the CEF programme to finance projects that are successful under CEF, but for which there is insufficient budget available under the respective CEF Calls, under programmes that allow the use of such SoE (e.g. RRF or ERDF). It is also possible to use CEF actions as best practices to address similar use cases under other programmes, for instance in the context of smart communities, or using RRF funding for infrastructures falling within the national borders, for example to link to cross-border infrastructures funded under CEF and providing successive financial support (staging) to complete the end-to-end infrastructure.

21 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A0574%3AFIN

This work programme will support the deployment of 5G systems, including, if appropriate, integrated cloud-edge computing facilities, along major transport paths as well as in local communities. An integrated approach encompassing active as well as passive network components (e.g. masts, antennas and distributed antenna systems), federated cloud and edge infrastructures, as well as relevant operational service platforms will be ensured by complementary actions funded under CEF Digital and Digital Europe and other programmes such as InvestEU and ERDF. The aim is to enable service continuity and the interoperability of 5G services along transport paths across the continent. It will also support the interconnection of the national terrestrial quantum communication networks of the EuroQCI, a pan-European secure quantum communication infrastructure,[22] with each other and with the EuroQCI's space segment. This will complement support from other EU funding programmes, most notably the Digital Europe Programme.

International dimension of connectivity

In line with the EU Global Connectivity Strategy[23] and the EU's overall geopolitical framework in tackling global challenges, CEF Digital will support the development of global gateways[24] connecting the European Union with the rest of the world. This will be done by investing in secure and resilient backbone networks connecting Europe with third countries, including submarine cables, satellite and terrestrial backbones. It will also seek to leverage the EU's geostrategic presence in the Caribbean, Latin America, the Indian and the Atlantic Ocean through its Outermost Regions, which are a key asset to strengthen regional cooperation[25].

Enable access to shared digital capacities

The EU and the Member States are tackling major societal challenges by investing massively in digitalisation and innovation. The deployment of cloud, and high performance computing (HPC) and data infrastructures will enable a broad range of applications for the benefit of citizens, SMEs and industries. Projects funded under this work programme will ensure high-capacity, high-speed, reliable connectivity between these digital capacities.

Contribute to innovation and competitiveness in the EU digital ecosystem

Alongside the Digital Europe Programme, projects funded under this work programme will contribute to invigorate the digital readiness and competitiveness of the EU's business, industrial and public services ecosystem by supporting a number of innovative 5G based solutions that could later be replicated at a larger scale. Firstly, they are expected to accelerate the modernisation of vertical sectors such as healthcare, transport, education and training and public administration, which depend heavily on access to reliable, affordable high-quality digital networks and can benefit from innovative 5G based solutions. Secondly, the deployment of 5G and Gigabit networks should generate new and greater demand for very high quality connectivity and enable new user experience of these technologies, e.g. use of virtual and augmented reality in education and training, tele-operated robotics in surgery, data analytics in precision agriculture and environmental risk management, etc., including in rural and less densely populated areas. These challenging application scenarios are expected to generate a spill-over effect on the digital supply side of the value chain, i.e. the deployment of newer

---

22 https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

23 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en

24 In the context of this Work Programme, a digital global gateway is a telecom backbone infrastructure, typically a submarine cable or a terrestrial backbone, providing backbone connectivity within and between EU member states or between the Union and third countries.

25 See New Agenda for Relations between the EU and Latin America and the Caribbean

generations of innovative technologies and infrastructures. Meanwhile, the EuroQCI initiative is stimulating the development of Europe's industrial ecosystem for quantum communication technologies and systems, which will have major implications for future competitiveness in a highly strategic area. CEF Digital projects are therefore expected to stimulate new synergies across the digital value chain, in particular the bundling of high performance infrastructure, including 5G and Gigabit network deployment, with edge cloud solutions, and help creating new business models for the telecom sector, advancing the creation of a "Connected Collaborative Computing" network ('3C Network')[26].

Strengthen cybersecurity and resilience

Dependencies and vulnerabilities in digital connectivity infrastructures can open the door to increased foreign influence and control over key EU assets as well as over other critical infrastructures and essential services. This in turn can lead to disadvantageous knowledge transfers, disruption of services and long-term economic costs caused by cyber-attacks, and make Europe susceptible to undue foreign influence. Cyber incidents can be either accidental or the deliberate action of criminals, states and other non-state actors. Cyber-attacks on infrastructure, economic processes and democratic institutions, undermine international security and stability and the benefits that cyberspace brings for economic, social and political development.

Therefore, the digital connectivity infrastructures deployed within the Union or between the Union and third countries must meet strong cybersecurity requirements that aim to increase the EU's collective resilience against foreign cybersecurity threats.

As a consequence, on the basis of Article 11(4) of the CEF Regulation, legal entities established in the Union, or in third countries associated to the CEF, but directly or indirectly controlled by third countries or nationals of third countries or by entities established in third countries ("non-EU controlled entities") may not be eligible to participate in some of the actions under this work programme, as set out in the relevant sections below. The networks and backbone infrastructures funded under the CEF Digital work programme are expected to be major enablers for critical services of public interest, including for instance energy, financial services, transport and water supply networks, security, firefighting and police. Furthermore, several actions in this work programme will deploy infrastructures intended specifically to support services and applications that rely on critical processes and/or data. The growing interdependencies of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts to public order and security in the Union. In order to protect society against manipulation of such critical service networks with a disruptive effect and therefore to maintain public order and security, there is a need to protect such critical services from attacks and undue influence exercised through the unauthorised control of the digital infrastructure.

In particular, 5G-related investments have a very high relevance for national and EU security and for ensuring the technological sovereignty of the Union. The EU Toolbox on Cybersecurity of 5G networks, agreed by Member States in January 2020[27], followed up by the

---

[26] See section 3.1 of White Paper - How to master Europe's digital infrastructure needs? | Shaping Europe's digital future (europa.eu)

[27] Commission Communication Implementing the EU Toolbox on Cybersecurity of 5G networks COM(2020)50 of 29 January 2020.

Communication of 15 June 2023 on "Implementation of the 5G Cybersecurity Toolbox"[28], recommends a set of measures, including the assessment of the risk profile of suppliers and implementation of necessary restrictions concerning key network assets and other sensitive assets (government services, critical infrastructures). The above-mentioned Communication indicates that the measures identified in the 5G Cybersecurity Toolbox should be reflected in relevant EU funding instruments, both within and outside of the EU, in accordance with respective governance rules.

A similar approach should be applied to backbone infrastructures covered by this Programme as a potential widespread disruption on these infrastructures would have serious consequences and may impede the well-functioning of the overall network.

In view of the above, participation in calls for proposals under CEF Digital will be subject to the specific security-related requirements set out in section 8 of this work programme.

Climate mainstreaming

Finally, projects funded under this work programme are expected to contribute to the European Green Deal by supporting smart, efficient and sustainable mobility, energy, or agriculture projects, and green ICT infrastructures. The high performance infrastructure supported under CEF, including 5G, will enable significant advances in scalability and energy efficiency, in particular through fibre-based infrastructures, thereby sustainably supporting the goals of the Green Deal. Furthermore, projects will contribute to the EU's long-term decarbonisation commitments, e.g. end-users and businesses in formerly digitally underserved areas will be able to work and benefit from services without commuting.

The "smart" digital infrastructure (i.a. for submarine cables) supported by the global gateways topic (section 4.2) would ensure the monitoring of environmental conditions (e.g. temperature, currents) and marine fauna, underpinning research activities close to the infrastructures, as well as the gathering of information in areas where there are no, or limited means, to observe (e.g. deep waters, arctic region) and analyse data relevant for environmental monitoring, climate change or the observation of endangered species.

Furthermore, the 5G connectivity financed under "5G large scale pilots" (section 3) can enable innovative applications contributing to environmental monitoring and data gathering.

2.3 Overall approach and expected results

Based on Articles 8(4) and Article 9(4) of the CEF Regulation, CEF Digital can support projects contributing, amongst other, to:

1. The deployment of and access to very high-capacity networks providing Gigabit connectivity and 5G systems for socioeconomic drivers;
2. Uninterrupted coverage with 5G systems of all major transport paths, including trans-European transport networks;
3. Significant upgrade or deployment of new backbone networks, including submarine cables, that significantly increase the performance, resilience and capacity of the electronic communications networks within and between Member States as well as between the Union and third countries to address a lack of redundancy, insufficient capacity or competition concerns.

[28] C(2023) 4049

4. The implementation of digital connectivity infrastructures related to cross-border projects in the areas of transport or energy and/or supporting operational digital platforms directly associated to transport or energy infrastructures.

This work programme is designed in a way that facilitates incremental development through appropriate phasing of call topics and priority actions. The actual planning of calls and priority actions depend on technological maturity of the underlying connectivity technology and the related ecosystem (e.g. 5G-based Cooperative Connected Automated Mobility - CCAM), availability of use cases (e.g. for 5G communities), readiness of market players, availability of key enablers (e.g. spectrum licences), etc. It also depends on the evolution of the policy context, in particular with regard to major geo-political and economic developments and the related priorities set at political level. Information days will be organised around each call for proposals in order to raise awareness of policy objectives, foster community building and proposal preparation.

Funding will be provided mostly through calls for proposals (grants), and, to a minor extent, via procurement (for some of the Programme Support Actions)[29]. The execution of the grant calls for proposals and the management of the resulting project portfolios will be delegated to the Health and Digital Executive Agency (HaDEA). The use of financial instruments under InvestEU is also envisaged for some actions where leverage of private funding and scale up are critical factors for the success of the programme.

Wherever appropriate, simplified forms of funding (e.g. lump sums) and/or of implementation (e.g. voucher schemes) may be used in order to simplify the management of the grants.

In addition, the Commission intends to establish under Article 17 of CEF Regulation a CEF Digital Connectivity Blending Facility in order to provide flexibility for the Implementing Partners and efficiency in combining the CEF Digital grants. For this purpose, the Commission will consult Implementing Partners such as National Promotional Banks and Institutions/NPBIs, the EIB Group, the European Bank for Reconstruction and Development/EBRD[30] and private investment banks and funds, in order to define the scope and implementation details of the grant Blending Facility.

CEF Digital will also provide support to Member States and applicants with Programme support actions.

3. Deployment of 5G infrastructures in Europe

In its White Paper on "How to master Europe's digital infrastructure needs", the European Commission shared its vision as regards the transformation of the electronic communications sector and the need to build an ecosystem between actors in different sectors in the value chain (called the "3C Network"), including chips manufacturers, electronic communications network equipment providers, edge and cloud service providers. The ability of people and devices to communicate with each other depends on the widespread availability of high-performing digital infrastructures, which are virtualised and provided as service "in the cloud" to a multitude of applications. Moreover, edge cloud technology is expected to facilitate the presence of computational capacity closer to the users and available in a wide range of devices, robots,

[29] IT development and procurement choices will be subject to pre-approval by the European Commission Information Technology and Cybersecurity Board.

[30] https://www.ebrd.com/home

drones, medical devices, wearables and self-driving cars. Connectivity and computing are therefore converging and the stakeholders in these different segments of the value chain also need to work in close collaboration in order to succeed.

In order for the EU to build industrial capacity in this transition towards cloud-based networks and the integration of telco-edge infrastructures and services, today's connectivity providers must become tomorrow's providers of connected collaborative computing solutions ("3Cs"). This transformation could be supported by the development of a "3C Network" ecosystem between actors in the different sectors and facilitated by exploiting synergies between existing EU funding programmes.

The first CEF work programme supported the deployment of 5G infrastructures underpinning the first use cases in smart communities and along transport corridors, which are also mentioned as potential areas for large-scale pilots in the White Paper. This second CEF work programme contributes, together with other programmes, to the co-financing of projects bundling together the deployment of Gigabit and standalone[31] 5G infrastructure and the integration of edge cloud and computing capabilities with their take-up by vertical sectoral applications.

As an infrastructure deployment programme, CEF Digital supports the deployment of Gigabit and 5G networks which are necessary to implement a Connected Collaborative Computing solution, whereas other programmes such as DEP, RRF or ERDF could be used to deploy the necessary cloud edge and computing capacities as well as the vertical integration of the sectoral applications (use cases). This would be complemented by the R&I dimension under Horizon Europe. Financing in this work programme will be channeled to a number of large-scale "3C network" pilots deploying end-to-end infrastructures and platforms and bringing together players from different segments of the connectivity value chain.

3.1 5G large-scale pilots

Legal base: art. 8.4.a and 9.4.a (for 5G for smart communities) and art 8.4.c, 9.4.c (for 5G corridors) of the CEF Regulation

Indicative budget: 205 million EUR implemented through grants (direct management) and financial instrument (see 6.3 and 7.2)

3.1.1 Background

The White Paper "How to master Europe's digital infrastructure needs?" proposes the development of the "Connected Collaborative Computing" Network ("3C Network"), an ecosystem that spans several segments of the digital value chain, both technically (e.g. integration of 5G standalone networks (5G SA) with edge cloud and computing capacities) and in terms of stakeholder collaboration by bringing together players from different segments of the digital sector and beyond.

[31] A 5G standalone (SA) network entirely relies on 5G technology, i.e. it uses dedicated 5G equipment and functionalities on the edge (RAN) and at the core of the network. 5G SA provides the full advantages of 5G standards/technologies, i.e.: the edge of the network relies on core network functions that are cloud native and service based; supports ultra-low latency; high density of connected devices; network slicing, etc.

The White Paper also puts forward the idea of launching *large-scale pilots* that set up end-to-end integrated infrastructures and platforms for telco, cloud and edge. These pilot infrastructures could enable innovative technologies and applications for various use cases. For instance, by combining advanced 5G standalone systems with other technologies, such as edge cloud, HPC, Artificial Intelligence (AI), Virtual Worlds and Web 4.0, it could be possible to support innovation and better services in such application fields as transport, healthcare, education, agriculture and manufacturing.

For the purpose of the present work programme, 5G large-scale pilots are defined as the combined deployment and take-up of 5G standalone networks, including their integration with edge computing capacities, that meet the very stringent requirements of innovative use cases in terms of very-high reliability, security, low latency, communication symmetry and high throughput.

The innovative use cases considered under the present work programme are[32]:

1. 5G SA deployment to improve the connectivity supporting the activity of socio-economic drivers, i.e. entities which by their mission, nature or location can directly or indirectly generate important socio-economic benefits for citizens, business and local communities. These socio-economic drivers include a variety of entities like schools, universities, transport hubs such as train stations, ports and airports, hospitals, security and public safety services, research centers, local governments, as well as digitally intensive enterprises.

2. 5G SA connectivity and computing continuum to be deployed along major terrestrial transport routes, integrating edge cloud capacities, with the view to enable innovative Connected and Automated Mobility (CAM) services, advanced digital transport and logistics applications, emergency services, as well as a broad range of digital services for the vehicle, the driver (e.g. Advanced Driver Assistance Systems, ADAS), the passengers and other relevant players (e.g. health monitoring services); ,5G SA connectivity infrastructure may also enable use cases for automated train and waterway operations with the goal to make these transport infrastructures more secure, efficient and sustainable.

To accelerate the deployment and take up of 5G, the first CEF Digital work programme supported these two groups of use cases through two complementary topics: 5G Smart Communities and 5G Corridors. The resulting portfolio provides a good basis of best practices[33] and the related community of 5G suppliers and adopters.

The next step is to scale up this portfolio and broaden its scope by involving more stakeholders along the 3C Network value chain, pursuing higher level of performance of networks. This will allow defragmenting the EU supply and creating the critical mass needed to compete at global level, which is one of the main challenges identified in the White Paper and also in the consultation with some private investors[34] to advance the single market for telecommunications.

3.1.2 Objectives

---

[32] See Projects of Common Interest defined under Article 8.4(a) and (c) of the CEF Regulation

[33] The portfolio includes also support actions aiming to facilitate the sharing of best practices, promoting the integration of 5G with edge cloud capacities, etc.

[34] https://digital-strategy.ec.europa.eu/en/news/commissioner-breton-calls-more-private-investment-connectivity-infrastructure

The objective of the topic "Large-scale 5G pilots" is to deploy large-scale 5G SA infrastructures integrating connectivity and edge cloud capacities along the "3C Network" value chain. Each pilot is expected to maximise the number of use cases enabled by 5G systems in areas such as mobility, transport, logistics, emergency services, education, healthcare, agriculture, manufacturing, etc., targeting urban, rural and cross-border contexts.

The investment strategy consists in bringing together the demand side of the individual projects (vertical sectors' use cases) with an EU-wide supply chain revolving around the Connected Collaborative Computing Network ecosystem. The CEF Digital support would take place in two phases:

1) Grant call for proposals supporting 5G SA connectivity for an indicative number of 4-5 large-scale pilots involving one or more of the above-mentioned use cases.

2) Top-up to InvestEU operation to leverage private investments to support more 5G SA projects with greater scale and scope, eventually targeting 5G SA applications for digitally intensive enterprises and industry.

The 5G SA large-scale pilots should be designed in a way that, with adaptations due to possible different requirements, they can be replicated across Europe, for instance under other funding programmes such as ERDF, EAFRD or national investments. Projects may be preceded by inception studies or best practices funded in earlier calls under this programme, or may be based on any other preparatory work funded under other programmes (such as R&I under Horizon Europe).

5G SA large-scale pilots funded under this action are expected to deploy 5G infrastructures delivering leading-edge connectivity characteristics e.g.: symmetric gigabit performance, high-user-density, ubiquitous coverage (e.g. to connect IoT devices), low latency and very high reliability. They will contribute to the integration of devices, networks, cloud and edge computing, and communication capabilities for telco edge cloud deployments to realise a ubiquitous mesh of computing and communication resources. Where necessary, they should bundle the deployed 5G networks with a cloud-to-edge middleware stack[35] capable of supporting the data-intensive use cases and applications designed for a multi-purpose context (5G corridors and/or 5G applications for socio-economic drivers).

The 5G SA large-scale pilots should demonstrate the benefits gained in specific vertical applications, following the evolution from current electronic communications networks towards virtualised and cloud-native network functions and distributed telco edge cloud, opening new opportunities to Europe's key industries.

The 5G SA large-scale pilots will stimulate the wider and faster deployment and take-up of 5G across Europe, while providing the foundation for the development of "lead markets" for 5G and edge cloud systems, possibly relying on technologies and standards developed under other EU programmes, in particular the Digital Europe Programme and Horizon Europe.

The large-scale best practices *beacons* will cover at least four different use cases. Cross-sector synergies between multiple use cases are expected to be enabled by the 5G SA deployments supporting the local smart communities and between multiple sites distributed across multiple countries and regions.

[35] See topic 2.2.1 of the 2021/2022 work-programme of the Digital Europe Programme

3.1.3 Market failure requirements and funding rates

The CEF Digital grant does not constitute state aid, however, it must be consistent with the state aid framework from the outset. In particular, the grant should be used to address market failures or sub-optimal investment situations of a given use case, in a proportionate manner, without duplicating or crowding out private financing, in particular where actions are not commercially viable but where they have a clear Union added value.

Market failures exist when the private sector fails to address demonstrated end-users' needs. This may also occur when connectivity is provided at an insufficient level of quality or at excessive prices possibly due to insufficient competition. Market failures are often linked to the geographical areas concerned (e.g., cross-border sections of a transport corridor, rural vs. urban, etc.)[36]. State intervention should be used where it is impossible to address such market failure through less distortive policy and measures.

5G Corridors use cases

Concerning the 5G corridors use cases, the large-scale 5G SA pilots can be deployed along key European transport paths including, but not limited to the indicative list of 5G corridors in the Annex part V of the CEF Regulation. The priority will be to support investment in cross-border sections involving two or more Member States, with a co-funding rate of 50%.

The supported cross-border section of a 5G corridor must cross at least one Member State border and its length on both/all sides of the border may vary, depending on the national circumstances including the means of transport, the geographic situation and the maximum size of the project/EU funding indicated in the call. For Member States with large highway and rail networks (e.g., +/-1000 km), cross-border segments of 5G corridors may represent up to 15% of the corresponding combined length of TEN-T comprehensive corridors, per mode of transport (e.g., road, rail) in a Member State[37]. If justified by the project objectives and in the absence of 4G coverage or where 5G networks cannot support services addressing evolving end-users' needs′), longer cross-border sections can be considered. For Member States with significantly smaller highway and rail networks, similar conditions for adjusting the scale of corridor lengths as described above may be considered for cross-border sections funded under CEF, potentially going beyond 15%[38] of the corresponding TEN-T sections of the 5G corridors in a Member State, provided that a market failure is demonstrated.

For Member States without intra-EU borders due to their geographic situation, or with no relevant sections of TEN-T corridors going across their intra-EU borders, actions for the 5G coverage of intra-national sections of corridors with insufficient mobile coverage suitable for CAM services, or in sections without 4G coverage,[39] are eligible. Under the same conditions, 5G corridor deployment projects crossing the border of a third country or terminating at a port with maritime connections to other EU Member States are also within the scope.

---

[36] See section 2 of the Commission Notice on the notion of State aid as referred to in Article 107(1) of the Treaty on the Functioning of the European Union, ‘OJ C 262, 19.7.2016

[37] An indication of the overall length of TEN-T corridors within a Member States, per mode of transport, can be found in annex of the WIK Consult study on ”Investment and funding needs for the digital Decade targets” conducted for the European Commission

[38] See footnote 9

[39] See section 4.2 of the Commission Notice on the notion of State aid as referred to in Article 107(1) of the Treaty on the Functioning of the European Union

Beyond cross-border sections, actions also addressing the coverage of intra-national sections of corridors with demonstrated market failures (which are supported by CEF Digital at a 30% funding rate) can complement national deployment initiatives, including those funded under other programmes in line with State aid rules. Such intra-national sections funded under other programmes may also complement the cross-border sections funded in the first phase of the CEF programme.

In both cases, *i.e.* cross-border sections with or without intra-national sections, the projects supported by CEF Digital will not undermine coverage obligations of the mobile network operators stemming from spectrum licence conditions. Should the same area be considered for deployment, the applicants will demonstrate that the service requirements fulfilled by the CEF funded project for future CAM services along the section concerned are going beyond the requirements of the coverage obligations, in particular service continuity with guaranteed quality of service, such as data capacities offered per vehicle, speeds, latency, or other service enablers. In any case the costs related to the fulfilment of coverage obligations under spectrum licences will not be eligible for financing under CEF Digital.

Funding of projects that foresee the sharing of both passive and active infrastructure, e.g. through wholesale offers, is encouraged to increase the efficient use of funds provided under this programme. The sharing by network operators of passive, but also active equipment (e.g. through a neutral host model) should aim at substantially reducing network deployment costs and at the same time at facilitating the energy efficient use of resources when deploying and operating the 5G SA infrastructures. In addition, wherever possible, existing infrastructures such as ducts, fibre, equipment shelters, power supply and utility poles should be used[40].

Large-scale pilots for advancing the 3C Network should demonstrate the benefits gained from the deployment of 5G corridors and their integration with edge and cloud infrastructure through the design of the supporting network architecture and its evolution towards the computing continuum, with the view to enable the development of innovative applications and use cases in the field of connected and automated mobility (e.g. solutions for multi-modal mobility).

5G smart communities use cases

Concerning the use cases involving smart communities, the CEF will co-fund the deployment of the connectivity infrastructure elements required by vertical innovative applications, in rural, urban or suburban areas, which are not already available on the market. The access to an existing backhaul Gigabit network close to the location where the 5G-supported project will be deployed is a prerequisite. The project may however include a limited investment to complete the access to such Gigabit backhaul.

Large-scale pilots for advancing the 3C Network would demonstrate the benefits gained from the evolution of the current network infrastructures towards virtualised and cloud-native ones. This would include the development of innovative applications in European vertical sectors as well as social innovations, like new operation models and roles for different stakeholders and public services, as well as enabling new business models and opening new opportunities to Europe's key industries.

Projects would need to demonstrate the soundness of the financing for the remaining parts of the project (infrastructure or otherwise) enabling the intended 5G use cases (e.g. end-user

[40] See Regulation (EU) 2024/1309 of the European Parliament and of the Council of 29 April 2024 on measures to reduce the cost of deploying gigabit electronic communications networks, the "Gigabit infrastructure act"

devices, sensors, connectivity subscriptions…), which are not eligible for support under the CEF Regulation and should therefore be supported by other programmes or the consortium's own contribution. Projects would also need to demonstrate that the infrastructure will be operated in a forward-looking and future-proof way based on state-of-the art protocols and standards, such as IPv6, and that they are located in areas where no 5G network is providing services addressing evolving end-users' needs.

The beneficiaries will be operators that will deploy 5G SA networks and provide access to 5G services to socio-economic drivers; the socio-economic drivers should jointly apply together with the above-mentioned operators and contribute to describe the 5G innovative use case(s) they plan to develop. Eligible cost items may include 5G radio equipment and – where necessary for installation of additional base stations for densification – the passive infrastructure. Priority will be given to projects that can demonstrate more than one 5G-based use case relying on the same 5G SA network.

In line with the CEF Regulation (see recital 40), internet services and software services that make use of the digital infrastructure are not in scope of CEF financing. However, the Granting Authority will assess the innovative aspects of the use case in its evaluation.

The maximum CEF co-financing rate will be 75% of the CEF-eligible costs as a general rule. The use of the financed 5G infrastructure to provide 5G services to users other than socio-economic drivers[41] may be subject to specific conditions in the calls.

In general, the requested overall co-funding and the number of socio-economic drivers that will benefit from the 5G service will be considered as part of the assessment of the catalytic effect of EU assistance and the economic impact award criteria.

In case of co-funding from national or shared management funds (including Cohesion Policy funds), State aid rules within the meaning of Article 107(1) TFEU apply (see section 10 for details). However, if the projects concern the provision of dedicated 5G SA connectivity to enable highly demanding use cases by socio-economic drivers that are public administrations or public or private entities using it for the operation of SGIs (services of general interest) or of SGEIs (services of general economic interest) and that such connectivity is necessary for discharging those services, such co-funding will either not constitute State Aid (when no economic activities are supported) or can be considered compatible with the TFEU without the need of its notification and approval by the Commission, if compliant with the SGEI Decision.

3.1.4 Implementation 2024 -27

The timetable below describes the foreseen distribution of calls and the type of actions to take place over the remaining CEF Digital funding period from 2024-2027.

5G deployment calendar				
	2024	2025	2026	2027
Implementation mode	Fixed deadline call	Top up to InvestEU – Blending operation		
5G Large-scale pilots	Deployment works	Deployment works		

[41] Socio economic drivers is defined Art 2(s) and, more in detail, in Recital (37) of the CEF Regulation

The 2024's call for large-scale 5G pilots under CEF Digital will consist in deployment works only (i.e. no inception study projects). Proposals should be able to rely on the results of CEF-funded inception studies or best practices conducted under Calls 1-3, or on any other relevant programme. The deployed 5G infrastructure should address several use cases.

For the remaining period, 2025-2027, a shift of implementation mode as part of Invest EU will enable to submit proposals in a more flexible manner. In particular, project consortia will be able to seek for equity financing from financial institutions benefitting from the InvestEU guarantee at any time. The list of financial institutions, chosen by the Implementing Partner with which the Commission will sign a guarantee agreement, will be public and regularly updated.

Benefits and expected outcomes - including EU added value

The projects funded under this topic are expected to accelerate the deployment of 5G standalone services across the Union, thus directly contributing to the achievement of the Digital Decade connectivity goals and the other Digital Decade targets. The benefits of the actions depend also on the innovative use cases addressed.

By closing deployment gaps and removing capacity bottlenecks and technical barriers, the deployment of 5G corridors along the TEN-T networks will contribute to strengthening the social, economic, and territorial cohesion in the EU.

The projects would deliver uninterrupted coverage with service continuity meeting relevant quality of service requirements over the entire range of the corridor section. In the case of 5G road corridors, this will enable the provision of a broad range of 5G-enabled CAM services, including for rail and waterways, and, where appropriate (i.e. focusing on hotspots e.g. traffic junctions, roadworks, etc.), complementary safety-related services based on existing direct short range communication technologies, such as 4G LTE-V2X and ITS-G5 as well as their successors, compatible with existing deployment and supporting complementarity between existing and future infrastructure deployments.

The deployed infrastructures may contribute in the future to the improved safety of road/rail/waterway operations (e.g. Intelligent Transport Systems (ITS), Future Rail Mobile Communication System (FRMCS), River Information Services (RIS)) and enable 5G services for multiple application domains.

Projects may also contribute to the objectives of the Commission's strategy on the mobility of the future[42] in terms road safety, optimised road traffic and reduced CO2 emissions and traffic congestion, as well as the competitiveness of the European telecom and automotive industries.

5G smart communities use cases are expected to accelerate the take-up of 5G connectivity for the provision of innovative services and contribute to a wider deployment and take-up of 5G at the same time. Such services can help reboot the overall economy, as well as support the transition towards the smart provision of services in line with the objectives of the European Green Deal. 5G SA innovation can include:

- IoT infrastructure and community services that require a flexible, low-latency, reliable, high-user-density connectivity infrastructure, e.g. through a combination of fibre and wireless connectivity (5G, small cells, and Wi-Fi) that is IPv6 enabled.

[42] "On the road to automated mobility: An EU strategy for mobility of the future", Communication of 17 May 2018, COM(2018) 283 final

- 5G-and edge cloud based use cases that leverage new 5G characteristics, e.g.: higher bandwidth and ubiquitous coverage (eMBB), ultra-low latency (uRLLC), massive machine-type (mMTC)[43].
- Process and data innovations that require connectivity infrastructures with advanced service features, e.g. quality of service guarantees enabled by edge computing facilities and support by network slicing.
- Projects that rely, where relevant, on open, disaggregated, and interoperable technology solutions and contributing to the emergence of a European ecosystem of 5G suppliers.
- Leveraged impact on investment in 5G and edge cloud for vertical sectors by all types of public and private investors.
- Positive spill over effect to Digital Decade indicators not only for "digital infrastructure" but also to other use cases in Digital Skills, Digital Transformation of Businesses and Digital public Services.

In addition to the support for local innovation, the EU added value is also based on the dissemination and the early adoption of concrete 5G SA use cases that will contribute to gaining insights and increasing maturity for 5G applications in different sectors. It is expected that this will generate spill over effects across the Connected Collaborative Computing value chain, in particular by nurturing consumer-supplier synergies between actors working on converged, cloud-enabled connectivity and computing infrastructures.

Governance, operations and stakeholder involvement

Each proposal must be supported by the relevant competent authorities involved in the deployment of 5G SA network infrastructure in the area where the deployment is foreseen to take place, e.g. along a transport path on the two sides of the border, at national and/or regional and/or local levels.

The deployment of 5G corridors has been identified as a Multi-Country Project (MCP)[44] in the Path to the Digital Decade Policy Programme. In addition, the Smart Networks and Services Joint Undertaking (SNS JU) provides guidance in reviewing the 5G Strategic Deployment Agendas for both road and rail, with a particular focus on deployment scenarios, cooperation models, and regulatory incentives. Therefore, each proposal must foresee cooperation with relevant Programme Support Actions funded under CEF Digital as well as relevant working groups and fora of the Smart Networks and Services Joint Undertaking (SNS), which is expected to provide strategic input to the implementation of the CEF Digital programme with the support of dedicated CSA projects.

Beneficiaries will be asked to share their knowledge, achievements and lessons learnt, including in the context of Support Actions, in order to demonstrate to users the benefits of 5G SA by providing concrete examples of 5G based use cases for socio-economic drivers. Sharing of project information (technical, financial, procedural…) will be essential for project replication (e.g. requirements elicitation, use of open technical standards and interoperable solutions, e.g. Open RAN) scoping and templates for financial sizing, using of complementary funding sources, etc…). This should facilitate the spillover effect of CEF Digital investments across the Union.

---

[43] eMBB: enhanced Mobile Broadband; URLLC: Ultra-reliable low-latency communication; mMTC: Massive machine type communications.

[44] MCPs aim to help Europe meet its digital targets and objectives through large-scale projects that no one Member State could achieve alone Europe's Digital Decade | Shaping Europe's digital future (europa.eu)

Beneficiaries will be also asked to cooperate with the ongoing CSA projects (or follow up actions) that support and enhance 5G edge and distributed cloud integration for European 5G corridors and 5G smart communities.

The Broadband Competence Offices (BCO) Network will also play an important role in helping to overcome the challenges related to the envisaged deployment and take-up of 5G SA, e.g. by conveying knowledge and good practices as well as to foster local, regional and cross-border collaboration.

Specific measures addressing green policy objectives, in particular in terms of reducing the carbon footprint, should be taken into account in the governance and operation of the deployed infrastructures.

The beneficiaries should demonstrate that they have access to use case infrastructures and capacities, including relevant radio spectrum resources (in case of passive infrastructure deployment, either directly or contractually with 5G spectrum band owners). They should provide reassurances as to the operation of the service beyond the specific areas (e.g. 5G corridor section) supported by CEF, and beyond the time horizon of the CEF-funded project, in view of the long-term development of the infrastructures (e.g. more extensive pan-European corridor network, replication of a smart community use case, etc.).

Proposals concerning corridors would need to demonstrate how the infrastructure is intended to be made available for other service providers or users inside or outside the consortium, e.g. providing access on a non-discriminatory basis to all operators that hold relevant spectrum licenses in the territory concerned, while keeping in mind the respective levels of risk undertaken. The provision of open, fair and non-discriminatory wholesale access is a key consideration for ensuring consistency with State aid rules. Compliance with State aid rules must be ensured if State aid is involved in corridor projects. Proposals may include limitations to third party wholesale access to active network elements for the provision of FRMCS or ITS if justified on security grounds.

Proposals should define post-project ownership and describe the mechanism(s) set in place for long term cooperation and sustainability. The functional and operational relationship(s) between the different participants in the value chain for the provision of digital services should be clearly defined.

5G corridors proposals should describe how the project will be used for the provision of Connected and Automated Mobility (CAM) or FRMCS services along the entire corridor. Any arrangements for network sharing options to ensure uninterrupted provision of services along the entire corridor should be clearly defined.

Project consortia targeting 5G corridors use cases should be composed of at least two private undertakings and/or public bodies taking responsibility as regards ownership, operation and use after the project.

The participation of mobile network operators, operators deploying infrastructure and associated facilities such as tower companies, telecom backhaul operators, road operators – including transport authorities, rail infrastructure managers, waterways infrastructure managers, automotive manufacturers, mobility and security service providers – is encouraged, when and if appropriate. The consortia may include public authorities in the field of transport.

Proposals addressing 5G Corridors use cases should include a solid implementation plan, including access to services and applications with social, economic, and environmental benefits extending beyond the financing Member States, the beneficiaries or telecoms sector, as well as a commitment to maintain the infrastructure beyond the lifetime of the project. Proposals should

also include a plan to enable uninterrupted service beyond the cross-border sections funded. Such plan should include the same security conditions that apply to the CEF-funded project.

Digital security requirements

Due to the sensitivity of the 5G infrastructures and data needed to implement the use cases and their relevance for security and public order (e.g. safety-related services such as automated driving, traffic management, functioning of healthcare, environmental security, etc. and their relevance to public order and security), there is a need to ensure cybersecurity of infrastructures funded under this action.

The dependence of many critical services on these infrastructures would make the consequences of systemic and widespread disruption particularly serious. For instance, if a 5G corridor infrastructure is compromised, problems affecting public order and security may arise such as perturbed or even closed traffic, traffic accidents, collisions, the spread of dangerous misinformation related to traffic conditions or other, etc. Impact could also extend to supply of critical inputs such as energy, raw material, food, etc.

Furthermore, the interconnected and transnational nature of the infrastructures underpinning the digital ecosystem, and the cross-border nature of the threats involved, mean that any significant vulnerabilities and/or cybersecurity incidents concerning these infrastructures happening in one Member State would affect the Union as a whole.

A cyberattack perpetrated, for instance, through or against the 5G infrastructure connecting medical equipment and devices used for the monitoring or control of vital physiological functions may endanger the life of patients wherever they are, at the hospital, in the ambulance or at home. The fault of the network infrastructure caused by a cyberattack could paralyse the functioning of public utilities such as gas or water in an entire area, but also could cause the malfunctioning of equipment to monitor and control critical safety systems such as, for instance, those used in power plants or transport.

Therefore, the 5G infrastructures supporting those use cases and applications must comply with the strictest security principles, including the necessary controls concerning the participating entities. This will significantly reduce the risk that cyberattacks are perpetrated against users, businesses or public institutions, which could have severe consequences for public order and security.

Applicants for this topic will have to comply with the conditions set out in section 8.3.

As provided in section 8.4, proposals submitted to this action will also have to involve only suppliers suitable for the deployment of secure systems, as they take a critical role for the security of critical communication systems such as the one needed for safety-related CAM services, i.e. critical services directly impacting public safety such as automated driving, traffic management, healthcare, environmental control, etc.

In the context of 5G SA networks, the role of suppliers has been identified in the EU coordinated risk assessment and the EU Toolbox on 5G cybersecurity as of particular relevance for cyber-security[45]. In particular, the Toolbox recommends assessing the risk profile of suppliers and applying appropriate restrictions- including necessary exclusions- for key assets considered as critical and sensitive.

[45] COM(2020)50 of 29 January 2020.

This is notably the case for suppliers of equipment (including hardware and software) that implement core network functions, network management and orchestration functions, as well as access network functions.[46]

The reason is that the deployment, operation or management of active and/or passive components of the infrastructure may entail security risks for the Union, for instance if critical data is shared with un-authorized parties or un-authorized parties are able to influence the use of such data or components and potentially compromise the integrity or availability of the deployed infrastructure. Such risks are more probable if the active components and related services are sourced from suppliers established in or controlled from third countries[47].

4. EU connectivity backbone infrastructures

4.1 Quantum communication infrastructure - The EuroQCI initiative

Legal base: art.8.4.d and 9.4.d of the CEF Regulation

Indicative budget: 90 million EUR, implemented through grants, direct management (see 7.2)

4.1.1 Background

Europe's critical infrastructures and sensitive communications and data are vulnerable to cyber-attacks and other security threats. Advances in supercomputing and the advent of quantum computing may soon undermine modern encryption systems, threatening the security of transmitted data and secure access to remotely stored data in the long term. To keep the EU's government data and critical infrastructures safe in the medium and long term, the EU must develop new and more secure forms of encryption and devise new ways of protecting the EU's critical communication and data assets.

In order to address this challenge, and as set out in the Joint Cybersecurity Strategy,[48] the Commission is working with Member States and the European Space Agency towards the deployment of a secure quantum communication infrastructure (EuroQCI) spanning the entire EU, including its overseas territories, to meet the needs of national governments and public services of general interest. The EuroQCI will provide an unprecedented way of securing communications and data, integrating innovative and secure quantum products and systems into conventional communication infrastructures, by enhancing them with an additional layer of security based on quantum physics.

The EuroQCI will consist of a terrestrial component relying on new and/or existing fibre communication networks linking strategic sites at national and cross-border level, complemented by a space satellite component to cross-link and cover the entire EU. As it will contribute to the security of the Union, , CEF Digital will encourage the use of EU technologies.

The EuroQCI's deployment is partly supported by the Digital Europe Programme and by IRIS². CEF Digital will support the interconnection of national quantum communication infrastructure networks between neighbouring countries, as well as the interconnection of the EuroQCI's

---

[46] See p. 5 COM(2020) 50 final - Secure 5G deployment in the EU - Implementing the EU toolbox. See alsoCOM(2023)4049, "Implementation of the 5G cybersecurity toolbox"

[47] According to the EU coordinated risk assessment of 5G networks, the risk profiles of individual suppliers can be assessed based on several factors. These factors include the likelihood of interference from a third country. This is one of the key factors specified in paragraph 2.37 of the EU coordinated assessment.

[48] JOIN(2020) 18 final

ground and space segments. Since 2023, EuroQCI has been part of IRIS², the Union Secure Connectivity Programme[49], and it will be gradually integrated to offer services under IRIS².

4.1.2 Objectives

The first services provided by EuroQCI will be based on quantum key distribution (QKD), which uses the properties of quantum physics to establish a secure encryption key at each end of a communications line in order to protect against vulnerabilities, namely eavesdropping. The first phase of the EuroQCI infrastructure deployment is focused on the deployment of terrestrial backbone components. It should aim for solutions providing end-to-end security.

CEF Digital actions to co-fund the terrestrial backbone network components will be complementary to those developed through the Digital Europe Programme, and should be focused on supporting cross-border links between two or more national quantum communication networks in Member States, and/or linking the EuroQCI's terrestrial and space segments. While it is not permitted to use RRF funding as co-funding for activities funded under CEF Digital, Member States are invited to complement actions under CEF Digital and the Digital Europe Programme with actions funded from the RRF. Actions funded under IRIS² will further complement these and will, in particular, cover activities to support the further deployment of the EuroQCI's space and terrestrial infrastructure.

4.1.3 Implementation

The following requirements have been set for the co-financing for the EuroQCI under CEF Digital for the needs of EU's national governments and critical infrastructures supporting services of general interest ("critical infrastructures"):

- The deployment of the first cross-border quantum terrestrial backbone networks for interconnecting neighbouring national quantum communication infrastructures across borders, including, if necessary, through the deployment of "trusted nodes" (i.e., secure access points to the network which make it possible to link distant sites securely). Addressing the coexistence of QKD with conventional communications technology is encouraged. Solutions should rely on state-of-the-art interoperability methods and standards and address scalability, upgradability and end-to-end security.
- Interconnection with the EuroQCI's space segment,[50] which will be implemented via the optical ground stations and related ground equipment, serving as an interface between the EuroQCI's space components and its terrestrial fibre network.
- Where relevant, the provision of fibre links between the EuroQCI and a pan-European network of Security Operation Centres (SOCs).

The management of encryption keys between all elements of the EuroQCI in an end-to-end manner should also be considered. This would include the actions needed at the level of telecommunications networks to manage these keys efficiently and securely and ensure their transmission to recipients.

The key performance indicators for this topic will be the number of (terrestrial) cross-border quantum interconnections and the number of optical ground stations deployed.

[49] Regulation (EU) 2023/588

[50] Interconnection with the demonstrator satellite Eagle-1, and preparation for interconnection with the EuroQCI first generation satellite (developed under the ESA SAGA programme).

Grants call planning: European Quantum Communication Infrastructure				
Type of Call	2024	2025	2026	2027
Works	√	-	-	-

Benefits and expected outcomes - including EU added value

The CEF Digital support for EuroQCI will:

- Enable reliable and resilient transmission of sensitive communications and data between public authorities, research entities and critical infrastructures in Member States, including outermost regions and OCTs;
- Boost Europe's capabilities in developing quantum-secure optical communication networks and its capacity to protect critical public infrastructures by securing their communications and data, especially those that cross national borders and serve more than one Member State;
- Promote quantum-based secure networks and the emergence of a new ecosystem that would enable a large market uptake. This will ultimately support the growth of a pan-European quantum industry that would develop new, innovative systems and technologies critical for the EU's digital strategic autonomy.

Operations and stakeholder involvement

Funding will be open for consortia, which can include, for example, operators, authorities, investors and suppliers.

Specific eligibility requirements

Proposals should define the post-project ownership of the infrastructure and describe the mechanism to be used to provide services, as well as the operational relationship(s) between the different participants in the value chain for providing services.

Security requirements

Quantum communication is an emerging technology of global strategic importance that will bring a change of paradigm in communication capacities. It has extensive uses in security applications and dual-use technologies, and will enable the EU and its Member States to safeguard sensitive governmental data and infrastructures against potential interference. Therefore, in order to safeguard the EU's security interests, it is necessary to achieve and maintain European capacities in this area and ensure the security of these critical supply chains.

In the context of this topic, the deployment, operation or management of services based on quantum communication technologies (during and after the lifetime of the projects) may trigger security threats for the EU; for instance, if critical data were shared with unauthorised parties or unauthorised parties were able to influence the use of such technologies or infrastructure. For the reasons above, applicants under this topic will be subject to Article 11(4) of the CEF Regulation, as described in section 8.3.

Regarding the equipment and technologies to be deployed, in order to be eligible, all proposals must include security declarations by participating entities and commitments, as described in section 8.4.

4.2 Backbone connectivity for Digital Global Gateways

Legal base: art.8.4.d and 9.4.d of the CEF Regulation

Indicative budget: 542 million EUR, implemented through grants (direct management), blending facility and financial instrument (see 6.2, 6.3 and 7.2)

4.2.1 Background

Backbone connectivity including submarine cables plays an essential role in ensuring high capacity and high performance (in terms of resilience, security, redundancy and latency) of digital connectivity throughout the EU, in particular for the Outermost Regions (ORs[51]), islands and Member States with coastlines, as well as the Overseas Countries and Territories (OCTs[52]). Those infrastructures are also crucial in providing the efficient international connectivity of strategic importance such as linking the EU with its trading and research partners around the globe and essential to reach our connectivity and climate change commitments.

Submarine cables are central in the reflection about the future digital infrastrucure needs of the Union[53]. At various stages, Member States have stressed the importance of planning and investing in reinforcing the security and resilience of EU's backbone network, particularly submarine cables. In the Recommendation on "Secure and Resilient Submarine Cable Infrastructures", the Commission recommended specific actions to assess and improve coordination between the Union and its Member States as regards the security and resilience of existing and new submarine cable infrastructures, calling for jointly supporting the deployment or significant upgrade of such infrastructures.

The Recommendation introduces the concept of Cable Projects of European Interest ('CPEI') and announces the setup of an Expert Group composed of Member States authorities to advise the Commission on the cable infrastructures to be prioritised in order to strengthen the resilience and security of the Union's backbone connectivity. CEF Digital is one of the funding instruments mentioned in the Recommendation to support the deployment of CPEIs, in line with the legal base of the programme. Synergies with NIS2[54] and CER[55] Directives are also called for in the Recommendation.

Recent geopolitical tensions, such as Russia's war of agression against Ukraine and the conflicts in the Middle East, raise concerns about the security and resilience of critical infrastructures potentially affected by those conflicts. The security and resilience of those critical infrastructures, including, where appropriate, the diversification of the routes is essential for assuring the backbone connectivity and consequently some important geopolitical interests of the Union. It is of utmost importance to ensure that the European Union is connected with top

---

51 Outermost Regions https://ec.europa.eu/regional_policy/en/policy/themes/outermost-regions/

52 Overseas Countries and Territories https://ec.europa.eu/international-partnerships/where-we-work/overseas-countries-and-territories_en

53 White Paper - How to master Europe's digital infrastructure needs? | Shaping Europe's digital future (europa.eu)

54 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

55 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992

quality infrastructure available in all populated areas, including those territories that may be affected by geopolitical tensions.

CEF Digital will support projects that deploy this backbone connectivity in line with Articles 8(3)d and 9(4)d of the CEF Regulation, regarding the deployment of new or significant upgrades to existing backbone networks, which contribute significantly to the increased performance, resilience and very high capacity of the electronic communications networks.

Pursuant to the principle of technological neutrality, this backbone connectivity can be provided with the best suited technology, e.g. including submarine cables, terrestrial backbones or satellite ground stations and their possible inter-connections.

This work programme will support the deployment or significant upgrade of backbone networks, particularly submarine cable infrastructures via Cable Projects of European Interest ('CPEI'), that meet one of the following conditions:

(1) they involve at least two Member States;
(2) they connect a Member State with one or several of its islands, outermost regions, or oversea countries and territories;
(3) they establish or significantly enhance connectivity between one or several Member States and third countries, including accession and neighbourhood countries, directly, or indirectly via other cable infrastructures linked to the Union.

4.2.2 Objectives

The objective of this action is to deploy strategic networks contributing to strengthening the resilience, security and quality of connectivity within the Union, as well as with third countries. This action includes the deployment of submarine cables, terrestrial backbones, satellite infrastructures and connectivity to internet exchange points in demonstrated market failure areas.

By supporting the targeted deployment of such connectivity, CEF Digital will have a positive impact not only on increasing the connectivity capacity, but also on facilitating commercial offers of connectivity.

CEF Digital will support the deployment of new cables as well as investments in related deployment, maintenance and repair facilities, that the market alone will not carry out. These investment must concern routes (within Member States, between Member States, and between the EU and third countries), including Outermost Regions and other remote territories, where:

- There is a lack of the necessary security and redundancy to guarantee the reliability and resilience of backbone connectivity that can ensure adequate, safe and secure connectivity within the Union and with overseas territories and third countries; or
- Existing infrastructures cannot satisfy demonstrated demand to provide affordable and adequate services in line with the EU connectivity objectives for 2030[56] taking into account, among others, the lack of sufficient capacity, identified resilience gaps, excessively high prices that discourage take-up and innovation compared to prices charged for the same services in more competitive, but otherwise comparable areas or regions.

[56] As defined in the Communication "2030 Digital Compass: the European way for the Digital Decade" COM(2021) 118 final

- There is a lack of the necessary redundancy to guarantee the reliability and resilience of international connectivity that can ensure adequate, safe and secure connectivity for the Gigabit society.

CEF Digital will not support projects that concern routes already served by at least two present or credibly planned submarine cables, as it is expected that redundancy is addressed by the two infrastructures. However, on the grounds of EU security and resilience considerations, the CEF intervention is justified if a route is not served by at least two existing or credibly planned infrastructures that fulfil the conditions set out under Section 8. In projects concerning territories (e.g. small islands or territories with limited population density) where backbone connectivity needs can be satisfactorily served using satellite infrastructure, the presence of such infrastructure will be taken into account when assessing the lack of redundancy.

In case of co-funding from national funds (including Cohesion Policy funds) State aid rules within the meaning of Article 107(1) TFEU apply (see section 10 for details).

4.2.3 Implementation

Access to backbone connectivity in EU Member States differs significantly. In certain regions it may also contribute to imbalances in the prices of services, both for network operators in these regions, as well as their inhabitants.

In particular the connectivity situation for Member States that are themselves islands and/or have islands as part of their territory differs significantly from other Member States. For remote territories such as the EU's Outermost Regions, islands, and Overseas Countries and Territories, the commercial prices and other conditions of connectivity may hinder the full participation in the digital European economy.

In such areas, it can be demonstrated that market forces may not provide answers to all of these challenges, and that certain areas will remain underserved or experience higher prices in terms of access to backbone connectivity. For these reasons, the evaluation of backbone projects under this section shall prioritise those offering the higher level of wholesale access to third parties. Besides the requirements to fulfil the CPEI criteria stemming from the Recommendation, proposals must therefore include a description of whether, or how they intend to provide wholesale access to third parties. Among others, this description may indicate the range of access products, the duration of the access, the method to determine access prices, the business model implemented (wholesale only or others). These elements will be taken into account in the evaluation of the proposal, in particular to assess its expected impact on competition as well as the contribution to the resilience and security of EU's backbone.

Pursuant to points 26 and 27 of the Recommendation, applicants, in agreement with the relevant Member State authorities, are encouraged to demonstrate in their proposals that:

(a) the proposal aims to fill a gap in backbone infrastructures, supported by evidence (e.g., mapping of resilience gaps), which may address the need to establish new or alternative secure routes, or to increase the capacity and resilience of existing infrastructures;

(b) the proposal contributes to a significant increase of the supply chain security through measures to include in the selection of any supplier to ensure the availability of components, technologies, systems and knowhow required in the planning, acquisition, construction, operation, maintenance and repair of the backbone infrastructures (see also section 8.4);

(c) the proposal should have geostrategic importance, in view of the interests of the Union and its Member States, notably to ensure a high level of security of the EU backbone infrastructure;

(d) the proposal fulfils connectivity needs that will not be met by private investments alone, due to the risks involved;

(e) the proposal combines budget from other funding programmes such as NDICI, ERDF or IPA III;

(f) the proposal increases the sustainability of backbone infrastructures by reducing their climate, energy and overall environmental impact.

The applicants may apply for grants for works and studies:

- **Works** include total project's investment costs required to construct the described networking solution for the foreseen system lifetime, from end to end, including e.g. cable landing stations or satellite ground stations, and the connectivity towards them. Works exclude costs for operating the infrastructure during the lifetime and extra components at the landing sites not required for the basic end-to-end connectivity such as data centres, hosting facilities and other services. Exceptionally,in order to facilitate the access to the financed infrastructure by the largest possible number of users, project costs may also include costs required to construct additional access poins In such a case, costs related to the deployment of additional access points must not exceed 5% of the entire project costs.
- **Studies** include all preparatory work required prior to signing a contract with a supplier, such as marine ground surveys for submarine cables and the application for required permits.

Grants call planning: Backbone connectivity for Digital Global Gateways				
Type of Call	2024	2025	2026	2027
Studies / Works	√	√	√	-

Following the call scheduled in 2024, this topic may be supported in the years 2025-27 through the combination of grant under Article 17 of CEF Regulation, for a total amount of EUR 384 millions to be managed in cooperation with HaDEA (for what concerns the grant allocation) and repayable finance from Implementing Partners such as EIB, NPBIs or private banks.

The Commission will commit EUR 30 million of CEF budget under this work programme to the Sustainable Infrastructure Window of InvestEU. The implementation (indirect management) will be given to the EIB group who will invest it eventually in the Digital Infrastructure (Leap) Fund to connect EU outermost regions and overseas countries and territories with main cables co-funded under the NDICI programme.

To be consistent with the basic act, this amount would serve only to finance parts of projects consistent with the policy priorities and the eligibility criteria under CEF and InvestEU. Moreover, certain eligibility conditions of CEF (exclusion of high-risk suppliers, security guarantees approved by the Member State of establishment, the infrastructure remaining under EU-control) would also apply to the entire project.

Benefits and expected outcomes - including EU added value

As a result of the CEF Digital intervention, it is expected that the security and resilience of the EU backbone networks will be significantly improved including, for example, in terms of removing single points of failure, creating appropriate redundancy, removing critical dependencies from existing or planned routes that are not fulfilling adequate security and

resilience requirements, ensuring security of new or upgraded cables. In this respect, the input from the concerned Member States and stakeholders notably via the Expert Group created under the Recommendation as well as the principles set out in the NIS2 and CER Directives will be crucial.

The capacity, security and resilience of the overall backbone network infrastructure will have to benefit all EU end-users. Even in landlocked Member States, users often depend on international connectivity and contribute to the traffic routed via international connectivity systems. It is therefore necessary to secure the availability, security and resilience of such vital infrastructures.

The expected benefits surpass those directly related to the individual supported projects and contribute to bridging the digital divide and ensuring widespread access to the Gigabit and 5G networks for all EU end-users and businesses. Moreover, such connectivity infrastructure can facilitate the implementation of other topics supported under CEF Digital, such as the take-up of 5G use cases, and the availability of cloud and HPC-related facilities, etc.

Among the key performance indicators for this funding action will be the total length of cables deployed or upgraded and the additional (significant) transmission capacity created as a result of the projects supported by CEF.

Finally, CEF Digital will foster the deployment of "Smart" Cable (optic fibre) Systems, which can use the actual length of the cable either by attaching sensors, or by other probing techniques at the edge, to observe and monitor displacement and/or acoustic signals. Where possible, the deployment of "Smart" cable systems may enable applications such as:

- Sensing of seismic, volcanic eruptions and tsunami events, giving possibility for an early warning to civil protection;
- Monitoring of critical energy (e.g. gas pipes, electric cables) and digital infrastructure which can be disrupted by natural cause, involuntary activity, or sabotage;
- Monitoring of events occurring along roads, railways, waterways that are nearby the deployed "Smart" digital infrastructure;
- Monitoring environmental conditions (e.g. temperature, currents) and marine fauna, underpinning research activities close to the infrastructures;
- Gathering information in areas where there are no, or limited means, to observe (e.g. deep waters, arctic region) and analyse data relevant for environmental monitoring, climate change or the observation of endangered species;
- Detection of abnormal events provoked by accidental or deliberate mankind activity, security threats and prevention of attacks, in combination with other measures, including for dual civilian and defence purposes.

By using "smart" cables technology one may reap the benefits of the applications mentioned above and serve in a cost-efficient way, many other EU policies including self-protecting critical infrastructures, in line with the relevant provisions of the CER and NIS2 directives.

Governance, operations and stakeholders involvement

Given the critical importance of backbone networks, particularly submarine cables, for the resilience and security of the Union, it is essential that Member States and stakeholders are involved in the identification of such requirements. This will take place through the CEF Digital

Programme Committee and the Expert Group foreseen in the Recommendation. Consortia applying to the calls, including (local) operators, utilities, (local) authorities, investors and suppliers, are therefore invited to discuss with relevant CEF Digital Programme Committee members and national contact points before submitting their proposals.

It is essential that consortia assess in their proposals the level of market failure, also taking into account the levels of resilience and security provided by existing and planned infrastructures. Besides the deployment of the actual cables, consortia are required to specify any other element, in particular in terms of technological solutions, business models, operational management and ownership (including cases where the affected Member States may apply 'golden power' on critical infrastructures), possible dual use, that may be relevant to the security and resilience of the cables.

The proposals must define the ownership post-project and describe the mechanism to be used to provide services, including business models. In particular, any arrangements for providing services on a non-discriminatory basis to different market players, as well as the operational relationship(s) between the different participants in the value chain for providing services, should be elaborated.

Digital security requirements

Given this relevance of the backbone cables to public security, from an international and geo-political perspective, there is a need to ensure the security of those infrastructures.

One of the purposes of backbone cables is to connect large geographical areas of the Union, including entire Member States or regions. They transport vast volumes of data which are highly sensitive to users, businesses and governments as they are essential for the functioning of critical services like transport, energy, water or emergency response. Their disruption would generate serious instabilities and undermine public order. A physical impairment from natural causes, involuntary or voluntary activity or a cyberattack perpetrated, for instance, against a submarine cable that ensures the connectivity of European islands could compromise the entire economy of such regions and of the Union at large.

Backbone networks deployed to provide the necessary redundancy for connecting the Union with third countries or connecting European islands and which contribute to increasing the capacity and resilience of the Union's digital networks, should comply with the highest possible security standards and protection against disruptions due to cybersecurity attacks, environmental factors or sabotage.

These infrastructures could indeed give rise to various types of vulnerabilities, including those related to the security of equipment, such as within landing stations or terrestrial satellite stations (which could become "single points of failure"), the involvement of potential high-risk suppliers, jurisdiction of ownership, and possible outsourcing of construction operation and maintenance of the infrastructure to third parties.

As recital 97 of the NIS2 Directive explains, , it is important that all providers of public electronic communications networks, have appropriate cybersecurity risk-management measures in place and report significant incidents in relation thereto. Moreover, since international connectivity enhances and accelerates the competitive digitalisation of the Union and its economy, incidents affecting submarine communications cables should be reported,

pursuant to Art. 23 of the NIS2 Directive[57], to the relevant Computer Security Incident Response Team (CSIRT) or, where applicable, the competent authority. The national cybersecurity strategy of Member States should, where relevant, take into account the cybersecurity of submarine communications cables and include a mapping of potential cybersecurity risks and mitigation measures to secure the highest level of their protection.

In this context, the role of entities supplying or managing equipment (including hardware and software) that implements and manages/operates core network functions, network management and orchestration functions, as well as access network functions are critical in relation to the security of the Union, its end-users and businesses. For instance, a security threat may occur if the entities involved in the management of active components of the infrastructure use their power to share critical sensitive data with un-authorised parties or un-authorised parties are able to influence the use of such components or infrastructure. The risk may be further exacerbated if the deployed infrastructure is used as a backbone to connect critical digital capacities such as cloud infrastructures (e.g. data centers hosting critical datasets) or high performance computing resources that are particularly relevant to implement the Global Gateway strategy of the Union.

Therefore, in view of the particular sensitivity of backbones infrastructures from a security perspective and the importance to reduce exposure to risks to the maximum possible extent, proposals under the Digital Global Gateways action will be subject to Article 11(4) of the CEF Regulation, as detailed in section 8.3.

Concerning infrastructures connecting the EU with third countries, legal entities established in those third countries should exceptionally be eligible to receive Union financial support under the CEF where this is indispensable for the achievement of the objectives of a given project of common interest and provided the conditions set out in section 8.3 are fulfilled. It is also expected that proposals under this topic would be developed in the context of agreements between the EU and the concerned third countries being connected to the EU.

As described in section 8.4, all works project proposals, to be eligible, shall include security declarations by the participating entities and commitments which demonstrate that the network technologies and equipment (including software and services) funded will comply with security requirements as specified in the call conditions, in accordance with the applicable EU law, national law, and EU guidance on cybersecurity[58].

4.3 Operational digital platforms

Legal base: art. 8.4.e and 9.4.e of the CEF Regulation

Indicative budget: 20 million EUR, implemented through grants (direct management)

4.3.1 Background

Amid accelerating climate change and a shifting geopolitical environment, the EU is facing an unprecedented energy crisis with supply shortages and possible blackouts that are threatening industry and are raising the cost of living. To address this crisis, reduce carbon dioxide emissions, decrease our usage of and dependence on fossil and imported fuels and achieve the

[57] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[58] See section 8.4

digital transformation of the EU economy there is a need for greater convergence and synergies between the transport, energy, and digital sectors.

The European Commission launched in October 2022 the "Digitalising the energy system – EU action plan". The action plan proposes concrete steps to further accelerate the digital and sustainable transformation of the EU's energy system, in line with the European Green Deal, REPowerEU and the Digital Decade Policy Programme 2030 for Europe, including actions related to the digitalisation of energy infrastructure, which will be supported through various instruments at EU level. The REPowerEU plan calls for a massive scale-up in renewables (wind, solar, hydro, tidal, etc) as well as faster electrification and replacement of fossil fuels.

Some members states have developed national data hubs for e.g. energy but connecting them on a European level has fallen short. Optimising electricity and transport infrastructures only on national basis could be counterproductive at European level and lead to less optimised systems. Operational Digital Platforms (ODPs) would reduce the risk that more renewable energy is lost through curtailing, with positive effects such as reduction of reliance on fossil fuels, and of the risks of deindustrialisation through European industries moving to other regions with cheaper energy. As the energy and the transport sectors are among the top contributors to greenhouse gas emissions, ODPs would also contribute to the ambitious environmental targets of the European Union (Fit for 55, 2030, 2050, etc.).

4.3.2 Objectives

ODPs aim to support EU environmental and energy targets as well as the ongoing energy crisis, by providing both technologies and connectivity to enable a cybersecure Internet of Energy and an optimised transport system along the major European paths, as per the 5G objectives in the Decision (EU) 2022/2481 establishing the Digital Decade Policy Programme 2030[3] and in the Regulation (EU) 2024/1309 on measures to reduce the cost of deploying high-speed electronic communications networks. This will optimise energy use of ICT and reduce the environmental impact, while increasing the benefits enabled by ICT. It will be dedicated to "retro-fitting" the existing energy and/or transport infrastructures with the required cross-border digital infrastructure. ODPs will build on and integrate with existing and emerging European data, cloud and edge computing and connectivity infrastructures, in particular those supported in other parts of CEF Digital, the Digital Europe Programme, and Horizon Europe. The ODPs will contribute to the achievement of EU technological and energy sovereignty and security of energy supply. The topic contributes to the Digital Decade goals such as the deployment of 10,000 climate neutral highly secure edge nodes, etc.

4.3.3 Implementation 2024-2027

The actions to be funded under this topic, will have to build upon the CSA funded under the first multi-annual work programme

The topic is mature for implementation, as it has been covered extensively in the Research and Innovation programmes of the European Union and the solutions are at a very high TRL level. Moreover, similar initiatives have been implemented on a national level in several member states. Other related background projects are part of the Digital Europe Programme such as the smart city platforms (local digital twins), the energy and mobility Common European data spaces as well as the EU Energy Saving Reference Framework.

Type of Call	2024	2025	2026	2027

Works	-	√	-	-

Indicative budget: EUR 20 million

Benefits and expected outcomes - including EU added value

The project will deploy cross-border digital infrastructure that will accelerate the digitalisation of the energy/mobility sector by enhancing interoperability and standardisation and trigger a public-private partnership virtuous circle of investment. This infrastructure will build on and integrate with existing and emerging European data, cloud and edge computing and connectivity infrastructures. The project will lead to a substantial reduction in GHG (greenhouse gas) and improvement in the energy and environmental performance of the European energy, transport and digital infrastructures thus addressing and easing the current energy crisis and avoiding blackouts.

The key performance indicators for the topic will include the amount of GHG emission savings, the number of connected operators, the number of countries involved, as well as the degree of integration with the European data, computing, and connectivity infrastructure both for leveraging digital infrastructure and optimising its energy and environmental performance.

Governance, operations and stakeholders involvement

The beneficiaries for the works phase can take the form of consortia, including *inter alia* local authorities, national authorities, energy companies, transport/mobility companies, transport authorities, equipment providers, system integrators, mobile networks operators, platform operators, companies providing security and privacy solutions, service providers, data centres operators.

The governance body for the emerging infrastructure should be set up by the CSA and include several entities of each major category of stakeholders, including in particular representatives involved in the long term operations of the infrastructure such as energy companies, data centre operators, transport, telecom and/or platform operators, public authorities, etc. It shall be open to new members and in particular foresee eventual participation by all Member States. It could leverage existing structures as long as this does not counter the interest of participating stakeholders.

The governance body will be responsible for defining ownership of the ODP, at any given time, based on the size of the infrastructure and operations as well as the number of parties involved. The Commission shall not be a member of the body, but shall be granted an observer role. Subject to approval by the Commission, the governance body shall propose a legal and financial framework for the operational and financial details of the infrastructure and services support. Provisions for open and fair access to the infrastructure shall be made, including related to new entities joining at a later stage.

5. Programme support actions

Legal base: art. 9.1 of the CEF Regulation

CEF Digital will also fund programme support actions in the field of connectivity, implemented through procurement, which aim at maximising the impact of the EU intervention.

5.1 Studies, communication and other measures

Studies

An indicative and non-exhaustive list of actions includes studies on: the average investment return of commercial digital submarine cables, on monitoring of the deployment of edge computing nodes, on a European framework for sharing public cloud capacities, on network requirements and returns of 5G standalone infrastructure investments, on the provision of connectivity, including the quality of service requirements, business models and access, for 5G transport corridors, and on assessing the demand for very high capacity connectivity networks and identifying investment trends, incentives and barriers in the EU telecom sector.

Communication and dissemination activities

The Commission plans to procure via framework contracts and/or call for tenders the delivery of communication services aimed at promoting the achievements of the CEF Digital programme, the synergies with other programmes, in particular the RRF Plans, and the impact on local and regional economies and societies. Such actions would ensure that reliable information is conveyed to the users, helping to address disinformation on connectivity topics.

The range of activities spans, for example, from dissemination, awareness-raising, communication and community engagement, to tailor made events, webinars, as well as facilitating thematic dialogues involving 5G stakeholders such as Mobile Network Operators, socio economic drivers, policy makers, etc. Support will also be provided for the extension of the connectivity pages of the broadband website, update of the study on National Broadband Plans and support for the annual Broadband Awards.

Other support measures

- Continuation of the activities of the 5G smart communities platform
- Contributing to the development, maintenance and efficient use of the IT systems, including managing the CEF Telecom legacy projects.

Indicative budget: EUR 6.5 million for procurement for studies, communication and other measures.

This work programme will also cover programme monitoring and evaluation costs, project reviews and expert group advice (indicative amount: EUR 200 000).

5.2 Broadband Competence Offices Support Facility

This work programme will continue to support the Broadband Competence Offices[59] (BCO) network, jointly managed by DG AGRI, DG REGIO and DG COMP. The tasks of BCO Support Facility jointly funded by CEF and Technical Assistance resources available under European Agricultural Fund for Rural Development (EAFRD) and European Regional Development Fund (ERDF), include the organisation of workshops, trainings, reporting, social media promotion, web presence and events organisation, the preparation of multimedia material as well as the sharing of experiences and good practices, etc.

The support provided to the national BCOs and/or other relevant competent authorities will cover the identification and mapping of Gigabit and 5G infrastructure needs and the use of available financial resources to cover these needs. Furthermore, it includes the identification and promotion of use cases harnessing Gigabit connectivity to generate value (for demand stimulation) as a way to showcase the benefits and returns of the public and private investments. Previous CEF Digital work programmes provided EUR 0.333 million per year to support the Broadband Competence Offices.

Indicative budget: EUR 1.3 million procurement for 2024-27.

5.3 Overview of Programme support actions 2024-27

(Budget line 02 03 03 01)

Type	Title	Form[60]	Indicative amount (EUR)
CSA	Studies, Communication and Dissemination	P	4 800 000
CSA	Support for the network of Broadband Competence Offices	P	1 300 000
Other support measures	Contribution to the development, maintenance and efficient use of the IT support systems, including eGrants, SEDIA and for CEF Telecom legacy projects, including the WiFi4EU programme.	P	1 700 000
	Total		7 800 000

Total indicative amount for procurement: EUR 7 800 000.

Programme monitoring and evaluation: EUR 200 000

6. Forms of Union financial contribution and co-financing rates

6.1 Main implementation measures and EU financial contribution

[59] As announced in Section 4.5 of the Commission Communication "Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society", COM(2016) 587 final, 14.9.2016.

[60] CSA = Coordination and support action; P=procurement;

In accordance with Article 6(2) of the CEF Regulation, the Programme may provide funding in the form of:

- Grants (calls for proposals), whereby the EU provides financial support and the beneficiaries largely retain control over their results.
- Procurement, which will yield service contracts, whereby the EU covers all cost and owns the results and the related intellectual property and exploitation rights[61].

CEF Digital may also contribute to blending operations in accordance with the InvestEU Regulation[62] and Title X of the Financial Regulation[63], or on the basis of Article 17 of the CEF Regulation for combinations of grants with other sources of financing not supported by the Union budget (i.e. with blending facilities).

EU financial support under calls for proposals shall take the form of reimbursement of eligible costs actually incurred, as provided in Article 125(1)(b) of Regulation (EU) 2018/1046[64], or of simplified forms of funding as defined in the Article 125(1)(a), (c), (d), (e) and/ or (f) of Regulation (EU) 2018/1046 where specified in the call documentation.

The following maximum co-financing rates shall apply to the eligible costs or contributions, in accordance with Article 15 of the CEF Regulation:

For works activities, the amount of EU financial support shall not exceed 30% of the eligible costs or contributions of each action. A number of exceptions are foreseen and the co-financing rate may be increased as follows: up to 50% for actions with a strong cross-border dimension, up to 70% for works carried out in the outermost regions, up to 75% for actions implementing Gigabit connectivity for socio-economic drivers.

Grants dedicated to studies will co-finance a maximum 50% of the total eligible costs or contributions, according to Article 15.1 of the CEF Regulation.

Detailed information will be provided in the call documentation for each topic.

6.2 Combination of funds under under Article 17 of the CEF Regulation - Blending facility

Under the CEF transport sector, the Commission has successfully launched a CEF "blending facility" as a cooperation framework between the European Commission and various "Implementing Partners" (IPs) such as the EIB and various National Promotional Banks and Institutions (NPBIs) for transport projects[65]. The aim of this direct cooperation with financial institutions in Member States was to support projects with a combination of CEF investment

---

61 IT development and procurement choices will be subject to pre-approval by the European Commission Information Technology and Cybersecurity Board.

62 Regulation (EU) 2021/523 of the European Parliament and of the Council of 24 March 2021 establishing the InvestEU Programme

63 Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union

64 Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 (OJ L 193, 30.7.2018)

65 For more information, see https://ec.europa.eu/inea/en/connecting-europe-facility/cef-transport/apply-funding/blending-facility

grants (managed under Title VIII of the Financial Regulation) and financing in repayable form , such as loans or equity capital, possibly together with established commercial partners.

For the second part of the 2021-2027 programming period, the Commission intends to also establish a CEF Digital blending facility for Digital Global Gateways infrastructures.

The blending facility offers several benefits, such as the possibility to support projects which need grants because of limited financial viability, but have the potential to attract market-based financing once de-risked by the grant component. Moreover, it provides increased certainty on the financial soundness and operational readiness of projects through bank co-financing and implementation in time and budget.

The scope of the Digital Connectivity Blending calls will be limited to backbone connectivity for Digital Global Gateways and will depend on the ongoing interests and pipeline development of the participating IPs. The eligibility criteria will be those established in the current work programme on the basis of the CEF Regulation.

The specific delivery mechanism will be negotiated with interested parties and take inspiration from existing Blending Facility schemes such as the Alternative Fuel Infrastructure Facility under CEF and the EU-Catalyst Partnership under Innovation Fund and Horizon Europe.

6.3 Financial instruments under InvestEU

As defined in Article 2 of the InvestEU Regulation[66], blending operations require the pooling of EU resources with non-EU funding from Implementing Partners (IPs). The EU's contribution must include at least one form of repayable support, such as a budgetary guarantee or a financial instrument, and must also feature a contribution from sector-specific programme.

Until now the Commission has signed 8 blending operations with the EIF all in the form of financial instruments providing "top-ups" to InvestEU guarantee and three of them in the digital sector ("MediaInvest" with a contribution from Creative Europe, "Investment Platform for Strategic Digital Technologies" and "Chip Fund" both with a contribution from Digital Europe Programme). Under these operations, the sector specific programmes are used to increase the EU guarantee capacity available to a specific implementing partner that will offer investment products along the lines of an agreed investment strategy (typically a sub-segment of the broader InvestEU investment target).

Blending operations in the form of financial instruments providing "top-up" to EU guarantee offer several benefits including:

- Leverage effect allowing to increase the impact of EU budget
- The possibility to define the support in a way that is market conform would allow intervening in a broader range of projects (releasing some eligibility constraints driven by state aid consistency such the the restriction to SGEIs for 5G for smart communities)
- A provisioning rate of 100% for blending operations in the form of financial instruments significantly enhances the capacity of the recipient Implementing Partner to support a larger volume of high-risk operations.

[66] Regulation (EU) 2021/523 of the European Parliament and of the Council of 24 March 2021 establishing the InvestEU Programm

The Commission may use EUR 100 million from the 5G topics to top up EU guaranteee of the InvestEU's Sustainable Infrastructure Window managed by the EIB Group. The top-up would cover large-scale 5G pilots with the same scope described under section 3.

The Commission will also gradually commit EUR 30 million of CEF budget under this work programme to the Sustainable Infrastructure Window of InvestEU. The implementation (indirect management) will be given to the EIB group who will invest it eventually in the Digital Infrastructure (Leap) Fund - co-funded under the NDICI programme - to connect EU outermost regions and overseas countries and territories[67].

7. Indicative timetable and budget for the calls for proposals 2024-2027

7.1 Indicative call planning, per topic

Topic	Type of call	2024	2025	2026	2027
5G large scale pilots	Studies/works	√			
Quantum communication infrastructure	Works	√	-	-	-
Backbone connectivity for Digital Global Gateways	Studies/Works	√	√	√	
Operational digital platforms	Studies/Works	-	√	-	-

7.2 Indicative amounts available for the topics and implementation planning

Budget line: 02 03 03 01
Allocations in EUR million

Legal base	Topic	2024	2025	2026	2027	Total 2024-27 (EUR million)
Art. 8.4.c, Art. 9.4.c Deployment of 5G corridors along major transport paths	5G large scale pilots	105	100			205
Art 8.4.a, Art. 9.4.a Deployment of and access to VHC networks, 5G and other state of the art connectivity in areas where SEDs are located.						
Art. 8.4.d, Art. 9.4.d	EuroQCI	90				90

[67] To maximise synergy between CEF and NDICI programmes, it is required that each programme has non-overlapping eligibility requirements. For instance, the CEF funds could focus on the sections from the landing station in an outermost region to a branching unit in the main trunk of a cable.

Deployment or significant upgrade of cross-border backbone networks	Backbone connectivity for Digital Global Gateways	128	190	224		542
Art. 8.4.e, Art.9.4.e Deployment of operational digital platforms	Operational digital platforms		20			20
Art. 9.1 Actions contributing to the achievement of the objectives of the programme	Programme Support Actions (procurement)	2,8	1,8	1,7	1,7	8
Total (EUR million)		**325,8**	**311,8**	**225,7**	**1,7**	**865**

	Indicative CEF Digital implementing modes (2024-27, budget in EUR million)			
Topic	**Grant call (2024)**	**Blending Facility (grants) (2025-2026)**	**Financial Instruments (InvestEU Top Up) (2025-27)**	**Total WP2 (2024-27,** EUR million)
5G large-scale pilots	105		100	205
EuroQCI	90			90
Global Gateways	128	384	30	542
Operational Digital Platforms (2025)				20
Support Actions (procurement)				8
Total (EUR million)				**865**

Estimated breakdown of annual instalments in EUR million[68]

Budget Line	2024	2025	2026	2027	TOTAL
02 03 03 01	81.53	210.18	286.76	287.20	865.67
Grand total of all budget lines					865.67

[68] Article 4.5 of the CEF Regulation: Budgetary commitments for actions extending over more than one financial year may be broken down into annual instalments, over two or more years

8. Common provisions

8.1 Technical specifications

Applicable technical specifications for projects will be specified in the relevant calls for proposals, where necessary.

8.2. Security

Cross-border and internal Member State infrastructures funded under CEF must comply with the highest security standards as they underpin the entire economy and society. Vulnerabilities of such infrastructures can undermine public order and security within the Union.

Ensuring security in the Union encompasses, for example, protection from external or internal threats, including the protection and resilience of critical infrastructure against systemic risks and hybrid threats that could extend to energy and transport infrastructures, data processing infrastructures and networks, including space surveillance and tracking and governmental satellite communications.

Threats to electronic communications infrastructures can undermine the public order and security in the Union because they are fundamental enablers for critical services of general interest such as electricity transmission, road safety, protection of confidential information, effective functioning of justice and police, water supply, health services, food supply chain and farming. In addition, dependencies and vulnerabilities of the Union's digital connectivity infrastructure can open the door to increased foreign influence and control over democratic processes (for instance the spread of misinformation).

Pursuant to Article 8(2)(b) of the CEF Regulation, PCIs funded under this work programme shall guarantee that the deployed network infrastructures fulfil the highest possible levels of cybersecurity, resilience and security. This concerns also subcontractors and suppliers involved in such PCIs.

Beneficiaries participating in CEF Digital actions described under sections 3 and 4 will manage critical network configuration functions and data needed to operate the deployed networks including, for instance, information about the levels of security protection applied to the infrastructure, access rights to active components, architectural aspects, etc. Because of their critical importance from a cybersecurity point of view, these fundamental functions and data should be protected from unauthorised access.

For these reasons, stringent requirements as regards cybersecurity are set for all projects financed on the basis of the CEF Digital work programme. Those requirements are addressed at two levels:

- Eligibility of participants (see section 8.3);
- Conditions and assessments related to the supply of technologies and equipment (see section 8.4) applicable to proposals.

8.3 Eligible applicants

In addition to the criteria set out in Article 197 of the Financial Regulation, Article 11 of the CEF Regulation sets out the eligibility criteria for participation to CEF Digital and provides for the possibilityto restrict eligibility to participate for duly justified security reasons[69].

In accordance with Article 5.2 of the Regulation, legal entities established in associated countries shall be eligible where this is indispensable for the achievement of the objectives of a given PCI.

For the security reasons specified above under section 8.2 and in sections 3 and 4, legal entities established, or deemed to be established, in Member States and directly or indirectly controlled by Member States or by nationals of Member States will,, be eligible to receive funding under the topics described in sections 3 and 4.

In addition, legal entities that are established in the Union, but are not EU controlled, and legal entities established in associated countries shall be eligible to participate under the topics described in sections 3, 4.2 and 4.3, on the condition that those entities provide security guarantees, approved, on the basis of national law, by the country in which they are established. Security guarantees are not required for EU controlled entities established in an associated country.

Legal entities established in a third country which is not associated to the CEF will exceptionally be eligible where this is indispensable for the achievement of the objectives of a given PCI[70], on the condition that those entities provide security guarantees, approved, on the basis of national law, by the country in which they are established.

The above-mentioned security guarantees shall certify that the legal entity:

a) Exercises full control over its corporate structure and decision-making process in a manner that does not restrain or restrict in any way its ability to perform and complete the action;

b) Is not subject to non-eligible third country jurisdiction obligations that may undermine the security of the Union;

c) Ensures that the results of the CEF funded action shall remain within the beneficiary/beneficiaries and shall not be subject to control or restrictions by non-eligible third countries or non-eligible third country entities during the action and for a specified period after its completion, as defined in the relevant call conditions;

Concerning eligible legal entities established in third countries, the “non-eligible third countries” mentioned above under points (b) and (c) should be understood as any third country other than the country of establishment.

---

69 Art. 11 (4) of the CEF Regulation “The work programmes may provide that legal entities established in third countries associated to the CEF in accordance with Article 5, and legal entities established in the Union but directly or indirectly controlled by third countries or nationals of third countries or by entities established in third countries, are not eligible to participate in all or some of the actions under the specific objectives set out in Article 3(2), point (c), for duly justified security reasons. In such cases, calls for proposals and calls for tenders shall be restricted to entities established, or deemed to be established, in Member States and directly or indirectly controlled by Member States or by nationals of Member States.”

70 Art 11(5) CEF Regulation

In the case of the EuroQCI topic (section 4.1), participation will be restricted to entities established, or deemed to be established, in Member States and directly or indirectly controlled by Member States or by nationals of Member States.

8.4 Eligible applications

Assessments related to the use of suppliers of technologies and equipment need to be applied to all proposals.

Therefore, to be eligible, all proposals for works shall include security declarations by the participating entities receiving funding for the deployment of equipment and technologies. The declarations should demonstrate that the network technologies and equipment (including software and services) funded by the project will comply with the call's security requirements, in accordance with the applicable EU law, national law, and EU guidance in place on cybersecurity[71]. In addition, where the project provides that network technologies and equipment funded under the project could interconnect (or are part of the same network) with other network technologies and equipment not funded under the project, in a way that could undermine the security of the networks, the requirement to comply with the security requirements of the call shall apply also to any network technology and equipment that would represent a risk as regards the security of networks.

Furthermore, the declarations will ensure that effective measures are in place to address underlying security issues, including, wherever relevant, measures to avoid falling under non-eligible third country jurisdiction obligations, or influence. The project should also comply with the strictest cybersecurity requirements, imposed by national law, in accordance with the 5G toolbox (where applicable) and other relevant EU guidance, of all the eligible countries where the infrastructure is deployed. Finally, the declaration will confirm that the results of the CEF funded action shall remain within the beneficiary during the action and for a specified period after its completion, as defined in the relevant call conditions.

The content of the declarations and commitments in the project proposal will be assessed during the evaluation phase.

Based on these security declarations and commitments, as well as the evaluation carried out by independent experts, the Commission (or funding body) may carry out a security assesment, including the beneficiaries' suppliers and sub-contractors. Funding for actions which do not comply with the conditions related to security issues may be suspended, terminated or reduced at any time in accordance with the Financial Regulation. A proposal must address studies and/or works within the meaning of Article 2(n) and 2(r) of the CEF Regulation or other accompanying measures necessary for the implementation of the CEF Digital[72], as specified in the call for proposals.

---

[71] Such as: the Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, C(2019)2335; the Report on EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks of 9 October, 2019; the Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G of 3 December, 2019; the Cybersecurity of 5G networks - EU Toolbox of Risk Mitigating Measures of 29 January, 2020 and COM(2020)50 of 29 January 2020 on Secure 5G deployment in the EU – implementing the toolbox;the Communication on implementing the 5G cybersecurity Toolbox C(2023)4049 of 15 June 2023.

[72] Article 9 of the CEF Regulation

Proposals for studies and/or works are eligible only if submitted by one or more Member States or, with the agreement of the Member States concerned, by international organisations, joint undertakings, or public or private undertakings or bodies, including regional or local authorities.

8.5 Synergetic elements

In accordance with Article 10(2) of the CEF Regulation, eligible actions under this work programme may include synergetic (ancillary) elements relating to another sector of the CEF programme, i.e. energy and transport, if these synergetic elements allow to significantly improve the socio-economic, climate or environmental benefits of the action. CEF co-funding may be provided as long as the cost of these synergetic elements does not exceed 20% of the total eligible costs of the action.

8.6 Selection criteria

The applicant(s) must have stable and sufficient resources of funding to maintain its activity throughout the period of the grant. The applicant(s) must have the professional skills and qualifications required to complete the proposed action.

The verification of the financial and operational capacity does not apply to applicants which are a Member State, a third country, a public sector body established in a Member State i.e. regional or local authority, a body governed by public law or association formed by one or several such authorities or one or several such bodies, in particular a Joint Undertaking, in accordance with eligibility criteria established under Article 187 of the Treaty on the Functioning of the European Union, or an international organisation.

8.6.1. Financial Capacity

Applicants must have stable and sufficient resources to contribute their share and successfully implement the project for which the grant is requested. Successful applicants will be expected to provide, during their grant preparation, the documents specified in the call for proposals.

8.6.2. Operational capacity

Applicants must have the know-how, qualifications and resources to contribute their share and successfully implement the projects for which the grant is requested (including, where appropriate, sufficient experience in projects of comparable size and nature). They must provide appropriate documents attesting to that capacity as specified in the call for proposals.

8.7 Evaluation and award procedure

The evaluation of the proposals will take into account, the following award criteria, as appropriate:

- **Priority and urgency of the Action**: evaluating correspondence of the proposal with the sectoral policy objectives and priorities, measuring its EU added-value and, where applicable, assessing the possible synergies with other sectors or CEF Digital topics and, where applicable, ensuring a geographical balance of the CEF digital support in the respective area;

- **Maturity:** assessing the maturity of the action in the project development. The criterion will measure among others, i) the readiness/ability of the project to start by the proposed

start date and to complete by the proposed end date, ii) the status and planning of the contracting procedures and the necessary permits and iii) information on the availability of the financial resources needed to complement the CEF investment;

- **Quality:** evaluating the soundness of the implementation plan proposed, both from the technical and financial point of view, the architecture and design approach, the organisational structures put in place (or foreseen) for the implementation, the risk analysis, the control procedures and quality management and the communication strategy of the applicant. Moreover, when applicable, it will also assess the information related to the operations/maintenance strategy proposed for the completed project;

- **Impact:** assessing, when applicable, the economic, social, competition and environmental impact, including the climate impact and other relevant externalities. This criterion may be substantiated by a Cost Benefit Analysis (CBA), in which case the evaluation will look at the soundness, comprehensiveness, and transparency of the analysis as well as proposed means to monitor its impact. The criterion will also assess, where applicable, the safety, security, cybersecurity of telecommunication networks, interoperability and accessibility aspects of the proposal, innovation and digitalisation, as well as its cross-border dimension, and contribution to network integration and territorial accessibility, including in particular for Outermost Regions and islands. Moreover, the criterion will assess, where applicable, potential complementarities with other public funding programmes.

- **Catalytic effect of EU assistance:** evaluating the effect of the EU financial assistance on the realisation of the project, for instance by overcoming a financial gap generated by insufficient commercial viability, high upfront costs or the lack of market finance, increasing the capacity to mobilise differentiated investments sources, improving the quality of the project, or accelerating the overall investment plan.

As a standard practice, a score is assigned for each of the criteria on a scale from 0 (insufficient) to 5 (excellent).

The result of the evaluation will enable the creation of a ranking system per call for proposals. Only proposals passing an established threshold (defined in each call) will be ranked. The ranking will be determined by adding the scores obtained under the five award criteria listed above.

Once the ranking list established, the selection of proposals will be based on the budget availability for the specific call as identified in the call text. Proposals not retained due to budgetary reasons may be included in a reserve list. They shall also be awarded a "Seal of Excellence"[73].

More detailed information on the evaluation and award procedure will be included in each call for proposals.

[73] CEF Regulation art 19.2

9. Financial provisions

9.1 No-profit principle

For projects generating income, the no-profit principle applies, as defined in Article 192 of the Financial Regulation.

9.2 Compliance with EU Law

The granting of EU financial support to PCIs is conditional upon compliance of the project with relevant EU law *inter alia* concerning interoperability, environmental protection, competition and public procurement.

10. State aid considerations

Disclaimer: this section constitutes non-exhaustive guidance notably regarding co-financing of CEF funded projects by Member States. It is the responsibility of the Member States to design State aid measures which are compatible with Union's State aid rules, including the GBER, when the latter is applicable. This guidance is provided without prejudice to the application of the detailed guidance provided in the Commission Notice on the notion of State aid as referred to in Article 107(1) of the Treaty on the Functioning of the European Union ("Notice on the notion of State aid")74, or to the interpretation of the Treaty provisions on State aid by the Union Courts and by the Directorate General for Competition in the application of State aid rules. In any case, the services of the Directorate General for Competition (DG Competition) are available to provide further guidance to Member States on the issues below.

EU resources such as CEF funding awarded directly by the Union do not constitute State Aid75.

The aim of the CEF Digital Programme is to accelerate investment in digital infrastructures and to leverage funding from both the public and the private sectors. For this reason, different maximum funding rates are foreseen for different categories of projects and co-funding with private and/or other public resources is necessary.

Co-funding of CEF projects using public funding that fulfils the conditions defined in Article 107(1) of the Treaty of the Functioning of the European Union (TFEU) constitutes State Aid and must, be notified by the relevant Member State to the Commission for assessment under State aid rules before any public funding is granted, unless covered by block exemptions.

National, regional or local funding provided by a Member State or EU funds under shared management, such as Cohesion Funds and the RRF (where national authorities have discretion as to their use), as well as funding imputable to a Member State (e.g. funds provided via National Promotional Banks and Institutions if NPBIs are acting within the public remit as defined by the Member State and not in line with market conditions) **may constitute State aid** within the meaning of Article 107(1) TFEU. In principle, the Commission must be notified of their use and it will assess them accordingly.

---

74 OJ C 262, 19.7.2016, p. 1.

75 See paragraph 60 of the Commission Notice on the notion of State aid as referred to in Article 107(1) of the Treaty on the Functioning of the European Union, C/2016/2946 OJ C 262, 19.7.2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.262.01.0001.01.ENG&toc=OJ:C:2016:262:TOC

On the contrary, CEF Digital projects co-funded exclusively with purely private funds will in principle not contain any State Aid element.

However, in certain cases these public funds may not constitute State aid or can be considered compatible with the TFEU without a notification and the adoption of a Commission decision.

Notably, as recalled in the Commission Notice on the notion of State aid, public support to connectivity projects not used for economic activities (e.g. the exercise of public powers, certain health care and public education activities) **may not constitute State aid**. This may be particularly relevant for the co-financing of certain types of projects, for instance quantum communications infrastructure for the exclusive use of public authorities or entities that do not carry out an economic activity[76]. The presence of State aid is also excluded in those projects in which the public authorities intervene in line with normal market conditions or when the public support granted can be considered as *de minimis*.

In addition, even when State aid is present, **no notification is required** for certain types of projects, notably those covered by the General Block Exemption Regulation (GBER)[77]or the SGEI Decision[78]. The Commission has exempted[79] from notification under certain conditions State aid used to fund or co-fund certain projects financed by CEF Digital or having received a CEF Seal of Excellence. Specifically, this concerns certain cross-border sections of i) 5G corridors, ii) backbone networks interconnecting certain computing facilities and data infrastructures supporting the objectives of the European High-Performance Computing Joint Undertaking, iii) backbone networks interconnecting cloud infrastructures of certain Socio-Economic Drivers, and certain submarine cables.

---

[76] See section 2 of the Commission Notice on the notion of State aid as referred to in Article 107(1) of the Treaty on the Functioning of the European Union.

[77] Commission Regulation (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty, OJ L 193 of 30.7.2018

[78] Commission Decision of 20 December on the application of Article 106(2) of the Treaty on the Functioning of the European Union to State aid in the form of public service compensation granted to certain undertakings entrusted with the operation of services of general economic interest Official Journal L7, 11.01.2012.

[79] See above footnote 76.