EUROPEAN
COMMISSION

Brussels, 19.4.2023
C(2023) 2533 final

ANNEX

ANNEX

to the

Commission Implementing Decision

amending Implementing Decision C(2021) 9463 on the financing of the Connecting Europe Facility – Digital sector and the adoption of the multiannual work programme for 2021-2025

ANNEX

‘ANNEX
CONNECTING EUROPE FACILITY (CEF) – DIGITAL SECTOR MULTIANNUAL WORK PROGRAMME FOR 2021-23

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 trans-European infrastructures as the "nervous system" of an increasingly interconnected European society. With these characteristics, CEF is set to fulfil a key role in Europe's recovery from the COVID-19 pandemic crisis through investments in short-term recovery and long-term prosperity.

Digital transformation in accordance with European rules and values and in line with the European Green Deal is a '*make-or-break*' issue for successful recovery. That reflects the importance of investing in our European tech sovereignty, *inter alia* through investments in sustainable high-performance infrastructure, including 5G and fibre in an unprecedented manner.

The Communication "2030 Digital Compass: the European way for the Digital Decade"[1] sets a vision of a human-centred, sustainable and more prosperous digital future. As a part of that it reaffirms the crucial role of digital connectivity and sets levels of ambitions for 2030, namely a Gigabit network for all European households and 5G in all populated areas. It also stresses the importance of connecting the Union with its international partners in line with the European Data Gateways Ministerial Declaration[2] and the new Global Gateway strategy announced by the President of the European Commission[3].

Following the Communication, the Commission issued a proposal for a decision of the European Parliament and of the Council establishing the 2030 Policy Programme "Path to the Digital Decade" on 15 September 2021.[4] The draft Decision aims to ensure that the European Union achieves the objectives and targets of the Digital Decade in line with the EU´s values, reinforcing Europe's digital leadership and promoting human-centred, inclusive and sustainable digital policies. The proposal also sets out the concrete digital targets which the Union as a whole is expected to achieve by the end of the decade, as first delineated in the Digital Compass Communication. The digital targets for 2030 are based on four cardinal points: digital skills, digital infrastructures, digitalisation of businesses and digitalisation of public services.

The objective of the digital part of the Connecting Europe Facility ("CEF Digital) is to contribute to the development of *projects of common interest*[5] (PCIs) relating to the deployment of safe, secure and sustainable high-performance infrastructure, including Gigabit and 5G networks. CEF Digital will also contribute to the increased capacity and resilience of

---

1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0118&from=en
2 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=74941
3 https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701
4 https://digital-strategy.ec.europa.eu/en/library/proposal-decision-establishing-2030-policy-programme-path-digital-decade
5 The projects of common interest in the area of digital connectivity infrastructure are defined in Article 8 and exemplified in Annex V of the CEF Regulation.

digital backbone infrastructures in all EU territories, as well to the digitalisation of transport and energy networks.

CEF Digital will foster public and private investments and will allow cumulative funding with other funding instruments, including the Recovery and Resilience Facility (RRF) as well as with the InvestEU[6] fund.

CEF Digital is based on Regulation (EU) 2021/1153 of the European Parliament and of the Council (the "CEF Regulation"), which determines the general principles, legal base and procedures for providing EU financial support to trans-European networks in order to support PCIs in the fields of transport, energy and digital connectivity infrastructures. The CEF Regulation also establishes the breakdown of resources available for 2021-2027 in transport, energy and digital.

In accordance with Article 20 of the CEF Regulation, the 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 2021-2023. It contains information about the legal commitments expected as a result of the calls for proposals to be launched in years 2021, 2022 and 2023.

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 2021-2023.

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

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 accelerate recovery if access to Gigabit networks is made available to all citizens, businesses and 'socio-economic drivers' (SEDs), notably schools, universities, hospitals, transport hubs, public administrations, etc., irrespective of their location and economic factors. 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 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.

The COVID-19 pandemic has reconfirmed the importance of universal access to very high speed, reliable, secure and affordable internet connections for all: businesses, public services and citizens. It has also highlighted the consequences of the digital divide - for example

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0523&qid=1617090511360

between different regions, rural versus urban areas, or linked to socio-economic factors. The aftermath of the crisis and the vision set in the Communication "2030 Digital Compass: the European way for the Digital Decade"[7] and the proposal for the 2030 Policy Programme "Path to the Digital Decade"[8] demand an even greater quality of connectivity, for instance in terms of bandwidth, low latency, security and resilience[9].

Indeed, the increased online interaction between people and objects and the emergence of new ways of working, living, doing business and delivering public services require adequate capability of the underlying digital connectivity infrastructure. Furthermore, sustainable state-of-the-art backbone infrastructures are needed to interconnect digital capacities, such as cloud, data and computing, which are vital to support the EU's ambition to be digitally sovereign in an open and hyper-connected world.

In spite of the growing importance of connectivity, there is still a significant combined private and public funding gap to be bridged which has been calculated in view of the EU's mid-term 2025 Gigabit connectivity objectives, as confirmed by different studies. For instance, the European Investment Bank estimates a combined private and public investment gap of €254 billion for 2020-2025. This amount corresponds to €42 billion per year, or €294 billion over 7 years, whereby additional investments in 2026 and 2027 are likely to be required. In order to fill in this gap and achieve the 2030 targets, it essential to pool CEF Digital together with other funding instruments, including the Recovery and Resilience Facility (RRF), EAFRD, ERDF as well as the InvestEU[10] Fund. Altogether, this will provide an unprecedented amount of investments devoted to high-performance infrastructure, including, in particular in 5G and fibre, as stated in the 2021 State of the Union's address.

In the context of the implementation of the RRF, many Member States have committed very significant amounts of public support for deployment of Gigabit and 5G networks. Based on the applicable co-funding rates, with a budget of EUR **2065** million (EUR 1832 million in constant prices) for 2021-27, CEF Digital will leverage in addition between €3- 6 billion targeted investments in line with the 2030 digital connectivity targets by supporting Gigabit infrastructures, including 5G, and backbone networks addressing market failures. CEF Digital will thus contribute to 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 when preparing eligible projects by coherently combining CEF and RRF investments or designing complementary interventions under ERDF/EAFRD or national and regional programmes.

2.2 Work programme objectives

Pursuant to the CEF Regulation, CEF Digital will 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.

---

7 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0118&from=en

8 https://digital-strategy.ec.europa.eu/en/library/proposal-decision-establishing-2030-policy-programme-path-digital-decade

9 See COM(2021) 574 final - Staff Working Document Accompanying the Commission's Proposal for the Digital Decade Policy Programme, section 3.3.1.1

10 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0523&qid=1617090511360

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 when possible in market failure areas. 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.

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 via targeted financial instruments, notably through the support of eligible operations through relevant InvestEU Fund's financial products.

Cross-fertilise investments and ensure complementarity of funding programmes

Digital connectivity infrastructures are supported at European, national, regional and local levels. 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 fund sources and taking into account the existence of complementary projects (e.g. national segments in market failure areas complementing cross-border projects or complementary backhaul and access networks), the work programme aims at reducing the fragmentation of 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.

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. Energy efficient technologies such as fibre and 5G will bring a huge contribution to the European Green Deal[11] as they have the potential to enable significant energy efficiency gains and carbon emissions reduction in 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. The RRF and the Cohesion policy funds can complement the financing offered by CEF Digital in order to accelerate recovery and contribute to a sustainable data economy.

While CEF funding does not constitute State aid, the use of RRF resources or other public resources to provide the necessary co-financing of a project may require its notification and assessment by the Commission. However, the work programme includes several scenarios in which the use of RRF or other public resources would not constitute State aid or could be considered compatible with the Treaty on the Functioning of the European Union[12] without its notification. More details on State Aid and assessment by the Commission are provided in section [10].

---

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

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

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/EARDF, etc. In this respect, several approaches can be envisaged provided that the provisions of the relevant Regulation are respected, notably for what concerns the avoidance of double funding. In most cases close coordination between all public actors is needed, in particular to ensure that the same costs will not be financed twice, where national RRF Plans foresee the combination of prospective CEF Digital projects with the RRF funding sources[13].

As stated in the Digital Decade Policy Programme[14], the work programme will support the implementation of Multi-Country Projects in selected areas, involving several Member States, and by pooling resources from the Union, Member States, and where appropriate private sources. They will require a coordinated approach, in close cooperation between the Commission and the concerned Member States. CEF Digital will contribute to accelerate the deployment of 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 intends to also establish a CEF Digital Connectivity Blending Facility (based on Art. 17 of CEF Regulation) where the Commission services work closely with Implementing Partner institutions in Member States, including National Promotional Banks and Institutions (NPBIs), to efficiently combine grants from CEF2 with equity and loans from the partners, to support infrastructure deployment projects in Member States.

Ensure that nobody is left behind by the digital transformation

In the past few years, the DESI connectivity report has shown an overall improvement of connectivity indicators in the EU, both in terms of demand and supply**.** However, there are still significant disparities between regions and rural and urban areas, calling for more investments in connectivity infrastructures.

In particular, a study for the Commission[15] found that to achieve the EU mid-term Gigabit objectives by 2025, about €200 billion will be needed to deploy fibre to the premises (FTTP) networks to households and SEDs across the EU in all areas which have been identified as exhibiting enduring lack of commercial viability for private investments into such networks. A conservative estimate suggested that around €22 billion of public support (in particular) subsidies would be needed in this scenario. In addition, the estimated length of a pan-EU network of cross-border corridors of 26,000 km of highways will require investment for backhaul, 5G networks and vehicle-to-network infrastructure of around €5.46 billion in total.

This work programme will contribute to filling some of these connectivity gaps and ensure that local/regional infrastructures are efficiently connected through end-to-end high-performance infrastructure, including backbone networks. It will notably support strategic connectivity to remote regions including the outermost regions (e.g. through submarine

---

[13] In this context, several approaches are foreseen, including using RRF funds to co-invest in CEF projects to finance projects that receive a Seal of Excellence quality label under the CEF programme, replicating CEF actions as best practices, establishing dedicated financial instruments, using RRF funding for sections falling within the national borders, for example to link to other cross-border CEF projects, and providing successive support to the same project or program (staging).

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

[15] Supporting the implementation of CEF2- SMART 2017/0018 (published February 2020, see https://op.europa.eu/s/n8tU)

cables) and rural or sub-urban regions. This all-encompassing and inclusive approach to connectivity will give all citizens and businesses the opportunity to benefit from the digital single market and accelerate economic recovery.

Building pan-European, cross-border infrastructures

This work programme will support the deployment of 5G systems, including, if appropriate, integrated 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, distributed antenna systems), federated cloud and edge infrastructures, as well as relevant operational service platforms will be ensured by complementary deployment actions funded under CEF Digital and Digital Europe and other programmes such as InvestEU and RRF. The aim is to enable service continuity and the interoperability of 5G services along transport paths across the continent.

International dimension of connectivity

In line with the EU Global Connectivity Strategy and the overall the EU's geopolitical framework in tackling global challenges, CEF Digital will support the development of Global Gateways connecting the European Union with the rest of the world. This will be done by investing in ultra-secure and resilient backbone networks connecting Europe with third countries, including submarine cables and satellite terrestrial backbones.

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 backbone 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. 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 aggregate demand for very high quality connectivity and generate new user experience of these technologies, e.g. use of virtual and augmented reality in the education and training process, tele-operated robotics in surgery, data analytics in precision agriculture and environmental risk management, etc. 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 generations of innovative technologies and infrastructures. 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 cloud-to-edge solutions, and help creating new business models for the telecom sector, capturing the future demand for such connectivity.

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, state 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, require strong cybersecurity measures aiming at increasing the EU's collective resilience against foreign cybersecurity threats.

As a consequence, on the basis of Article 11(4) of the CEF Regulation, the 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 ("non-EU controlled entities"), will 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. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risk. In order to protect society against manipulation of such critical services 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, and endorsed by a Commission Communication,[16] recommends a set of measures, including the need to assess the risk profile of providers and adopt restrictions (including necessary exclusions) from key network assets and other sensitive assets (government services, critical infrastructures). The above-mentioned Communication indicates that the 5G cybersecurity toolbox should be applied in relevant EU funding both within and outside of the EU.

A similar approach should be applied to other backbone infrastructures covered in this Programme when the dependence of many critical services on these infrastructures would make the consequences of systemic and widespread disruption particularly serious.

---

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

Where the backbone infrastructures funded under the CEF Digital work programme are major enablers for critical services of public interest, participation to the calls funded under this work programme will be subject to the provisions of Article 11(4) of the CEF Regulation.

In order to protect duly justified security interests of the Union, non-EU controlled entities will not be eligible to participate in certain deployment actions under the CEF Digital programme. The reasons why it is necessary to exclude the participation of those entities are specified for each relevant topic.

In addition, to ensure the maximum level of cybersecurity, as described in section 8.4., *all* works project proposals submitted, to be eligible, shall have to include security declarations by participating companies which demonstrate that the network technologies and equipment (including software and services) funded on the basis of the programme comply with security requirements as specified in the call conditions, in accordance with the applicable EU law, national law, and EU guidance on cybersecurity. The security declarations also need to demonstrate for each company that effective measures are in place to address underlying security issues, including, wherever relevant, measures to avoid falling under foreign jurisdiction obligations or third country influence. Under specific topics, proposals must indicate that network equipment or operational services deployed or used within the proposal will be procured from eligible country suppliers.

Participation in calls for proposals under topics 3.1 ("5G Corridors") and 3.2 ("5G for smart communities") will be subject to specific security-related requirements.

Contribute to the European Green Deal

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

2.3 Overall approach and expected results

Based on Articles 8(4) and Article 9(4) of the CEF Regulation, CEF Digital can support the following key topics targeting specific types of deployment projects, namely:

1. The deployment of and access to very high-capacity networks, including 5G systems, capable of providing Gigabit connectivity in areas where socioeconomic drivers are located;
2. Uninterrupted coverage with 5G systems of all major transport paths, including the trans-European transport networks;
3. Deployment of new or significant upgrade of existing backbone networks including submarine cables, within and between Member States and between the Union and third countries, to the extent to which they significantly contribute to the increased performance, resilience and very high capacity of the electronic communications networks;

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. 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. Information days will be organised around each call for proposals in order to foster community building and proposal preparation.

Funding will be delivered through grants and procurement (for some of the Programme Support Actions)[17].

Wherever appropriate, the possible use of simplified forms of assistance (e.g. lump sums) and/or of implementation (e.g. voucher schemes) may be used in view of simplifying the management of the grants.

In addition, the Commission intends to establish a CEF Digital Connectivity Blending Facility with rolling call in order to provide the maximum flexibility for the Implementing Partners (such as National Promotional Banks and Institutions/NPBIs, the EIB Group or the European Bank for Reconstruction and Development/EBRD[18]) and efficiency in spending the CEF Digital grants.

CEF Digital will also support Member States and applicants with targeted Synergy and Programme support actions.

CEF Digital will contribute to the European Green Deal and the EU's decarbonisation objectives by supporting smart green ICT infrastructures for instance using energy-efficient optical fibre networks and state-of-the-art high capacity networks, including 5G, as enablers for the greening of societal and economic activities.

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

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

3. Deployment of 5G infrastructures in Europe

3.1 5G coverage along transport corridors

3.1.1 Background

The 5G Action Plan for Europe (5GAP) sets the objective to achieve uninterrupted 5G coverage along main transport paths across Europe by 2025.

Such infrastructure is expected to be a key enabler for connected and automated mobility (CAM) including safety and non-safety services. These include a broad range of digital services for the vehicle, the driver and the passengers and other relevant players, as well as connectivity services paving the way to driving with high levels of automation by the end of the current decade on certain sections of main transport paths equipped with 5G. It is also expected that 5G infrastructures strengthen the digitalisation of rail operations and inland waterways. Such infrastructure can also be used under certain conditions, where market failures are demonstrated, for services beyond the transport paths, e.g. in areas surrounding the corridor including populated areas or socio-economic drivers.

5G corridors can be defined as 5G systems – including, if appropriate, 5G edge computing facilities - that meet the very stringent service requirements of transport safety and digital rail operations, in particular in terms of ultra-high reliability, security, low latency, and high throughput. In particular, they should make these service characteristics available for advanced transport and logistics applications.

The Commission has underlined in its strategy on the mobility of the future[19] the specific contribution made by CAM to improved 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 is identified as major enabler. In this context, the strategy underlines the Commission's work together with the Member States towards a pan-European road network of 5G corridors. The objective of 5G corridor deployment in support of higher levels of automation has been reaffirmed by the Commission in its sustainable and smart mobility strategy of December 2020[20]. Such a road network functioning across borders at European scale is essential in allowing for economies of scale and network effects that are needed for such digital ecosystems to develop in Europe.

Investment in 5G corridors is expected to be particularly challenging because, as compared to today's wide area deployment of mobile networks, it will require uninterrupted coverage in a high speed mobility scenario and, where necessary, a dense network in order to meet challenging performance requirements for digital services such as CAM. This would require the installation of a large number of additional network elements equipped with 5G capabilities on existing or new sites, including, if appropriate, 5G edge computing facilities along the transport paths. It would equally require backhaul networks connected to the public telecom network and, if appropriate, the interconnection to federated cloud and edge computing infrastructures and access to electricity supply.

---

[19] "On the road to automated mobility: An EU strategy for mobility of the future", Communication of 17 May 2018, COM(2018) 283 final; https://ec.europa.eu/transport/sites/transport/files/3rd-mobility-pack/com20180283_en.pdf

[20] "Sustainable and smart mobility strategy: putting European transport on track for future, COM(2020) 789 final; https://eur-lex.europa.eu/resource.html?uri=cellar:5e601657-3b06-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF

According to a Commission study[21], the prospect of return on investment of CAM services is expected to emerge around 2025, due to the large road mileage to be equipped with 5G in order to create the needed conditions for widely available services. In particular, the penetration rate of vehicles capable of higher levels of automation is not expected to be significant until the necessary infrastructure has reached a critical mass. However, service providers should be able to obtain a certain level of return on investment from the start based on other digital services, such as those linked to mobile office or entertainment services, in particular on high traffic sections of highways.

3.1.2 Objectives

CEF Digital will co-fund a set of 5G corridor deployment projects under this work programme. The goal is to leverage the needed private investment in order to establish a full pan-European transport network of 5G corridors by the end of the CEF programme.

CEF Digital will support investments in challenging areas, where market forces alone will not deliver 5G services with the necessary quality of service, and focus on key European transport paths including, but not limited to the indicative list of 5G corridors in the Annex part V of the CEF Regulation. Additional sections considered relevant from a European perspective are also in scope. The priority for the first three years of this work programme will be to support investment in cross-border sections involving two or more Member States, with a co-funding rate of 50%.

The corridor must cross at least one national border and the length of corridors envisaged for deployment or study 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 TEN-T comprehensive corridors in a Member State. If justified by the project objectives and in the presence of demonstrated market failures, 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% 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 in areas with insufficient mobile coverage suitable for CAM services and where there is no commercial interest to invest in the near future may be possible as a second step if designed as market-conform interventions[22].

Actions addressing coverage of intra-national sections of corridors with demonstrated market failures with a 30% funding rate can complement national deployment initiatives, including those funded under the RRF in line with State aid rules. Such intra-national sections funded

---

[21] https://op.europa.eu/en/publication-detail/-/publication/8947e9db-4eda-11ea-aece-01aa75ed71a1/language-en

[22] See section 10 below.

under RRF and in the later phase of the CEF programme should complement the cross-border sections funded in the first phase of the CEF programme.

Concerning such actions for the deployment of intra-national sections, as a basic rule, sections with no 4G coverage can be considered as market failure. Beyond this basic rule, in case of existing 4G coverage in parts of the section concerned, a market failure needs to be demonstrated by the proposal (e.g. in terms of absence of an infrastructure capable of providing the performances required for 5G corridor services).

In both cases of actions aimed at cross-border sections and intra-national sections, the support provided by CEF Digital will need to go beyond any coverage obligations of the mobile network operators that arise out of spectrum licence conditions. In particular, the proposal should demonstrate that the service requirements fulfilled by the project for future CAM services along the section concerned are going beyond the requirements of the coverage obligations, such as data capacities offered per vehicle, speeds, latency, or other service enablers.

Cross-border sections that are complementary to national 5G corridor sections already planned for deployment by the private sector or identified under RRF or other national programmes in line with state aid rules are particularly encouraged in view of their additional potential impact at early stage.

Projects enabling 5G service continuity over multiple modes of transport, e.g. road/rail logistic hubs, inland or sea harbours, inland waterways, or sea waterways between European countries, are in scope.

Deployment projects may be preceded by inception studies to plan CEF and complementary RRF sections funded under this programme or may be based on other preparatory work e.g. as follow-up of ongoing trial and pilot projects funded under Horizon 2020 or other programmes.

In order to accelerate the development of edge computing solutions as part of 5G corridors a dedicated horizontal support action will be launched at the start of the programme. Such support action should accompany the 5G corridor and 5G for smart communities deployment projects to develop respectively concepts and facilities for the interconnection of newly deployed 5G corridor sections and 5G for smart communities with edge computing facilities and federated cloud infrastructures, as well as relevant operational service platforms funded under CEF Digital and Digital Europe.

The timetable below describes the foreseen distribution of calls and the type of actions to take place over the entire CEF Digital funding period from 2021-2027.

CEF2 Digital 5G corridor deployment calendar										
Year	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Early Wave	Call Q4-Q1		Deployment (CEF/RRF)							
1st big Wave	Call Q4-Q1		Studies							
			Call Q1-Q2	Deployment (CEF/RRF)						
2nd big Wave (TBC)			Call Q1-Q2	Studies						
				Call Q1-Q2	Deployment (tbc)					
Last Wave (TBC)										

Project proposals are encouraged to create complementarity and synergies with other activities implemented as part of other infrastructure projects including those under CEF Transport, CEF Energy, DEP and Horizon Europe programmes. This concerns in particular activities that aim at deploying cooperative intelligent transport systems, digitising and

electrifying transport paths, artificial intelligence applied to CAM, deploying pan-European federated cloud and edge computing capacities, and the use of 5G corridors as testbed for the validation of use cases developed under Horizon Europe. Furthermore, the potential to establish synergies with RRF investments should be considered, for instance by complementing cross-border sections with national and regional sections. Proposals submitted under this topic are expected to contribute to a wider plan to deploy uninterrupted, end-to-end 5G connectivity along the entire pan-EU network of 5G corridors, in synergy with national actions, such as those identified under RRF. The Member States involved in the proposals would commit to extending the 5G corridors on their respective territories, including the possibility to connect the CEF-funded projects with other corridors as described in the TEN-T Regulation.

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

3.1.3 Implementation 2021 -23

As of 2020, there were no operational 5G corridors in Europe. However, large-scale trials for testing, demonstration, and validation purposes have been conducted at different locations across Europe, with the support of European and national/local public funding.

Inception studies are therefore needed in 2022 and 2024 in order to prepare the actual deployment work of the larger waves of deployment which will be launched after the conclusion of the studies. One study for several deployment projects for the same or different calls, e.g. combined by region, are encouraged. These inception studies should include a detailed network planning, which should provide a basis for the deployment plan, the concrete deliverables in terms of deployed infrastructure, coverage and service capabilities, utilization of existing infrastructure (fiber, power, ground space etc), the associated costs as well as the assessment of market failure for each relevant action. The studies should also develop a corridor-specific deployment roadmap covering several phases using CEF Digital 2021-2023 and RRF in the first phase and identifying options for financing solutions for the following phases possibly using combinations of grants and loans, e.g. under the CEF Digital blending facility.

Two waves of deployment calls will be launched:

- 2022: an early wave of deployment actions for 5G systems deployment along mainly cross-border sections of transport paths that may encompass roads, rail and inland waterways, and if appropriate in multi-mode combination with other modes of transport, based on early preparatory work that already started before 2021. Unlike for the other subsequent waves, this work programme does not foresee for this specific early wave a call for inception studies. These tasks are expected to be done as part of the proposal preparation, or as part of ongoing pilot projects.

  Furthermore, in 2022 a dedicated horizontal support action in the area of 5G systems with edge computing that should in particular accompany 5G corridor and 5G smart communities deployment projects to develop concepts and facilities to be used by 5G-enabled covering: i) 5G edge computing facilities, ii) federated cloud and edge infrastructures funded under CEF Digital and Digital Europe, as well as iii) operational service platforms that enable the provision of CAM services and other commercial 5G connectivity services.

- 2023: a 1st larger wave of corridor deployment projects that may encompass road, rail and inland waterways, and if appropriate in multi-mode combination with other modes of transport based on inception studies, including those funded under CEF Digital as part of the first call.

- 2025: a 2nd larger wave of corridor deployment projects will be considered for 2025 based on inception studies called in 2023.

Grant call planning: 5G corridors			
Type of call	2021	2022	2023
Inception studies	√		√
Early deployment projects	√	√[23]	
Deployment projects			√

Benefits and expected outcomes - including EU added value

CEF Digital funding is expected to move forward and accelerate large-scale deployment of 5G corridors to support the adoption of CAM, including driving with higher levels of automation and the digitalisation of rail operations as well as other relevant modes of transport. Funding may also support the deployment of Future Rail Mobile Communication System (FRMCS) and trackside and associated on-board equipment related to critical automatic train control systems and applications (ETCS and/or ATO).

By closing the deployment gaps and removing capacity bottlenecks and technical barriers, the deployment of 5G corridors would contribute to strengthening the social, economic, and territorial cohesion in the EU.

Projects should deliver uninterrupted coverage over the whole range of the corridor section thus ensuring high-quality connectivity – depending on the expected traffic demand along the different parts of the section - suitable to provide a broad range of 5G 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 corridor should be capable of meeting service requirements for both safety-related road/rail/waterway operations (e.g. Intelligent Transport Systems (ITS), Future Rail Mobile Communication System (FRMCS), River Information Services (RIS)) and multi-service/multi-application 5G services and ensure business continuity across the entire section of the corridor, including in a cross-border environment. The infrastructure can be used for services beyond the transport paths under certain conditions, e.g. in areas surrounding the corridor including populated areas or socio-economic drivers where market failures are demonstrated, without causing undue competition distortions or crowding out effects and provided third party open wholesale access under fair, reasonable and non-discriminatory condition is provided.

[23] Call in 2022 planned only if the 2021 call needs to be delayed to 2022.

The infrastructure should make use of at least one 5G pioneer band (700 MHz, 3.6 GHz, 26 GHz) and, if appropriate, the 5.9 GHz ITS band and the 900 MHz and 1900 MHz FRMCS bands[24]. If 5G radio-communication technologies are used along the corridor, they should be based on the latest suitable 5G specifications made available by 3GPP, and furthermore be able to integrate upgrades when available. The infrastructure should support advanced service features such as quality of service guarantees enabled by 5G edge computing facilities and facilities allowing for 5G network slicing.

Proposals should demonstrate that interference issues with other C-ITS services using the 5.9 GHz ITS band are analysed and adequately addressed in the project. Particular attention should be given to ensure continuity of legacy services and in particular continued functioning of safety-related services.

The corridor should incorporate solutions to integrate long-range and, if appropriate, short-range communication technologies and support infrastructures. The choice of these solutions will have to take into consideration the level of complementarity of both technologies, as well as efficiencies that may impact deployment costs, network performance, including quality of service, as well as scope and degree of innovation in use cases enabled.

The network quality of the corridor must go beyond existing and/or planned infrastructure along the full corridor and beyond any legally binding 4G or 5G coverage obligations attached to spectrum licences that apply to relevant parts of the corridors in question.

The key parameters for describing the project will be the aggregate length of the corridors covered by 5G, the spectrum bands enabled along the sections, the inter-radio site distance, the availability of various service features along transport routes, as well as the available network performance such as data rate and latency for each vehicle as a result of CEF Digital support.

Funding of sharing models regarding both passive and active infrastructure 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 infrastructure. In addition, wherever possible, existing infrastructure such as ducts, fibre, equipment shelters, power supply and utility poles should be used.

The projects may conduct tests and pilots of connected and automated mobility use cases enabled by the newly deployed 5G corridor network infrastructure. In this regard, synergies with R&I funding programmes at national or European level including the partnerships for Smart Networks and Services (SNS) and Cooperative, Connected and Automated Mobility (CCAM) could be considered.

Governance, operations and stakeholder involvement

Project consortia should be composed of at least two different 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

[24] Commission Implementing Decision (EU) 2021/1730 of 28 September 2021 on the harmonised use of the paired frequency bands 874,4-880,0 MHz and 919,4-925,0 MHz and of the unpaired frequency band 1900-1910 MHz for Railway Mobile Radio. (OJ L 346, 30.9.2021, p.1)

facilities such as tower companies, telecom backhaul operators, road operators, rail infrastructure managers, inland waterways infrastructure managers, automotive manufacturers, mobility and security service providers is encouraged, when and if appropriate. The consortium may include public authorities in the field of transport.

If public resources are used to co-fund the project, the State aid considerations described in section 10 of this work programme must be taken into account.

The beneficiaries should demonstrate that they have access to transport paths and relevant spectrum (in case of active infrastructure, either directly or contractually through service providers).

The beneficiaries should offer reassurances as to the operation of the service beyond the specific section supported by CEF, in view of the long-term development of the more extensive pan-European corridor network.

Proposals would need to demonstrate how the infrastructure is intended to be made available for CAM service providers or other 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.

Proposals should define post-project ownership and describe the mechanism(s) set in place for long term cooperation and sustainability. In particular, it should be described how the project will be used for the provision of CCAM services. Any arrangements for network sharing options should be clearly defined, as well as the functional and operational relationship(s) between the different participants in the value chain for the provision of digital services throughout the 5G corridor.

Proposals 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.

Due to the use of 5G corridor infrastructures for safety-related services such as automated driving, traffic management, etc and their relevance to public order and security, it is essential to ensure the highest level of cybersecurity in this field.

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.

For this reason, stringent requirements as regards cyber security need to be set for 5G corridor infrastructure projects financed on the basis of the CEF Digital work programme. This will significantly reduce the risk that cyber-attacks are perpetrated against citizens, businesses or public institutions, which could have severe consequences for public order and security.

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

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 CCAM services, i.e. critical services directly impacting public safety such as automated driving, traffic management, etc.

In the context of 5G 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[25]. 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.

This is notably the case for suppliers of equipment (including hardware and software) that implements core network functions, network management and orchestration functions, as well as access network functions.[26] 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 are 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 likely if the active components and related services will be sourced from suppliers established in or controlled from third countries[27].

As a supporting action, the Toolbox recommends taking into account cybersecurity risks in public procurement and relevant funding instruments. In view of this, the Commission announced that it will ensure that participation in Union funding programmes in relevant technology domains will be conditional on compliance with security requirements, by making full use of and further implementing security conditions.

As described in section 8.4., *all* works proposals submitted, to be eligible, shall have to include security declarations by participating companies which demonstrate that the network technologies and equipment (including software and services) funded on the basis of the programme comply with security requirements as specified in the call conditions, in accordance with the applicable EU law, national law, and EU guidance on cybersecurity[28].

Based on the security declarations in the proposal, as well as the evaluation carried out by independent experts, the Commission or funding body, where appropriate, may carry out a security scrutiny, including as regards beneficiaries' suppliers and sub-contractors. Funding

---

25 COM(2020)50 of 29 January 2020.

26 See p. 5 COM(2020) 50 final - Secure 5G deployment in the EU - Implementing the EU toolbox.

27 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.

28 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.

for actions, which do not comply with the conditions related to security, may be suspended, terminated, or reduced at any time in accordance with the Financial Regulation.

Specific measures addressing green policy objectives, in particular in terms of reducing the carbon footprint are encouraged.

Each proposal should be supported by the relevant competent authorities involved in the deployment of 5G network infrastructure along a transport path on the two sides of the border, at national and/or regional and/or local levels. This support may be in the form of administrative letters, letters of intent, memoranda of understanding, or similar support documents.

Each proposal should foresee a cooperation with the relevant Programme Support Actions as well as relevant working groups and fora of the Smart Networks and Services Joint Undertaking (SNS), which is expected to provide strategic guidance to the implementation of the CEF Digital programme in support of 5G corridors.

3.2 5G for smart communities

3.2.1 Background

In line with Articles 8(4)a, and 9(4)a of the CEF Regulation[29], CEF Digital will support local innovators to harness the potential of digitisation to efficiently deliver public services, fight depopulation, and enable economic recovery and social cohesion. Connectivity will be a prerequisite and an enabler for such a digital transformation, especially in rural areas.

The CEF support should enable the provision of digital services such as those needed in public administrations, healthcare[30] centres, schools and other education and training institutions to become "smarter", i.e. more efficient, resilient and able to adapt according to the evolving needs of citizens, the environment and the economy and society at large. Therefore, within the context of this action, socio-economic drivers are public administrations or public or private entities entrusted with the operation of services of general interest or of services of economic interest (SGEIs).

By supporting local innovations that are enabled, for example, by standalone 5G systems, such "smart communities" will provide blueprints of digital innovation projects that can be replicated across Europe, for instance under national RRF Plans.

Already today, European cities have bundled their efforts to develop the necessary platforms to provide services enabled by high-speed connectivity[31]. The Digital Education Action Plan (2021-2027)[32] points to connectivity for education and training as a critical component for enabling a high-performing digital education ecosystem. Tackling connectivity gaps is also

---

29 Actions supporting the deployment of and access to very high-capacity networks, including 5G systems, capable of providing Gigabit connectivity in areas where socioeconomic drivers are located

30 E.g. hospitals, large medical centres, solo primary care practices, small primary care practices, nursing homes, rural health clinics, clinics or large physician practices.

31 www.living-in.eu

32 COM/2020/624 final https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-communication-sept2020_en.pdf

one of the key enabling factors suggested under the Structured Dialogue on digital education and skills with Member States. Similarly, recent studies[33] show that healthcare centres need significant bandwidth to cover digital use cases such as electronic health records, real time medical imaging and patient health monitoring. Other use cases benefitting from 5G connectivity could be emergency health monitoring and care in ambulances, or continuous health monitoring and support outside healthcare facilities.

The COVID-19-induced health crisis has further underlined the importance of state-of-the-art connectivity to support the functioning of public administrations as well as the provision of services of general interest and SGEIs, especially in rural areas[34]. Coupling local demand for specific applications tailored to socio-economic drivers with the availability of 5G connectivity funded under CEF Digital will pave the way for concrete 5G-enabled use cases, which will modernise specific sectors and unlock digital growth across Europe.

This would in most cases require backhaul networks connected to public telecom networks and, if appropriate, the interconnection to federated cloud and edge computing services, which are themselves outside the scope of CEF Digital eligible costs.

3.2.2 Objectives

The aim is to support the early deployment of 5G-based systems to enable use cases for socio-economic drivers.

Projects funded under this action are expected to:

a) Deploy 5G infrastructures capable of delivering leading-edge connectivity characteristics e.g.: Gigabit performance, high-user-density, ubiquitous coverage (e.g. to connect IoT devices), low latency and reliability
b) Where necessary, bundle the deployed 5G networks with a cloud-to-edge middleware stack[35] capable of supporting the data-intensive use cases and applications for the involved socio-economic drivers

The action 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 cloud-to-edge systems, eventually relying on technologies and standards developed under other EU programmes, in particular the Digital Europe Programme and Horizon Europe.

The action will produce at least 20 *5G best practices beacons*, covering different areas, that can serve as templates for possible replication under other programmes, in particular RRF. The synergy with RRF and other programmes could encompass wider "local digital transition projects" in which the 5G connectivity would be (co-)funded under CEF and the remaining modules that are non-eligible under CEF (e.g. the deployment of local computing, data or other digital capacities and solutions) would be funded under RRF or other programmes.

---

[33] For example: https://5g-health.org/wp-content/uploads/2020/11/5G-Health-Whitepaper-V1.pdf

[34] 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

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

3.2.3 Implementation

The CEF funding will apply to the deployment or usage of the connectivity infrastructure elements required by local innovation projects which are not already available. The access to an existing 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 network.

Projects would need to demonstrate the credibility of the financing for the remaining parts of the project (infrastructure or otherwise) enabling the intended 5G use cases (e.g. end-user devices, sensors, connectivity subscriptions…) that are not eligible for support under the CEF Regulation. 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 other 5G network is providing services.

Priority will be given to projects that can demonstrate more than one 5G-based use case relying on the same 5G network.

The beneficiaries will be operators that will deploy 5G networks and provide access to 5G services to socio-economic drivers: these targeted end-users can 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 will be 5G radio equipment and – where necessary for installation of additional base stations for densification – the passive infrastructure.

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 Commission will assess the innovation brought by the innovative use case in its evaluation.

The maximum CEF co-financing rate will be 75% of the CEF-eligible costs as a general rule. The financed 5G infrastructure will be dedicated and used to provide 5G services to socio-economic drivers that will provide innovative use cases.

In general, the claimed overall co-funding rate 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 funds (including Cohesion Funds and the RRF), State aid rules within the meaning of Article 107(1) TFEU apply (see section 10 for details). However, since the projects concern the provision of 5G connectivity required to enable use cases by socio-economic drivers that are public administrations or public or private entities entrusted with the operation of services of general interest or of SGEIs (services of economic interest), 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[36] .

[36] Commission Decision of 20 December 2011 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 OJ L 7, 11.1.2012, p. 3

Grants call planning: 5G for Smart Communities			
Type of Call	2021	2022	2023
Works	√	√	√

Benefits and expected outcomes - including EU added value

CEF funding for 5G for smart communities is 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. Such 5G enabled 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.
- 5G-based use cases that leverage new 5G characteristics, e.g.: higher bandwidth and ubiquitous coverage (eMBB), ultra-low latency (uRLLC), massive machine-type (mMTC)[37].
- 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 (such as OpenRAN for example) and contributing to the emergence of a European ecosystem of 5G suppliers.

In addition to the support for local innovation, the EU added value is also based on the dissemination of the early adoption of concrete 5G use cases that will contribute to gaining insights and increasing maturity for 5G-based applications in different sectors, including based on dedicated Programme Support Action (see Section 5.3).

All supported projects are expected to rely on the performance characteristics of 5G technology that are indispensable to implement one or more use cases necessary for socio-economic drivers to deliver new services.

Beneficiaries will be asked to share their knowledge, achievements and lessons learnt, including in the context of the "5G for Smart Communities Support Platform" (section 5.3), in order to demonstrate to citizens the benefits of 5G by providing concrete examples of 5G based use cases for socio-economic drivers.

In order to assess the third award criterion "Priority and urgency of the action", the Commission will consider the relevance to the policy of the relevant sector, in particular for hospitals/ medicals centres and education and training/research centres.

The key performance indicator will reflect the number of new users of the 5G networks and the number of 5G-based use cases enabled as a result of CEF Digital support.

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

Governance, operations and stakeholders involvement

To coordinate and facilitate the sharing of best practices and collaboration between projects, this work programme will support accompanying measures relevant to this topic (c.f. Support Actions sections in this work programme and in particular the Smart Communities Support Platform).

This will include the:

- Sharing of project information that can be useful for project replication (e.g. requirements elicitation, scoping and templates for financial sizing, facilitating identification of complementary funding sources…).
- Use of a broader platform for CEF Digital communication, dissemination of results, community engagement,, mutual learning and sharing of experiences. The "5G for smart communities" projects will be instrumental in providing inputs to this second measure.

In addition, a dedicated Coordination and Support Action (CSA) will support the integration of 5G with cloud and edge computing (see section 5.7 below)

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, e.g. by conveying knowledge and good practices.

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. functioning of healthcare, environmental security, etc.), there is a need to ensure cybersecurity of infrastructures funded under this action. 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.

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

In the context of 5G 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[38]. 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.

This is notably the case for suppliers of equipment (including hardware and software) that implements core network functions, network management and orchestration functions, as well

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

as access network functions.[39] The reason is that the deployment, operation or management of active and/or passive components of the infrastructure, within and beyond the project's duration, may entail security risks for the Union, for instance if critical data are 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, even if the scope of such infrastructure is limited to local communities[40]. Such risks are more likely if the active components and related services will be sourced from suppliers established in or controlled from third countries[41].

As described in section 8.4., *all* works project proposals, to be eligible, shall have to include security declarations by participating companies which demonstrate that the network technologies and equipment (including software and services) funded on the basis of the programme comply with security requirements as specified in the call conditions, in accordance with the applicable EU law, national law, and EU guidance on cybersecurity[42] .

Based on the security declarations in the proposal, as well as the evaluation carried out by independent experts, the Commission or funding body, where appropriate, may carry out a security scrutiny, including as regards beneficiaries' suppliers and sub-contractors. Funding for actions, which do not comply with the conditions related to security, may be suspended, terminated, or reduced at any time in accordance with the Financial Regulation.

Specific measures addressing green policy objectives, in particular in terms of reducing the carbon footprint, would be taken into account.

Each proposal should be supported by local and/or regional authorities in the area where the deployment is foreseen to take place. This support may be in the form of administrative letters, letters of intent, memoranda of understanding, or similar support documents.

---

39 See p. 5 COM(2020) 50 final - Secure 5G deployment in the EU - Implementing the EU toolbox.

40 A local 5G infrastructure supporting critical services in the fields of, for instance, healthcare, environmental monitoring or security, can represent a single point of failure for wider-scale infrastructures (and services) at regional, national or European level.

41 According to the EU coordinated risk assessment, 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.

42 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.

4. EU connectivity backbone infrastructures

4.1 Quantum communication infrastructure - The EuroQCI initiative

4.1.1 Background

Today, 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 new Joint Cybersecurity Strategy,[43] the Commission is working with Member States 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.[44] It will also cooperate with the European Space Agency in this context. 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, i.e. quantum key distribution.

The Union Secure Connectivity Programme aims at providing an EU satellite-based, multi-orbital communication infrastructure for governmental use and developing further and gradually integrating the EuroQCI initiative to allow for quantum distribution of cryptographic keys.

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, it will use existing and new technologies developed and manufactured in the EU.

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

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 such as eavesdropping. The first phase of the EuroQCI infrastructure deployment (2021-2023) will be focused on the deployment of terrestrial backbone components.

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

[43] JOIN(2020) 18 final, 16.12.2020.

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

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. It is also anticipated that Member States will complement actions under CEF Digital and the Digital Europe Programme with funding from the RRF.

4.1.3 Implementation

The following requirements have been set for the prioritisation of 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, built with EU technologies, 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).[45]
- Interconnection with the EuroQCI's space segment, which will be implemented via the optical ground stations serving as an interface between the EuroQCI's space components and its terrestrial fibre network.
- 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. 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 cross-border interconnections and the number of optical ground stations deployed.

Grants call planning: European Quantum Communication Infrastructure	
Type of Call	2024-27
Studies	
Works	√

Benefits and expected outcomes - including EU added value

The funding will:

• Enable reliable and resilient transmission of sensitive communications and data between public authorities, research entities and critical infrastructures in Member States, including outlying territories;

• Boost Europe's capabilities in developing quantum-secure optical telecommunication networks and its capacity to secure its critical public infrastructures, especially those that cross national borders and serve more than one Member State;

[45] The EuroQCI Action Plan states that links between terrestrial networks 'will be guaranteed by a number of trusted nodes, as an interim solution to be replaced later on by solutions extending user connectivity to much larger distances (e.g., by using quantum repeaters, which are now under development in nationally- and EU-funded R&D projects).'

• 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 strategic autonomy and digital sovereignty.

Operations and stakeholder involvement

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

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.

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 and dual-use technologies which will enable the EU and its Member States to safeguard sensitive governmental data and infrastructures against potential interference. Building secure European capacities in developing and producing quantum communication technologies has a strategic importance for the EU in the deployment of security applications and dual-use technologies. For these reasons, security interests of the Union require achieving and maintaining secure capacities in this area and ensuring the security of these critical supply chains.

The deployment, operation or management of quantum communication technologies within and beyond the project's duration, may constitute security threats for the Union, for instance if critical data are shared with un-authorised parties or un-authorised parties are able to influence the use of such technologies or infrastructure. Such risks are more likely if the active components and related services of the quantum communication infrastructure will be sourced from suppliers established or controlled from third countries. Therefore, no security-sensitive equipment or services deployed or used within the project will be procured from third country suppliers. For the reasons above, proposals under this topic will also be subject to Article 11.4 of the CEF Regulation and security guarantees relating to the operational phase shall be provided in accordance with the same security conditions that apply to the deployment phase.

4.2 Backbone networks for pan-European cloud federations

4.2.1 Background

End users' tight budgetary constraints, the growing awareness of cloud technologies' impact on climate change, the relatively low cloud uptake among both the public and private sectors (18%)[46], and the need to enable the free flow of data across the EU are all fuelling the demand for a federated cloud and edge infrastructures. Such infrastructures need to be interconnected in a highly secure, highly energy-efficient, fully interoperable manner, respecting data protection and offering very low latency. This demand is driven by a technological shift in which cloud has become the technology underpinning the uptake of emerging technologies such as AI, Blockchain, IoT and HPC.

Yet, the market for cloud services and infrastructure is highly concentrated among a limited number of companies. While some local alternatives exist at national level, none of the pan-European providers is European-owned. Similarly, DNS[47] resolution, a critical backbone function to access resources on the internet and supporting interconnection, is increasingly concentrated in the hands of a few non-European operators and potentially insecure in terms of privacy safeguards.

This situation is especially problematic for public administrations or public and private entities entrusted with the operation of services of general interest or of Services of General Economic Interest (SGEIs) as well as critical infrastructures, who are in need for particularly robust and secure backbone networks and interconnection services such as DNS resolution. Their respective infrastructures are not properly interconnected and alternative (sub)contractors which could provide such services are either too small or not in line with their high demands in terms of data management [48].

4.2.2 Objectives

Answering this challenge, in its Data Strategy of February 2020[49], the European Commission committed to invest in a High Impact Project on European data spaces, and federated cloud-to-edge infrastructures and services.

Together with the Digital Europe programme, InvestEU and the RRF, CEF Digital will be the catalyst to deploy cross-border and national cloud-to-edge infrastructure interconnections at both the physical (i.e. very high capacity networks) and functional levels (i.e. DNS resolution, management systems and software-defined infrastructures) among socio economic drivers[50] across the EU to the benefit of EU citizens and businesses. The associated architectural requirements to enable security, safety, energy and resource efficiency, data protection and

---

[46] Only 1 company in 4 and 1 in 5 SME are using cloud computing in the EU according to the 2019 Digital Economy and Society Index (DESI)

[47] The Domain Name System is the system allowing connecting a domain name to a resource on the internet, like a website or an application server.

[48] https://ec.europa.eu/digital-single-market/en/news/study-economic-detriment-smes-unfair-and-unbalanced-cloud-computing-contracts; https://ec.europa.eu/digital-single-market/en/reports-and-studies/75981/3494?nr_type=3823&nr_topic&nr_start_date&nr_end_date

[49] COM(2020) 66 final https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

[50] Within the context of this action, socio-economic drivers are public administrations or public or private entities entrusted with the operation of services of general interest or of SGEIs.

interoperability of those interconnections is also an inherent part of this CEF Digital topic. In this context, these federated cloud-to-edge infrastructures 'as a product' will need to:

1. cope with the latest digital and sustainability challenges, in particular:
    - enabling the industrial and low power processing of large amounts of data including in HPCs and at the edge;
    - fostering a swift and sustainable uptake of emerging technologies such as AI applications;
    - supporting the operationalisation of data spaces and specific use cases for socio economic drivers;
2. respond dynamically to the needs of beneficiaries by providing data processing and storage capacities across the EU including at the edge at high speed, with low latency and in an energy and resource efficient manner;
3. leverage high-performance end-to-end backbone connectivity;
4. allow effective access to resources through a high-performance DNS resolution infrastructure, supporting a variety of use cases, conforming to the latest security and privacy standards, guaranteeing data protection according to EU rules, and ensuring a high-level of protection from malware, phishing and cyberattacks;
5. meet EU data-protection, security, portability and environmental requirements; and be role models when implementing forthcoming rules pursuant to the legislative work programme of the European Commission, notably the Data Governance Act, Digital Services Act, Digital Market Act and the Data Act.

4.2.3 Implementation

The projects foreseen for 2021-2023 will focus on the development of cross-border and national cloud infrastructure interconnections at both the physical (i.e. very high capacity networks) and functional levels (i.e. management systems, software-defined infrastructures and DNS resolution) which will ensure distributed, secure, energy-efficient and high-speed connectivity.

Participants will need to demonstrate that they adhere to the data protection, security, portability and energy and resource efficiency requirements applicable to data-processing/storage services and activities developed under the relevant European codes of conduct, initiatives and legislation. Participants should also demonstrate that they have put in place all reasonable technical, legal and organisational measures in order to prevent transfer or access – including unsolicited transfers or access - to personal or non-personal data (including processed data and meta-data) held in the Union that would be unlawful under Union law or applicable national law.

This topic should be read together with the actions foreseen under the Digital Europe Programme (DEP) which focuses on the large scale deployment of the next generation of European cloud to edge services, the associated EU marketplace, and modular middleware platforms for interoperability between different data services.

Where applicable, projects can as well be combined with the RRF in line with State aid rules as relevant, where CEF Digital is used to e.g. interconnect stakeholders across borders and RRF is used to complement with intra-national cloud infrastructure investments.

Federated cloud infrastructures will also gradually need to be interconnected with other cloud, HPC and edge infrastructures, as those data capacities are becoming available. Calls for

feasibility studies for these interconnections will be launched in order to anticipate the technical, legal and economic requirements to progressively establish a fully secured and highly energy-efficient European computing continuum[51].

CEF Digital will co-fund, through grants, the investment costs (feasibility studies, works and equipment) related to the development and deployment of cross-border and national cloud infrastructure interconnections at both the physical (i.e. very high capacity networks) and functional levels (i.e. management systems, software-defined infrastructures and DNS resolution infrastructures) for public administrations or public and private entities entrusted with the operation of services of general interest or of SGEIs across the EU.

Grants call Planning

Type of call and topic	2021	2022	2023	2024	2025	2026	2027
Studies & works for the interconnection of backbone networks for cloud federations	√	√	√		√		
Feasibility studies for the interconnection of backbone networks for cloud federation with other cloud, HPC and edge infrastructures.	√	√					
Works for equipping existing backbone networks with high-performance and secure DNS resolution infrastructures.	√						
Studies & works for the interconnection of backbone networks for cloud federations (federation of federations) and with HPC and edge infrastructures				√		√	
Studies & works for the development of backbone networks for cloud federations and interconnections of cloud infrastructures of economic entities operating in at least one strategic economic sector in the EU.					√		

Benefits and expected outcomes - including EU added value

This topic will support targeted investments to connect cloud and edge infrastructures of the public administrations or public and private entities entrusted with the operation of services of general interest or SGEIs across Member States of the EU. The key benefits include:

a) providing the key data processing infrastructures to support the digital transformation and modernisation of the public sector in Europe;

b) increased competitiveness, cybersecurity and resilience of the EU computing industry in line with EU rules on data protection, security, portability and sustainability;

c) technological autonomy in essential digital computing infrastructures to process EU data, in particular through European common dataspaces; the infrastructure will also be an essential

[51] This computing continuum would encompass highly centralised data processing infrastructures such as HPC and cloud, as well as highly distributed ones such as edge, in a fully integrated and seamlessly interoperable manner.

enabler for the roll-out of emerging technologies, including AI, 'internet of things' (IoT), HPC;

d) energy efficiency and sustainable large scale deployment of interconnected cloud-to-edge infrastructures across the EU territory.

The key performance indicator will reflect the number of data centres of socio economic drivers, including public-sector end-users which will be interconnected physically (fibre) or virtually (new software or middleware deployment).

Governance, operations and stakeholder involvement

The beneficiaries will be public administrations or public and private entities entrusted with the operation of services of general interest or SGEIs. Services of general economic interest (SGEI) are economic activities that public authorities identify as being of particular importance to citizens and that would not be supplied (or would be supplied under different conditions) if there were no public intervention. The concept may apply to different situations and terms, depending on the Member States, but SGEIs can typically range from activities such as postal services, energy supply, or public transport, to social services, such as care for the elderly and disabled, or hospitals being part of national health service, to public education organised within the national educational system funded and supervised by the State.

By making possible the emergence of a European federated cloud-to-edge infrastructure, the cloud interconnections financed under this topic will process data, including sensitive data of European individuals, businesses and public administrations.

Vulnerabilities in the underlying network layer would undermine the resilience of the cloud infrastructure as a whole and the applications deployed on it. Due to the shared nature of these infrastructures, a disruption in a cloud node in one MS could create disruptions in one country and propagate to other Member States and even globally, with unpredictable consequences in economic, legal and public order and security terms.

Cloud services fall within the scope of the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems, which considers relevant cloud service providers as entities that are essential for ensuring a high common level of cybersecurity within the Union. The Commission proposal (COM/2020/823) for a revision of that directive adds edge computing and data centre service providers to the directive's scope. The proposal COM/2020/823 furthermore highlights the necessity for operators of essential services to address the cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers, given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services.

The deployment of a European Cloud infrastructure foresees:

1. development of the EU cloud stack middleware,
2. the deployment of cloud infrastructures and middleware (cloud/edge nodes, including the servers in data centres and related facilities, the deployment of the cloud stack as well as any other service such as DNS, etc.);
3. the connectivity infrastructures (passive fibre + active equipment) needed to connect nodes and regional/national clouds as well as the needed services (DNS) into a federated EU cloud service.

From the security/resilience point of view, the connectivity infrastructure is by definition more critical than the higher layers that rely on it. In essence, with reference to the standard

seven OSI layers describing a network,[52] one could say that the deeper one goes into the layers, the stronger the security requirements needs to be.

The reason is that a collapse of the network infrastructure (in particular at physical, data link and network levels) typically affects higher layers such as the cloud services that run over it (and the applications on top of it). Such an attack would cause the interruption of services that are vital for the functioning of the EU social fabric and would entail enormous economic losses.

Attacks can also take place at higher levels, including those involving users' misbehaviours, however, because of the inherent structure of networks, higher level attacks (e.g. Denial of Service) typically do not affect the integrity of the underlying network. With the usual caveats of an analogy, this could be seen as a home network: if the ADSL connection fails, everything fails (IP telephony, VOD, IT TV, Wifi, etc), but not the other way round (a failing video stream would not have consequences on email traffic). This is why the network layers need to be protected with the highest level of security.

Therefore, in view of the particular sensitivity of cloud infrastructures from a security perspective and the importance to reduce exposure to risks to the maximum possible extent, proposals under this action will be subject to Article 11.4 of the CEF Regulation

In addition, as described in section 8.4., *all* works project proposals, to be eligible, shall have to include security declarations by participating companies which demonstrate that the network technologies and equipment (including software and services) funded on the basis of the programme comply with security requirements as specified in the call conditions, in accordance with the applicable EU law, national law, and EU guidance on cybersecurity[53] and indicate that no security sensitive equipment or services deployed or used within the proposal will be procured from third country suppliers[54].

Conditions and assessments related to the use of suppliers of technologies and equipment are set out in detail in section 8.4.

Proposals should also define the post-project ownership of the infrastructure and provide the necessary security commitments to ensure the continuity of the level of security required during the implementation phase, as well as the operational relationship(s) between the different participants in the value chain. They should explain how operators of essential services related to connectivity involved in the cross-border interconnection of national cloud infrastructures address the cybersecurity risks.

---

52 OSI model describing the overall architecture of a telecommunications network: Layer 7 - Application. Layer 6 - Presentation. Layer 5 - Session. Layer 4 – Transport. Layer 3 - Network. Layer 2 – Data Link.Layer 1 - Physical.

53 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.

54 According to the EU coordinated risk assessment, 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.

Based on the security declarations in the proposal, as well as the evaluation carried out by independent experts, the Commission or funding body, where appropriate, may carry out a security scrutiny, including as regards beneficiaries' suppliers and sub-contractors. Funding for actions, which do not comply with the conditions related to security, may be suspended, terminated, or reduced at any time in accordance with the Financial Regulation.

Specific measures addressing green policy objectives, in particular in terms of reducing the carbon footprint, will be taken into account during the evaluation.

No State aid approval is required, if no public resources are used to co-finance the project. Applicants can find information on when State aid applies and whether it needs to be notified for cloud and edge investment in the State aid Cloud Capabilities Guiding Document[55].

4.3 Backbone connectivity for Digital Global Gateways

4.3.1 Background

In her State of the EU speech on 15 September 2021, Commission's President Ursula von der Leyen stated that the European Union will provide strategic connectivity for all territories of the Union through Digital Global Gateway partnerships. This specifically includes Member States that have islands, and remote territories in the Outermost Regions and Overseas Countries and Territories.

It is of utmost importance to ensure that everybody in the European Union is connected with "quality infrastructure, connecting goods, people and services around the world". By offering transparency and efficient governance, the Union has the ambition to provide trusted connectivity in Member States and partners worldwide.

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.

This backbone connectivity can be provided with the technology best suited, e.g. including submarine cables, satellite ground stations and their possible inter-connections.

Backbone connectivity including submarine cables and satellite-based connectivity play 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[56]), islands and Member States with coastlines, as well as the and Overseas Countries and Territories (OCTs[57]). They 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.

CEF Digital will support the deployment of backbone networks addressing connectivity needs, such as:

- Connecting all territories of the EU including its Outermost Regions.

---

55 https://ec.europa.eu/competition/state_aid/what_is_new/template_RFF_cloud_capabilities.pdf

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

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

- Supporting the specific needs of Member States which are islands themselves, or have islands as part of their territory.
- Intermeshing backbones interconnecting major points of connectivity in the EU.
- Addressing the specific needs of Overseas Countries and Territories in the EU.
- Ensuring international connectivity, to EU partners worldwide as a basis for European digital autonomy.
- Promoting synergy projects addressing other objectives of CEF Digital, including sector specific considerations encompassing the connectivity of large-scale digital capacities such as HPC or cloud.

4.3.2 Objectives

The objective of this action is to deploy strategic networks as part of the Digital Global Gateway Strategy of the EU, contributing to strengthen the quality of connectivity within the Union, as well as with third countries. This includes submarine cables, 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 strengthening the connectivity capacity, but also on facilitating commercial offers of connectivity.

CEF Digital will support the deployment of new and significant upgrade of connectivity routes, for which the market alone will not invest, and for routes (within Member States, between Member States, and between the EU and third countries), including Outermost Regions and other remote territories, where:

- Existing infrastructure cannot satisfy demonstrated demand to provide affordable and adequate services in line with the EU connectivity objectives for 2030[58] taking for instance into account, among others, the lack of sufficient capacity, excessively high prices that have the effect of discouraging take up and innovation compared to prices charged for the same services in more competitive, but otherwise comparable areas or regions; or

- 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 served already by at least two present or credibly planned submarine cables, as it is presumed that redundancy is addressed by the two infrastructures. Only 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, will the presence of such infrastructure be taken into account when assessing the lack of redundancy.

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

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

4.3.3 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 Outermost Regions, islands, and Overseas Countries and Territories, the commercial prices and other conditions of connectivity 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 experiment 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. Proposals must therefore include a description of whether or how they intend to provide wholesale access to third parties. Amongst 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.

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, and in order to take advantage of the reinforced backbone infrastructure, in areas where there is no access network capable of supporting gigabit connectivity and such infrastructure is unlikely to be developed in the near future, project costs may also include costs required to construct the local access network if these solutions address the identified market failure and provide a sufficient step change. In such a case, costs related to the deployment or significant improvement of the access network 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	2021	2022	2023
Studies	√		√
Works	√	√	√

Benefits and expected outcomes - including EU added value

The capacity and resilience of the overall network infrastructure benefit all EU citizens. Even in landlocked Member States, users often depend on international connectivity and contribute

to the traffic routed via international connectivity systems without knowing it. It is therefore necessary for the EU to secure the competitive availability, reliability and resilience of such vital infrastructures.

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

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

Governance, operations and stakeholders involvement

Beneficiaries can take the form of consortia, including (local) operators, utilities, (local) authorities, investors and vendors.

The proposal 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.

Given this relevance of submarine cable and satellite infrastructure to public security, including of an international, geo-political scope, there is a need to ensure strict cybersecurity in this field.

The purpose of submarine cables and satellite infrastructures 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 citizens, 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 cyberattack perpetrated, for instance, against a submarine cable that ensures the digital inclusion of European islands could compromise the entire economy of such regions and of the Union at large.

Effectively, backbone networks deployed to provide the necessary redundancy for connecting the Union with third countries or connecting European islands and that contribute to increasing the capacity and resilience of the Union's digital networks should comply with the highest possible security standards and the strictest level of protection against cybersecurity attacks.

As set out in the proposal for a revised NIS Directive (Recital 51), 'The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place'.

The EU Digital Gateway Ministerial Declaration states that 'Besides a strong legal framework and high quality internal infrastructure, the EU needs to ensure future proof high quality connections to the rest of the world if it is to become such a hub and ensure that the services

provided can be offered on a worldwide basis. It is also of critical importance that European security and prosperity is not undermined by high-risk vendors.'

The Declaration notably calls for 'Increasing where needed and securing submarine connectivity', stating that 'Submarine cables are essential in order to sustain the exponential increase in internet traffic volumes and ensure the security, stability and resilience of the open internet' (…). It also underlines the need to 'expand space-based secure connectivity', which 'can help to increase the overall resilience, strategic autonomy and cybersecurity of the EU'.

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.

In this context, the role of entities supplying or managing equipment (including hardware and software) that implements and manage/operate 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 citizens 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-authorized parties or un-authorized 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 Digital Global Gateways strategy of the Union.

Therefore, in view of the particular sensitivity of backbones infrastructures for the Digital Global Gateways from a security perspective and the importance to reduce exposure to risks to the maximum possible extent, proposals under this 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 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.

In any case, *all* works project proposals, to be eligible, shall have to include security declarations as described in section 8.4., by the participating companies 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[59] and indicate that no

[59] 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.

equipment or services deployed or used within the proposal will be procured from third country suppliers [60].

Conditions and assessments related to the use of suppliers of technologies and equipment are set out in detail in section 8.4.

Based on the security declaration in the proposal, as well as the evaluation carried out by independent experts, the Commission or funding body, where appropriate, may carry out a security scrutiny, including as regards beneficiaries' suppliers and sub-contractors. Funding for actions, which do not comply with the conditions related to security, may be suspended, terminated, or reduced at any time in accordance with the Financial Regulation.

4.4 Terabit connectivity for High Performance Computing

Background

In line with articles 8(3)d and 9(4)d of the CEF Regulation regarding support for the deployment of new or significant upgrade existing backbone networks, which contribute significantly to the increased performance, resilience and very high capacity of the electronic communications networks, CEF Digital will support the interconnections between EuroHPC supercomputers, national High Performance Computing (HPC) and research centres, data infrastructures and participating countries with ultrafast connectivity.

Europe's leading role in the data economy and its digital autonomy depends on its capability to develop and master the next generation of HPC. HPC is the "engine" that powers the data economy, enabling key technologies like Artificial Intelligence (AI), data analytics and cybersecurity to exploit the enormous potential of big data. HPC is a transforming technology used in hundreds of applications that play a major role in boosting industry's innovation capability, advancing science, and improving the quality of life of citizens in the next decade. These could include for example, personalised medicine (design of new vaccines and drugs), clean energy (e.g., fusion energy simulators, evaluation of carbon reduction measures, the design of performant photovoltaic materials or optimising turbines for electricity production), etc.

The mission of the EuroHPC Joint Undertaking (EuroHPC JU), set up in October 2018, is to develop, deploy, extend and maintain in the EU an integrated world-class exascale supercomputing and data infrastructure, and to develop and support a highly competitive and innovative HPC ecosystem. In this context, the EuroHPC has already successfully started towards making Europe a top supercomputing region globally, with the acquisition of seven world-class supercomputers to be installed in seven Member States in 2021/2022. This supercomputing infrastructure will multiply at least by eight the available computing power at European level, addressing the need for computing and data resources for European industry and science.

The new Council Regulation (EU) 2021/1173 on establishing the European High Performance Computing Joint Undertaking (EuroHPC JU) sets out an ambitious mission and a substantially larger budget for the period 2021-2027.

---

[60] According to the EU coordinated risk assessment, 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.

Strategic priorities

The Commission foresees actions to support the connectivity aspect, which is considered critical for the success of the EuroHPC JU. The effective and efficient use of the future European HPC, quantum computing and data infrastructures will largely depend on a secure hyper-connection (at terabit level) of the centres hosting the EuroHPC supercomputers and quantum computers and other national HPC and data infrastructures.

Novel and future applications that depend on human intervention will require real-time and/or interactive computing, in which high-speed connectivity is essential for a fast access to the scattered big data and HPC resources and applications in which time is critical to ultimately save lives or reduce material impacts.

The scheduling of the demand-oriented and user-driven deployment of the HPC interconnection infrastructure and associated services will take into account the complementarity and synergies with the other HPC related activities supported by the Digital Europe and Horizon Europe programmes. For example, the procurement of new supercomputers and their operation foreseen in the Digital Europe programme. In this context, terabit connectivity between the acquired EuroHPC supercomputers will become a priority when these new supercomputers become operational.

CEF Digital support for terabit connectivity for HPCs will be implemented through the EuroHPC JU. Its Governing Board will prepare a dedicated work programme for the activities to be supported, as specified in the EuroHPC JU legal base. The budget to be delegated to the EuroHPC JU is EUR 200 million for the 2021-27 period.

The European High Performance Computing related backbone communications networks, which will facilitate cross-border Terabit connectivity and service provisioning between nodes of the pan-European HPC infrastructure and the participating countries national access infrastructures and EU research data centres, are part of Europe's critical infrastructure that needs to be protected from cyber-attacks and other security threats.

Given their key role in the functioning of EU's data and quantum computing infrastructures and, given the potential sensitivity of the data transported (including for instance nuclear research simulations), as well as the real time critical applications during emergency situations using dedicated supercomputing resources (meant to, for example, save lives by promptly forecasting and mitigating the impacts triggered by catastrophic phenomena such as tsunamis, earthquakes, and volcanoes), the integrity, resilience and security of these backbone networks interconnecting the pan-European HPC infrastructure and their access have to be duly safeguarded.

In view of the above, the eligibility to participate in the CEF funded actions for HPC backbones will have to be, where appropriate, based on the application of Article 11(4) of the CEF Regulation. To this end, appropriate security conditions concerning the participating entities and the equipment to be procured and used will have to be provided for in the dedicated EuroHPC work programme to be adopted by the EuroHPC JU Governing Board.

5. Synergy and Programme support actions

Where possible, as indicated under chapter 8 below, CEF Digital will ensure synergies with the CEF Transport and CEF Energy, taking into account, for instance, that the deployment of digital, transport and energy network infrastructure can share a number of passive network elements and associated facilities such as the civil engineering work and ducts for the deployment of dark fibre.

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

5.1 Operational digital platforms

5.1.1 Background

To reduce carbon dioxide emissions and achieve the digital transformation of the EU economy there is a need for greater convergence of the transport, energy and digital sectors. Synergies between these three sectors could be improved through more efficient and effective use of EU funds.

CEF Digital will fund Operational Digital Platforms (ODPs) to support digital services in the energy and transport sectors to be implemented across borders in the European Union. These synergies will have a leverage effect on the innovation of the energy and transport infrastructures. They will also provide spill-over opportunities for the public and private sector to re-use the underlying digital connectivity infrastructures for multiple purposes.

Due to the national and regional nature of stakeholder activities in the energy and transport sectors, the market has failed to deploy the necessary cross-border infrastructure for an EU level exchange of data in real-time. To fill this gap, in a 2-phased approach, CEF Digital will support a Coordination and Support Action (CSA) for an exploratory phase, to be launched in the first Call of this work programme, to identify the type of intervention which yields the highest impact and addresses the highest degree of market failure. This CSA will prepare for one or more works project(s) under the next work programme.

ODPs are physical and virtual information communication technology resources, operating via the communication infrastructure, which support the flow, storage, processing and analysis of transport or energy data, or both. Examples of potential use cases include:

- **Energy sector**: a platform with information on available energy from renewable sources to optimise the use of such energy generated throughout the EU and transmitted across its borders. The platform would build on high-capacity low latency cross-border connectivity, energy efficient cloud and edge data centres and smart electricity grids. Such a platform would help reduce the environmental footprint, balance the grid, enable the integration of renewable energy in the system and facilitate exchange and collection of information. Future scenarios include bi-directional EV-charging, to help balance the grid and shave peak consumption by enabling energy to be fed back to the electricity grid from the batteries of electric vehicles.
- **Mobility sector:** a platform to facilitate the efficient real-time cross-border use of available transport and intermodal routes and logistics for freight and passengers. It would enable the exchange and collection of information and help to reduce the environmental

footprint of cross-border transport, shorten the travel times and improve users' experience. Much like in the energy case, the platform would build on high-capacity low latency cross-border connectivity and energy efficient and trustworthy cloud and edge. Such a platform would interact with the electricity grid to minimise the inactivity time of electric vehicles, reduce charging costs and help balance the grid through flexible demand.

ODPs build on and integrate with existing and emerging European data, cloud and edge computing infrastructures. They include hardware (sensors, actuators, servers, storage subsystems, and networking devices like switches, routers and firewalls) and software (e.g. databases, analytics, artificial intelligence algorithms, simulation, data management, cybersecurity tools, software platforms).

5.1.2 Objectives

Synergy actions aim to support EU environmental and energy targets, by providing both technologies and connectivity to enable a cyber-secure Internet of Energy and an optimised transport system along the major European paths, in line with the 5G cybersecurity toolbox. This will optimise energy use of ICT and reduce the environmental impact, while increasing the benefits enabled by ICT.

5.1.3 Implementation 2021-2027

This topic will be funded on the basis of the eligible "actions implementing digital connectivity infrastructure requirements 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" (Article 8.4(e) and Article 9.4(e) of the CEF Regulation).

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.

This topic will be implemented in two phases via two interlinked actions: a Coordination and Support Action (CSA) in the current CEF Digital work programme and (a) works project(s) in the future CEF Digital work programme 2024-2027.

Coordination and Support Action

The CSA will prepare the works project(s) by identifying the most appropriate cases to be funded and by delivering the building blocks (such as governance, detailed design, etc.) needed for immediate deployment of the cross-border infrastructure within the works project. It will consist of four phases and it should last 27 months.

The first stage will consist of an exploratory study and will last 5 months. It will provide the following outcomes:

- Define the needs in digitalising the cross-border energy and/or transport infrastructure between Member States;
- Identify criteria and recommendations for selecting appropriate and most credible, within standard constraints (e.g. of budget, timing, complementarity to emerging European infrastructures in the targeted sectors), lead use cases and potential project(s), i.e. the most mature and realistic, with the highest degree of market failure, the most impactful, etc.;
- Identify relevant technologies, architectures and standards;

- Identify relevant stakeholders;
- Identify possible governance options;
- Develop the design principles and architecture for connecting the ODPs to the 5G infrastructures along transport corridors and smart communities; the emerging dataspaces in particular in the energy, mobility and related sectors; and the federation of European Cloud and edge services. In that context, the tenderers will collaborate closely with the Coordination and Support Actions and deployment projects supported under CEF Digital and Digital Europe Programmes;
- Identify at least 10 lead cases involving at least 9 Member States (preferably at least 12) in energy, mobility and cross-sector energy/mobility;
- Shortlist six cases, based on the criteria and recommendations identified earlier, while trying to maintain at least relative balance between energy, mobility and combined projects (priority given to combined projects).

The second phase will be a feasibility study for the six shortlisted cases from the first phase and it will last 7 months. It will deliver the following outcomes:

- For each case, create a high-level description, solution architecture and governance scheme;
- Based on these, create a cost-benefits analysis;
- Define the feasibility of each proposal i.e. how realistic is each case within the constraints;
- Shortlist three proposals, which are feasible and with the best cost-benefits outcome. For cases with similar characteristics, priority should be given to cross-sector cases between energy and mobility.
- Prepare a draft for the call text for the works call to be handed over to the Commission.

The third phase will be the detailed preparations for the three shortlisted cases from the second phase and it will last 9 months. It will deliver, to the extent possible, the following outcomes:

- Create detailed design/architecture for each of the cases;
- Define key performance indicators for each of the cases;
- Create detailed governance scheme and get feed-back and buy-in from the identified stakeholders;
- Set up governance bodies with the most relevant stakeholders and have a governance agreement signed for each of the three cases;
- Prepare procurement templates and framework agreements;
- Prepare purchasing orders for potential suppliers for the final deployment including integration and SLAs;
- Deploy testing environment from willing suppliers and test the solution;
- Deploy pilot solutions from willing suppliers involving at least 2 and preferably 3 Member States and pilot the solution.

The fourth and final phase will be the assistance to the works projects, which will last six months. This phase will run in parallel with the first six months of the works project(s) and it will serve to transfer the outcomes to the work project(s) and to assist them in the start of implementation. It will consist of the following tasks:

- Transfer all documentation and know-how;
- Fine-tune the documentation according to the works project reality;
- Prepare recommendations for future work.

Under guidance of the Commission (The Directorates-General for Communications Networks, Content and Technology (co-ordination), for Energy and for Mobility and Transport), the proposers will co-operate closely with the relevant national and EU authorities, as well as associations and multipliers across the relevant sectors.

Works projects:

Based on the outcomes of the CSA, the works project(s) selected via the call published in the second CEF Digital work programme (2024-2027) will deploy platforms which provide the necessary infrastructure to support the cross-border availability of digital services in the energy and transport networks. In particular, they will address interoperability issues related to different standards and different technologies used by largely national level operators.

ODPs works project(s) will build on and integrate with existing and emerging platforms as well as data exchange frameworks established according to EU law and in the context of EU expert groups and initiatives, emerging European dataspaces, federated Cloud and edge computing services, and 5G connectivity infrastructures along corridors and in smart communities, which are supported in parallel in the CEF Digital and Digital Europe programmes. Project(s) may need to procure and operate hardware or software to connect to these infrastructures (e.g. edge computing nodes). Where relevant the project(s) shall build on previous EU funded research and infrastructure projects.

Project(s) will be strongly encouraged to use possibilities for financial synergies such as cumulative funding (e.g. ERDF, national) and linking to emerging multi-country projects under the Recovery and Resilience Facility (RRF). The State-aid dimension shall be carefully considered.

Grants call planning: Operational Digital Platforms							
Type of Call	2021	2022	2023	2024	2025	2026	2027
Works				√			
CSA		√					

Indicative budget for the CSA: EUR 4 mil.

Benefits and expected outcomes - including EU added value

A joint European approach is needed for this action to enhance interoperability and standardisation of the appropriate ICT solutions that would not happen without initial public funding. Such intervention is also expected to trigger a public-private partnership virtuous circle of investment.

Basic investments in energy and transport will focus on retro-fitting existing energy and/or transport infrastructure with the required cross-border ODP infrastructure. The latter will build on and integrate with existing and emerging European data, cloud and edge computing and connectivity infrastructures.

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 consortium for the first phase (CSA) will be made up of representatives, or participants well balanced across the relevant stakeholder groups and sectors. In case the consortium does not have enough participants to provide the required balanced representation then these participants should be neutral i.e. in that case they should have no self-interest in a particular outcome of the CSA. Some third parties could be subcontracted for the purpose of building an advisory group, attracting additional expertise from outside the consortium, participation in governance bodies, preparation of the works, etc.

The beneficiaries for the works phase can take the form of consortia, including *inter alia* local authorities, national authorities, energy companies, transport/mobility companies, road 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 wholesale access to the infrastructure shall be made, including related to new entities joining at a later stage.

5.2 Studies, communication and other measures

Studies

As an indicative and non-exhaustive list, studies might cover:

- The evolution of broadband connectivity needs and the technologies supporting them,
- The monitoring of the deployment and characterisation of (cloud) edge nodes in each Member State.

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 citizens, 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 local communities, 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

- Contributing to the development, maintenance and efficient use of the IT systems, including managing the CEF Telecom legacy projects.
- Supporting evaluation and project reviews.

Indicative budget: EUR 9.500.000 for 2021-23 for Studies, Communication and other measures.

5.3 5G for Smart Communities Support Platform

Context

The preparation of quality proposals for 5G-based use-cases may require substantial effort and expertise, which may not necessarily be available in local communities.

The task may become even more challenging due to the shortage of high digital skills to design and implement local digital transformation projects. In addition, some socio-economic drivers, such as small schools or hospitals, may lack the capacity to embark in such an endeavour and would face further challenges in developing a sound "5G use-cases based project".

From understanding the technology, eliciting requirements, identifying main players, scoping the financial implications, to the final application for funding and implementation of the project – the process could become too complex for small entities.

Objectives

The objective of this coordination and support action is to build a community of best practices across Europe able to provide guidance and support to socio-economic drivers, when elaborating their 5G-based use-case proposals. This action will also aim to facilitate the replicability of the best practices matured under the "5G for Smart Communities" actions under other programmes, in particular the RRF Plans.

The action should develop and maintain a knowledge base with 5G-based use-cases pertinent to the socio-economic drivers with particular focus on education and training, health, public services, as well as smart community applications requiring 5G quality of connectivity. Synergies with smart cities initiatives and organisations funded under other programmes would be beneficial.

It should also develop templates to ease the elaboration of "5G for Smart Communities" proposals (cost items for typical use-cases identified, work breakdown elements, list of mobile operators per regions…).

The action would proactively reach out to existing vertical sectors communities to raise awareness of 5G potential in their sectors (e.g. newsletter with examples, networking, workshops…) and foster the exchange of best practises. It would also act as a broker to channel socio-economic drivers to the other interlocutors (Broadband Competence Offices,

Mobile Operators, Technology Providers, previous projects with similar goals, links with national relevant programmes…), ease coordination tasks or provide specific guidance on demand for instance.

Indicative budget: EUR 1,5 million

5.4 Programme Monitoring and Impact

The Commission plans to develop a dashboard for the monitoring of the European connectivity infrastructure. The annual process used for the telecom section of the DESI index would be the baseline, with a goal to streamline and automate the process of gathering broadband coverage and take up data.

The Commission will procure via framework contracts and/or call for tenders services aimed at monitoring the outcomes of the Programme, its funded actions and their intended impact.

Indicative budget: EUR 400.000 for 2021-23.

5.5 Broadband Competence Offices Support Facility

This work programme will continue to support the Broadband Competence Offices[61] (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 will cover the identification and mapping of Gigabit 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 Telecom work programmes provided EUR 0.333 million per year to support the Broadband Competence Offices.

Indicative budget: EUR 1 million for 2021-23.

5.6 5G Strategic Deployment Agenda coordination

A coordination and support action will be funded, which will - in close cooperation with the Smart Networks and Services Joint Undertaking - support the overall stakeholder engagement (especially mobile network operators, operators deploying infrastructure and associated facilities such as tower companies, telecom backhaul operators, road operators, rail infrastructure managers, automotive manufacturers, and mobility service providers) and their networking. It will also finance actions to coordinate the development of Strategic

[61] 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.

Deployment Agendas[62], facilitate project pipelines, elaborate best practices of studies and deployment projects to cover common challenges (e.g. local breakout), performance evaluation across projects and legal constraints (e.g. lawful interception, spectrum coordination, etc.), support progress monitoring, etc.

Indicative budget: EUR 1 million for 2021-23.

5.7 Integration of 5G with edge computing and federated cloud facilities

A dedicated programme support action will be launched in 2022 to accelerate the development and deployment of edge computing solutions as part of 5G actions (both 5G corridors and 5G for smart communities) and for ensuring an integrated approach with the development of European federated cloud and edge infrastructures funded under CEF Digital and Digital Europe. It will accompany 5G deployment projects to develop concepts and deploy facilities for the interconnection of newly deployed 5G infrastructure (both in corridor sections and in smart communities) with edge computing facilities and federated cloud infrastructures. It will also support integration with relevant operational service platforms that enable the provision of CCAM and high-value commercial 5G connectivity services as well as the support of smart communities.

Indicative budget: EUR 2 million for 2021-23.

5.8 Overview of Programme support actions 2021-23

(Budget line 02 03 03 01)

Type	Title	Form[63]	Indicative amount (EUR)
CSA	Communication and Dissemination	P	1 200 000
CSA	Programme Monitoring and Impact	P	400 000
CSA	5G Strategic Deployment Agenda coordination	G	1 000 000
CSA	Integration of 5G with edge computing and federated cloud facilities	G	2 000 000
CSA	5G Smart Communities Support Platform	P	1 500 000
CSA	Preparation of works for Operational digital platforms	G	4 000 000
CSA	Support for the network of Broadband Competence Offices	P	1 000 000
Studies	See 5.2	P	600 000
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	P	6 900 000

[62] https://5g-ppp.eu/europe-sets-5g-sda-for-cam/

[63] CSA = Coordination and support action; P=procurement; G=grant (100% funding)

	programme.		
	Call evaluations and project reviews	P	500 000
Total			19 100 000

Total indicative amount for procurement: EUR 12 100 000.

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

6.1 Main implementation measures and EU financial contribution

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, and with the EU covering the totality of the cost and owning the results and the related intellectual property and exploitation rights[64].

CEF Digital may also contribute to blending operations in accordance with the InvestEU Regulation and Title X of the Financial Regulation, or on the basis of Article 17 of the CEF Regulation for combinations of grants with other sources of financing (i.e. with blending facilities). CEF Digital support may also be delivered by means of a voucher scheme (lump sum grants), if specified in the call text.

EU financial support shall take the form of reimbursement of eligible costs actually incurred, as provided in Article 125(1)(b) of Regulation (EU) No 2018/1046[65], or of simplified forms of funding as defined in the Article 125(1)(a), (c), (d), (e) and/ or (f) of Regulation (EU) No 2018/1046 where specified in the call documentation.

Where EU financial support takes the form of reimbursement of eligible costs actually incurred, the following maximum co-financing rates shall apply to the eligible costs, in accordance with Article 15 of the CEF Regulation:

For works in the digital sector, the amount of EU financial support shall not exceed 30% of the eligible costs 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 in the outermost regions, up to 75% for actions implementing Gigabit connectivity for socio-economic drivers. Actions in the field of providing wireless connectivity in local communities, when implemented via low-value grants, may be funded up to 100% of eligible costs.

---

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

65 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)

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

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

6.2 CEF Digital Connectivity blending facility under Article 17 of the CEF Regulation

In the previous programming period (2014-2020), the Commission successfully launched a CEF "blending facility" as a cooperation framework between the European Commission and various "Implementing Partners" (IPs) such as the EIB, the EBRD, and various National Promotional Banks and Institutions (NPBIs) for transport projects[66]. The aim of this direct cooperation with financial institutions in Member States was to support projects with a combination of CEF investment grants (managed under Title VIII of the Financial Regulation) and financing in repayable form from the IPs, such as loans or equity capital, possibly together with established commercial partners.

For the 2021-2027 programming period, the Commission intends to also establish a CEF Digital blending facility for digital infrastructure investments eligible under the CEF Regulation, in close cooperation with the EIB, the EBRD, NPBIs and other interested IPs.

The blending facility offers several benefits, including:

- Simplified access to EU financing for potential project beneficiaries interested in attracting market-based financing, but which are in need of support through grants;
- Support for 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;
- Alignment of the grant award procedure decision to the project lifecycle: under the blending facility, projects can apply when ready (e.g. after the bank's due diligence) on a rolling basis (as opposed to a fixed deadline under traditional calls for proposals); and
- Increased certainty on the financial soundness and operational readiness of projects through bank co-financing and implementation in time and budget.

6.2.1 Scope

The scope of the Digital Connectivity Blending calls will be limited to the funding actions possible according to Art. 9(4) of the CEF Regulation and in response to 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.

6.2.2 Delivery mechanism

The first step is the conclusion of an "Administrative Agreement" between the Commission and each IP. Such agreement will detail the exact scope and duties of the Mandate henceforth given by the Commission to each IP, which will comprise mainly two activities:

- Activity 1: Initial screening of projects and possible consultation on the Project Pipeline
- Activity 2: Preparation and submission of the Operation File to the CEF Blending call

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

Any project supported by the IP shall present a favourable socio-economic cost/benefit ratio, and be subject to its standard due diligence process in terms of financial, social, economic, legal, risk or compliance assessment.

To be eligible, each grant application submitted by an applicant/project promoter under the Blending Facility shall include the Operation File signed by the IP.

6.2.3 Implementation

Blending calls will be organized on topics described in this work programme when and where the IPs see most potential to leverage private investments with additional public support for PCIs in the area of digital connectivity infrastructure as defined in Article 8 of the CEF Regulation.

7. Indicative timetable and budget for the calls for proposals 2021-2023

7.1 Indicative call planning, per topic

Topic	Type of call	2021[67]	2022	2023
5G corridors, including early wave actions for the interconnection of 5G edge computing facilities	Studies	√		√
	Works	√	√	√
5G for smart communities	Studies			
	Works	√	√	√
Backbone networks for pan-European cloud federations - Interconnection of backbone networks for cloud federations	Studies & works	√	√	√
Backbone networks for pan-European cloud federations - The interconnection of backbone networks for cloud federation with other cloud, HPC and edge infrastructures	Studies	√	√	
Backbone networks for pan-European cloud federations - Equipping existing backbone networks with DNS resolution infrastructures	Works	√		
Backbone connectivity for Digital Global Gateways	Study	√		√
	Works	√	√	√
Operational digital platforms	Support action	√		

[67] Due to the later adoption of the work programme, calls initially envisaged in 2021 will be issued in early 2022.

7.2 Indicative amounts available for the topics and calls

Budget line: 02 03 03 01

Legal base	Topic	Call 2021[68]	Call 2022	Call 2023	Procurement	Total 2021-23	Total 2021-27
Art. 8.4.c, Art. 9.4.c Deployment of 5G corridors along major transport paths	5G coverage along transport corridors, including interconnection of 5G edge computing facilities	41,6	28	160		229,6	*800*
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.	5G for Smart Communities	21,7	50	40		111,7	*141,7*
Art. 8.4.d, Art. 9.4.d Deployment or significant upgrade of cross-border backbone networks	Quantum communication infrastructure	0	0	0		0	*90*
	Backbone networks for pan-European cloud federations	3,3	3	20		26,3	*100,3*
	Backbone connectivity for Digital Global Gateways	82	153	60		295	*389*
Art. 8.4.e, Art.9.4.e Deployment of operational digital platforms	Operational digital platforms	0	0	0		0	*19*
Art. 9.1 Actions contributing to the achievement of the objectives of the programme	Programme Support Actions	1	6	0	12,1	19,1	*28*
Total (EUR million, current prices)		***149,6***	***240***	***280***	***12,1***	***681,7***	***1568***

[68] Due to the later adoption of the work programme, budget initially planned for year 2021 will be committed throughout year 2022, possibly in combination with 2022 budget.

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. Cybersecurity

Cross-border and internal member state infrastructures funded under CEF must comply with the highest security standards because they underpin the entire economy and society and vulnerabilities of those infrastructures can undermine public order and security within the Union.

Protecting the Union's security encompasses, for example, the protection of the EU 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 telecommunications 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 networks, road safety, protection of confidential information, effective functioning of justice and police, water supply networks, 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).

This is particularly the case for backbone networks described under section 4 and for 5G infrastructures described under section 3 above. For these reasons, stringent requirements as regards cyber security 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), in accordance with Article 11.4 of the CEF Regulation
- Conditions and assessments related to the supply of technologies and equipment (see section 8.4) applicable to proposals

8.3 Eligible applicants

Article 11 of the CEF Regulation lays down the eligibility criteria that apply, in addition to the criteria set out in Article 197 of the Financial Regulation.

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 requires the most appropriate safeguards, applicable to all entities, in terms of eligibility.

Operators 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.

A similar reasoning can be applied to equipment suppliers. It cannot be guaranteed from the outset that equipment manufactured in third countries does not embed functions or components that introduce vulnerabilities undermining the cybersecurity of the Union[69]. Therefore, the measure of exclusion of non-EU suppliers applicable to certain CEF actions is necessary and proportionate to the critical importance of the deployed infrastructures.

For the security reasons specified above under section 8.2 and in the sections 3 and 4 describing the individual topics, specific conditions will apply concerning participation in CEF Digital calls.[70]

For actions in the areas "EuroQCI", "Cloud federations" and "Backbone connectivity for Digital Global Gateways" this work programme excludes the participation of non-EU controlled entities on the basis of Article 11(4) of the CEF Regulation. This exclusion does not apply to entities established in the EU for which neither EU, nor non-EU control can be established, on the condition that those entities provide security guarantees approved[71] by the Member State in which they are established, on the basis of national law. The requirement to provide security guarantees for those entities is justified in view of the uncertainty as to their control and the risk of abuse of the procedure for determining the control.

These guarantees shall certify that the legal entity is not subject to non-eligible third country jurisdiction obligations that may undermine the security of the Union, and that the results of the CEF funded action will remain within the beneficiary/beneficiaries, and will 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.

For the topics "5G corridors" and "5G for smart communities", applicants shall be eligible to receive Union financial support conditional on providing security guarantees approved by the Member State[72] in which they are established, on the basis of national law.

The applicants for those topics could also be exposed to the risks of undue influence from third countries. Moreover, in order to achieve and maintain the highest level of cybersecurity protection, the strictest level of control will therefore have to be exercised on all participants

---

69 According to the EU coordinated risk assessment, 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.

70 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."

71 The approval can be provided in the context of Art 11.6, which says:
"To be eligible, proposals shall be submitted:(a)by one or more Member States; or (b)with the agreement of the Member States concerned, by international organisations, joint undertakings, or by public or private undertakings or bodies, including regional or local authorities. If the Member State concerned does not agree with a submission under point (b) of the first subparagraph, it shall communicate that information accordingly.

72 Same as footnote 71.

both during the actual project and thereafter, for as long as they remain responsible for operating the infrastructure which they have developed.

The security guarantees provided by applicants for the "5G corridors" and "5G for smart communities" topics shall certify that the legal entity:

1. 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 and is not subject to non-eligible third countryjurisdiction obligations that may undermine the security of the Union;
2. Effectively prevents access by non-eligible third countries or by non-eligible third country entities to classified and non-classified sensitive information relating to the action;
3. 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;
4. The involved legal entity fulfils the strictest cybersecurity requirements imposed by national law, on the basis of the 5G toolbox and relevant EU law, of all the Member States where the deployed infrastructure is located.

Concerning infrastructures connecting the EU with third countries, legal entities established in third countries would 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 conditional on submitting a declaration, approved by the connected third country, providing the guarantees set out under points a) to c) above, as well as ensuring that the involved legal entity fulfils the cybersecurity requirements set out in the 5G security toolbox.

8.4 Eligible applications

Assessments related to the use of suppliers of technologies and equipment need to be applied to all proposals. For the topics "EuroQCI", "Cloud federations" and "Backbone infrastructures for Global Gateways", the default approach is that the deployed security-sensitive active components funded under CEF Digital should be provided by suppliers established in and controlled by (entities established in) EU Member States.

For 5G-related projects, cybersecurity risks arising from the involvement of suppliers are more likely in case suppliers are established in or controlled from third countries[73]. Given their degree of sensitivity and role as backbone of the Union connectivity infrastructure, this is also relevant for the backbone infrastructures funded under this programme.

Therefore, to be eligible, all proposals for works shall include security declarations by the participating entities. 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

[73] According to the EU coordinated risk assessment of 5G networks, the risk profile 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.

guidance in place on cybersecurity[74]and 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.

For specific topics, the call conditions may require that the declarations ensure the alignment of the proposal's security approach with the strictest security requirements applicable amongst the concerned EU Member States where the entities involved are established. The call conditions may also require operators to indicate that any equipment from third country suppliers will be sourced from suppliers originating in, or controlled from third countries with which Member States, or the EU, have security agreements or similar arrangements (including e.g. data adequacy decisions, data protection agreements,…). This should apply to manufacturers of equipment, as well as suppliers of relevant services.[75]

The content of the declarations will be assessed during the evaluation phase.

Based on this security declaration, as well as the evaluation carried out by independent experts, the Commission (or funding body) may carry out a security scrutiny, 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.

For the topics "5G corridors" and "5G for smart communities", the relevant applicants should demonstrate that they are able to deploy, operate networks and/or provide electronic communication services in accordance with the EU and national law.

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[76], as specified in the call for proposals.

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.

---

74 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.

75 In particular, telecom operators may rely on third party entities to perform certain tasks, such as the maintenance and upgrade of the networks and software, as well as other outsourced managed services, in addition to the supply of network equipment. This may constitute a source of security risk. Thus, a thorough security assessment may also be required of the risk profile of the suppliers tasked with these services, in particular when these tasks are not performed in the EU.

76 Article 9 of the CEF Regulation

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 neighbouring/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:

- **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 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 particular for Outermost Regions and islands. Moreover, the criterion will assess, where applicable, potential complementarities with other public funding programmes.

- **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 ensuring a geographical balance of the CEF digital support in the respective area.

- **Catalytic effect of EU assistance:** evaluating: i) the financial gap (for instance the need to overcome financial obstacles generated by insufficient commercial viability, high upfront costs or the lack of market finance), ii) the capacity to mobilise different investments sources, iii) the capacity to trigger important overall investments with limited EU support and, where appropriate, iv) the extent to which externalities justify the CEF financial support. It shall be used to assess the catalytic effect of the EU financial support and determine whenever possible the actual co-funding rate to be granted.

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"[77].

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

[77] 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.

9.3 Other sources of financing

No EU financial support shall be awarded for actions receiving funds from other sources of EU financing, with exception of the Recovery and Resilience Facility and the InvestEU Programme, and without prejudice to Articles 6, 17 and 19 of the CEF Regulation.

9.4 Eligibility of costs and non-retroactivity principle

A grant may be awarded for an action which has already begun provided that the applicant can demonstrate the need for starting the action prior to signature of the grant agreement. In accordance with Article 193 of the Financial Regulation, costs incurred prior to the date of submission of the application shall not be eligible for financing. Costs incurred as of the date of submission of the grant application are considered eligible for financing. In accordance with Article 4(6) of the CEF Regulation, costs incurred as from 1 January 2021 are considered eligible for financing for actions selected on the basis of the first call for proposals under this multiannual work programme. No grant may be awarded retroactively for actions already completed.

10. State aid assessment

EU resources awarded directly by the Union do not constitute State Aid

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, in general, be notified to the Commission and approved before it is awarded and put into effect.

However, resources coming from the EU, European Investment Bank (EIB), European Investment Fund or international financial institutions (e.g. International Monetary Fund or the European Bank for Reconstruction and Development), are considered as State resources only if national authorities have discretion as to the use of these resources (e.g. concerning the selection of beneficiaries).

When **the above mentioned resources are awarded directly by the EU with no discretion on the part of the national authorities, they do not constitute State resources**[78]. For this reason, **funding awarded under the CEF Digital Programme**, does not constitute State aid.

Co-financing of CEF Digital projects with resources managed by the Member States

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 co-financing rates are foreseen for different categories of projects.

CEF Digital projects co-funded exclusively with private funds will not contain any State Aid element.

On the contrary, the **use of national funds** (including Cohesion Funds and the RRF) provided by a Member State or imputable to a Member State (e.g. via National Promotional Banks and Institutions, NBPIs, not acting 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. This is also the case of public resources used to fund projects having received a Seal of Excellence.

However, in certain cases these public funds may not constitute state aid or can be considered compatible with the TFEU without a notification (notably under the SGEI Decision or the General Block Exemption Regulation (GBER)[79]).

As recalled in the Commission Notice on the notion of State aid and in the relevant State aid guiding templates published by the Commission to assist Member States in the design of their national plans under the RRF "Guiding template: Measures to support the deployment and take-up of fixed and mobile very high capacity networks, including 5G and fibre networks "[80], public support to connectivity projects not used for economic activities (e.g. the exercise of public powers, certain health care and education activities) **may not constitute State aid**. The same principle applies to 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 GBER. The Commission has recently reviewed the GBER and has exempted from notification[81] State aid used to fund or co-fund certain CEF Digital projects financed 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

---

78 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

79 Commission Regulation (EU) 2021/1237 of 23 July 2021 amending Commission Regulation (EU) N°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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R1237

80 See https://ec.europa.eu/competition/state_aid/what_is_new/template_RFF_broadband_roll_out_and_demand_side_measures.pdf

81 See article 52b of the revised GBER.

of the European High-Performance Computing Joint Undertaking and iii) backbone networks interconnecting cloud infrastructures of certain SEDs as well as iv) certain submarine cables.

Double funding

Moreover, the implementation of CEF Digital will ensure that, when a project is supported (or has applied for support) also with State aid under any of the relevant applicable rules (such as, for instance, the Important Project of Common European Interest Communication, General Block Exemption Regulation, the Framework for State aid for research and development and innovation, the State aid guidelines for Broadband, or the State aid rules concerning SGEIs) double funding of the same costs as already supported by State aid will be avoided.

11. Prospective framework until 2027

The CEF Digital work programme beyond 2023 will build on the results of the first calls for proposals under this work programme and the relevant state of play of the project implementation. Calls for proposals after 2023 will take into account the new policy developments, including those resulting from the revision of relevant legislation.

It is envisaged that the remaining CEF digital budget (EUR 866,6 million) will be allocated, as tentatively presented in 7.2, to a future work programme covering the years 2024-2027.’